ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων,

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη υλοποίησης του πρωτοκόλλου IPsec με τη χρήση IP Encryptors στα IP δίκτυα της Βόρειο-Ατλαντικής Συμμαχίας (North Atlantic Treaty Organization, NATO)

Θωμάς Σ. Μπένος

Α.Μ. 19034

Εισηγήτρια: Ιωάννα Καντζάβελου, Επικ. Καθηγήτρια

(Κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη υλοποίησης του πρωτοκόλλου IPsec με τη χρήση IP Encryptors στα IP δίκτυα της Βόρειο-Ατλαντικής Συμμαχίας (North Atlantic Treaty Organization, NATO)

Θωμάς Σ. Μπένος

Α.Μ. 19034

Εισηγήτρια:

Ιωάννα Καντζάβελου, Επικ. Καθηγήτρια

Εξεταστική Επιτροπή:

Ιωάννα Καντζάβελου, Επικ. Καθηγήτρια Ioanna Kantzavelou Digitally signed by Ioanna Kantzavelou Date: 2021.07.27 18:25:58 +03'00'

Αντώνιος Μπόγρης, Καθηγητής Antonios Bogris Digitally signed by Antonios Bogris Date: 2021.07.28 09:13:23 +03'00'

Βασίλειος Μάμαλης, Καθηγητής Vasileios Mamalis Digitally signed by Vasileios Mamalis Date: 2021.07.27 23:18:09 +03'00'

Ημερομηνία εξέτασης:

26 Ιουλίου 2021

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Θωμάς Μπένος του Σπυρίδωνα, με αριθμό μητρώου 19034 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι …… και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή.

Ο Δηλών

Θωμάς Μπένος

(Κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Για την ολοκλήρωση της εργασίας αυτής, θα ήθελα να ευχαριστήσω την καθηγήτρια και επιβλέπουσα της εργασίας, κ. Καντζάβελου Ιωάννα, Επίκουρη Καθηγήτρια του τμήματος Μηχανικών Πληροφορικής και Υπολογιστών του Πανεπιστημίου Δυτικής Αττικής, για την υποστήριξη και την πολύτιμη βοήθειά της. Ακόμη, θα ήθελα να ευχαριστήσω θερμά τον Πλοίαρχο (Μ) κ. Παπαγεωργίου Σπυρίδωνα, Διευθυντή της Διεύθυνσης Κυβερνοασφάλειας του Γενικού Επιτελείου Εθνικής Άμυνας, για την συμβολή του και τις συμβουλές του σε όλη τη διαδικασία εκπόνησης της εργασίας. Τέλος, ένα μεγάλο ευχαριστώ χρωστώ στην γυναίκα μου Μαριάννα Μπάνου, της οποίας η πνευματική διαύγεια και η νοοτροπία αυτοβελτίωσης με ενέπνευσαν στο να κάνω τα πρώτα μου ακαδημαϊκά βήματα στο αντικείμενο της Πληροφορικής.

(Κενό φύλλο)

ΠΕΡΙΛΗΨΗ

Η κρυπτογραφία αποτελεί το πλέον διαδεδομένο εργαλείο για τη διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των πληροφοριών στις επικοινωνίες. Κατέχει δε κομβικό ρόλο στις στρατιωτικές επικοινωνίες, καθώς βοηθά στην προστασία απόρρητων πληροφοριών και ευαίσθητων δεδομένων, οι οποίες πρόκειται να «κυκλοφορήσουν» σε ένα δίκτυο. Αποτελεί τον κύριο τρόπο με τον οποίο μπορούν να μεταδίδονται με ασφάλεια μηνύματα μεταξύ των δυνάμεων μιας στρατιωτικής δομής, χωρίς η αντίπαλη δύναμη να έχει τη δυνατότητα παρεμπόδισης των μηνυμάτων ή και ανάγνωσής τους. Ακόμα κι αν το μήνυμα υποκλαπεί, θα πρέπει κατόπιν να αποκρυπτογραφηθεί ώστε να είναι σε αναγνώσιμη μορφή. Για την ασφάλεια επικοινωνιών σε στρατιωτικά IP δίκτυα χρησιμοποιούνται κυρίως συσκευές κρυπτογραφίας IP (IP Encryptors), οι οποίες μπορούν να προσφέρουν υψηλό βαθμό εμπιστευτικότητας ροής πληροφορίας, αυθεντικότητας και ακεραιότητας των δεδομένων, τα οποία ανταλλάσσονται σε ένα δίκτυο. Παρόλα αυτά, η ενσωμάτωση συσκευών αυτού του τύπου σε ένα δίκτυο, παρουσιάζει πρόσθετα προβλήματα στις περιπτώσεις δυσλειτουργίας τους ή της ανάγκης για συντήρηση και επισκευή, καθώς το κόστος προμήθειας - αντικατάστασής τους είναι σημαντικό για μία στρατιωτική δομή, και στις περιπτώσεις που η αντικατάστασή τους δε μπορεί να γίνει άμεσα, υπάρχει προσωρινή έλλειψη διαθεσιμότητας στο δίκτυο.

Σκοπός της πτυχιακής αυτής εργασίας είναι η μελέτη των IP Encryptors (ή αλλιώς, κρυπτομηχανών) που χρησιμοποιούνται για την υλοποίηση του IPSec στα IP δίκτυα της Βορειο-Ατλαντικής Συμμαχίας (ΝΑΤΟ), του τροπου λειτουργίας τους και ενσωμάτωσης του IPSec σε αυτές και θα αναλυθούν οι δυνατότητες μετάβασης από το μοντέλο ενσωμάτωσης του IPSec στις κρυπτομηχανές σε άλλο μοντέλο υλοποίησης του IPSec σε IP δίκτυα κορμού του ΝΑΤΟ, χωρίς τη χρήση ξεχωριστής IPSec συσκευής. Σε αυτή την εργασία, θα γίνει αρχικά παρουσίαση του πρωτοκόλλου IPsec, της αρχιτεκτονικής του και των τρόπων υλοποίησής του. Στη συνέχεια, θα περιγραφούν οι συσκευές κρυπτογράφησης IP

(IP Encryptors), σε ό,τι αφορά τη λειτουργία τους και τον τρόπο με τον οποίο χρησιμοποιούν το πρωτόκολλο IPsec. Επιπλέον, θα μελετηθούν τύποι συσκευών κρυπτογράφησης IP που έχουν αναπτυχθεί από εταιρείες τηλεπικοινωνιών και χρησιμοποιούνται από κράτη-μέλη της Βόρειο-Ατλαντικής Συμμαχίας (North-Atlantic Treaty Organization – NATO), οι οποίες θα συγκριθούν ως προς τις δυνατότητες και τη λειτουργία τους, και θα ερευνηθούν περαιτέρω οι απαιτήσεις του NATO ως προς τη σχεδίαση, αρχιτεκτονική και λειτουργία των συσκευών αυτών. Με τα παραπάνω ευρήματα, θα μελετηθεί κατά πόσο είναι δυνατή η μετάβαση από το μοντέλο IPSec με χρήση dedicated hardware στο μοντέλο χρήσης IPSec χωρίς dedicated hardware, με κριτήρια τη δυνατότητα συμμόρφωσης με τις προδιαγραφές - απαιτήσεις ασφαλείας που θέτει το NATO για τις συσκευές αυτές, του συνολικού κόστους που απαιτείται για την μετάβαση στο νέο μοντέλο καθώς και των πλεονεκτημάτων – μειονεκτημάτων του κάθε μοντέλου και θα γίνει παράθεση των συμπερασμάτων.

ABSTRACT

Cryptography is the most widely used tool to ensure the confidentiality and integrity of information in communications. It plays a key role in military communications, helping to protect confidential information and sensitive data that will be "circulated" on a network. It is the main way in which messages can be safely transmitted between the forces of a military structure, without the opposing force having the ability to block the messages or read them. Even if the message is intercepted, it must then be decrypted so that it is legible. IP Encryptors are mainly used for the security of communications in military IP networks, which can offer a high degree of confidentiality of information flow, authenticity and integrity of the data, which are exchanged in a network. However, the integration of such devices in a network presents additional problems in events of their malfunction or the need for maintenance and repair, as the cost of their supply or replacement is important for a military structure, and in cases where their replacement can not be done immediately, there is a temporary lack of availability in the network.

The purpose of this thesis is to study the IP Encryptors used for the implementation of IPSec in the IP networks of the North Atlantic Treaty Organization (NATO), how they operate and integrate IPSec and will examine the possibility of switching from the IPSec integration model in IP Encryptors to another IPSec implementation model in NATO IP backbone networks, without the use of a separate IPSec device. In this paper, the IPsec suite of protocols, its architecture and implementation modes will be presented first. Next, IP Encryptors will be described in terms of how they operate and how they integrate the IPsec suite of protocols. In addition, types of IP encryption devices developed by telecommunications companies and used by North Atlantic Treaty Organization (NATO) member states will be analyzed and compared in terms of their capabilities and operation, and NATO requirements for the design, architecture and operation of these devices will be further investigated. With the above findings, there will be a study of whether it is possible to switch from the IPSec model using dedicated hardware to the IPSec model without dedicated hardware. The criteria of this study will be the compliance with the specifications - security requirements set by NATO for these devices, the total cost required for the transition to the new model as well as the advantages - disadvantages of each model, and so, the conclusions will be presented.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια Δικτύων IP και Πληροφοριακών Συστημάτων

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: κρυπτομηχανή, IPSec, ΝΑΤΟ, IP δίκτυα, ενσωμάτωση, hosts, routers, κρυπτογράφηση, ακεραιότητα, ασφάλεια

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

IP Internet Protocol

IPSec Internet Protocol Security

NATO North Atlantic Treaty Organization

TCP Transmission Control Protocol

FTP File Transfer Protocol

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

UDP User Datagram Protocol

ICMP Internet Control Message Protocol

IGMP Internet Group Management Protocol

IETF Internet Engineering Task Force

MAC Message Authentication Code

VPN Virtual Private Network

NIST National Institute of Standards and Technology

DES Data Encryption Standard

AES Advanced Encryption Standard

MD5 Message Digest 5

SHA Secure Hash Algorithm

RSA Rivest-Shamir-Adleman

DSA Digital Signature Algorithm

FIPS Federal Information Processing Standard Publication

AH Authentication Header

ESP Encapsulating Security Payload

TTL Time To Live

NAT Network Address Translation

SPI Security Parameter Index

SA Security Association

DoS Denial of Service

ICV Integrity Check Value

IKE Internet Key Exchange

PSK Pre-Shared Key

DSS Digital Signature Standard

PKI Public Key Infrastructure

DH Diffie-Helman

SAD Security Association Database

GUI Graphical User Interface

CIK Crypto Ignition Key

NIAPC NATO Information Assurance Product Catalogue

INFOSEC Information Security

NIMP NATO Information Management Policy

IA Information Assurance

NHRC3S NATO Headquarters Consultation Command and Control

SECAN Security and Evaluation Agency

NCI Agency NATO Communications and Information Agency

CC Common Criteria

ISO International Organization for Standardization

TOE Target Of Evaluation

SFR Security Functional Requirements

SAR Security Assurance Requirements

PP Protection Profile

TEMPEST Telecommunications Electronics Material Protected from Emanating Spurious Transmissions

CE Compromising Emanations

NSTISSAM National Security Telecommunications and Information Systems Security Advisory Memorandum

SDIP SECAN Doctrine and Information Publication

NTA National Tempest Agency

DNS Domain Name System

BITE Built-In-Test Equipment

MTTF Mean-Time-To-Failure

MTBF Mean-Time-Between-Failures

OSPF Open Shortest Path First

GRE Generic Routing Encapsulation

VRRP Virtual Router Redundancy Protocol

FG Fill Gun

DHCP Dynamic Host Configuration Protocol

FIPS Federal Information Processing Standards

HAIPE High Assurance Internet Protocol Encryptor

HTTPS HyperText Transfer Protocol Secure

NSA National Security Agency

FCC Federal Communications Commission

JITC Joint Interoperability Test Command

CESG Communications-Electronics Security Group

CT Cipher-Text

PT Plain-Text

NPM Non Protectively Marked

POST Power-On-Self Test

ΚΣΔ Κεντρικό Σύστημα Διαχείρισης

MIL-STD Military Standard

BITS Bump-In-The-Stack

BITW Bump-In-The-Wire

RAM Random Access Memory

NVRAM Non-Volatile RAM

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ ΣΤΗΝ HARDWARE-BASED ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Για την υλοποίηση ασφαλών επικοινωνιών IP μεταξύ των διάφορων μονάδων μιας στρατιωτικής δομής του ΝΑΤΟ , όπως προαναφέρθηκε και θα αναλυθεί και εκτενέστερα στην παρούσα εργασία, χρησιμοποιούνται ως επί το πλείστον οι συσκευές κρυπτογραφίας IP. Με αυτό ως αφορμή, θα εξετάσουμε αρχικά την hardware-based κρυπτογράφηση γενικότερα, με τα υπέρ και τα κατά της.

Στην ουσία, η hardware-based κρυπτογράφηση αποτελεί την τεχνική με την οποία οι κρυπτογραφικοί αλγόριθμοι ενσωματώνονται σε υλικό συγκεκριμένου τύπου, όπως οι έξυπνες κάρτες (smart-cards) [79] προκειμένου ο κρυπτογραφικός αλγόριθμος να μπορεί να χρησιμοποιηθεί μόνο από τη συσκευή η οποία θα αναγνωρίσει την έξυπνη κάρτα. Έτσι, ο κρυπτογραφικός αλγόριθμος μπορεί να χρησιμοποιηθεί μόνο από το συνδυασμό συσκευής/κάρτας. Αποτελεί επίσης την τεχνική με την οποία η σουϊτα πρωτοκόλλων IPSec ενσωματώνεται ως “bump-in-the-wire", όπως θα αναλυθεί και στο κεφάλαιο 9, όπου τα χαρακτηριστικά του IPSec (κρυπτογράφηση, αυθεντικότητα) ενσωματώνονται στα IP πακέτα με την έξοδό τους από τον δρομολογητή σε μια ξεχωριστή ειδική συσκευή.

Τα πλεονεκτήματα της πρακτικής αυτής είναι ποικίλα. Οι συσκευές κρυπτογράφησης IP χρησιμοποιούν κατά την πλειονότητά τους, όπως θα δούμε και παρακάτω, ξεχωριστό επεξεργαστή (secure cryptoprocessor) για την κρυπτογράφηση των δεδομένων με τον αλγόριθμο κρυπτογράφησης. Έτσι, λόγω του ότι η κρυπτογράφηση δεν λαμβάνει χώρα

στον ίδιο επεξεργαστή στον οποίο λαμβάνουν χώρα και άλλες διεργασίες εκτός από κρυπτογράφηση δεδομένων (όπως π.χ στον επεξεργαστή ενός υπολογιστή), η διαδικασία της κρυπτογράφησης είναι πολύ ταχύτερη, με αποτέλεσμα να επιταχύνεται και η συνολική κρυπτογραφημένη επικοινωνία [79, 85, 86].

Επίσης, το γεγονός ότι οι κάρτες – κλειδιά και οι συσκευές είναι έτσι σχεδιασμένες ώστε να λειτουργούν ανά ζεύγη (μία συσκευή – μία κάρτα) ενισχύει τον παράγοντα της φυσικής ασφάλειας, καθώς η κρυπτογραφική ικανότητα της κρυπτοσυσκευής αφαιρείται με την αφαίρεση της κάρτας, καθώς δεν υπάρχει κρυπτογραφικός αλγόριθμος για να χρησιμοποιηθεί. Αν υπάρχει επίσης κεντρικό σύστημα διαχείρισης των κρυπτοσυσκευών, και μία από αυτές τις κάρτες βρεθεί σε λάθος χέρια, μπορεί να επισημανθεί από το σύστημα ως κακόβουλη και να μην επιδέχεται αναγνώρισης από τις λοιπές κρυπτοσυσκευές στο δίκτυο. Το ίδιο μπορεί να γίνει και με τις ίδιες τις κρυπτοσυσκευές, καθώς εάν κλαπεί μία κρυπτοσυσκευή, μπορεί να επισημανθεί από το σύστημα διαχείρισης ως κακόβουλη και να μην μπορεί να επικοινωνήσει με τις υπόλοιπες κρυπτοσυσκευές στο δίκτυο. Τα παραπάνω χαρακτηριστικά των κρυπτοσυσκευών θα αναλυθούν εκτενέστερα στο κεφάλαιο 3.

Ωστόσο, παρόλα τα πλεονεκτήματα της hardware-based encryption, υπάρχουν και σημαντικά μειονεκτήματα. Το πιο σημαντικό από όλα τα κατά είναι το κόστος. Η προμήθεια, συντήρηση ή και αντικατάσταση τέτοιων συσκευών, λόγω της πολυσύνθετης τεχνολογίας τους και της υψηλής ποιότητας υλικών που χρησιμοποιούνται για την κατασκευή τους έχει πολύ μεγάλο κόστος, οπότε συνήθως αυτές δε χρησιμοποιούνται παρά μόνο για την εμπιστευτικότητα πολύ ευαίσθητων δεδομένων, όπως τα δεδομένα που ανταλλάσσουν μεταξύ τους οι μονάδες μιας στρατιωτικής δομής. Ενδεικτικά, μία κρυπτοσυσκευή KG-240A με υποστηριζόμενη ταχύτητα 100 Mbps κοστίζει 11.700 $, και μία KG-245A με υποστηριζόμενη ταχύτητα 1 Gbps κοστίζει 21.810 $ [80]. Γενικά η επένδυση σε κρυπτομηχανές μπορεί να επιφέρει τον ύψιστο βαθμό ασφάλειας και ταχύτητας απόδοσης δικτύου για μια στρατιωτική δομή, όμως η απώλεια κάποιας συσκευής θα καθιστά μία ζεύξη μη κρυπτογραφικά λειτουργική (εφόσον οι συσκευές αυτές λειτουργούν ως ζεύγη των 2 για την επιτυχή κρυπτογραφημένη επικοινωνία μεταξύ δύο οντοτήτων), και οι πόροι που θα πρέπει να δαπανηθούν για την αντικατάστασή της θα μπορούσαν να δαπανηθούν σε

στοιχεία τα οποία είναι πιο σημαντικά για τη διεξαγωγή επιχειρήσεων, όπως πολεμοφόδια ή τρόφιμα.

Τα παραπάνω συντελούν στην προσπάθεια για αναζήτηση νέας λύσης για την ταχεία και ικανώς κρυπτογραφημένη επικοινωνία μεταξύ στρατιωτικών μονάδων, με την χρήση ειδικών συσκευών κρυπτογράφησης IP να περιορίζεται όσο το δυνατόν στο ελάχιστο. Έτσι, η παρούσα εργασία στα επόμενα κεφάλαια θα μελετήσει εκτενέστερα το IPSec, το πρωτόκολλο που χρησιμοποιείται κατά κόρον στη συμμετρική κρυπτογράφηση στις κρυπτοσυσκευές IP, θα εξετάσει τα χαρακτηριστικά των κρυπτομηχανών και τις προϋποθέσεις που πρέπει να πληρούν όπως αυτές τίθενται από την Βορειο-Ατλαντική Συμμαχία (ΝΑΤΟ). Με βάση αυτά τα χαρακτηριστικά, θα συγκριθούν οι δυνατότητες των μοντέλων ενσωμάτωσης του IPSec σε θεωρητικό επίπεδο και θα εξεταστεί αν είναι απαραίτητη και δυνατή η μετάβαση σε ένα νέο μοντέλο κρυπτογραφημένης επικοινωνίας.

ΚΕΦΑΛΑΙΟ 2

ΕΙΣΑΓΩΓΉ ΣΤΟ INTERNET PROTOCOL SECURITY (IPSEC)

2.1 Η ασφάλεια στο επίπεδο δικτύου

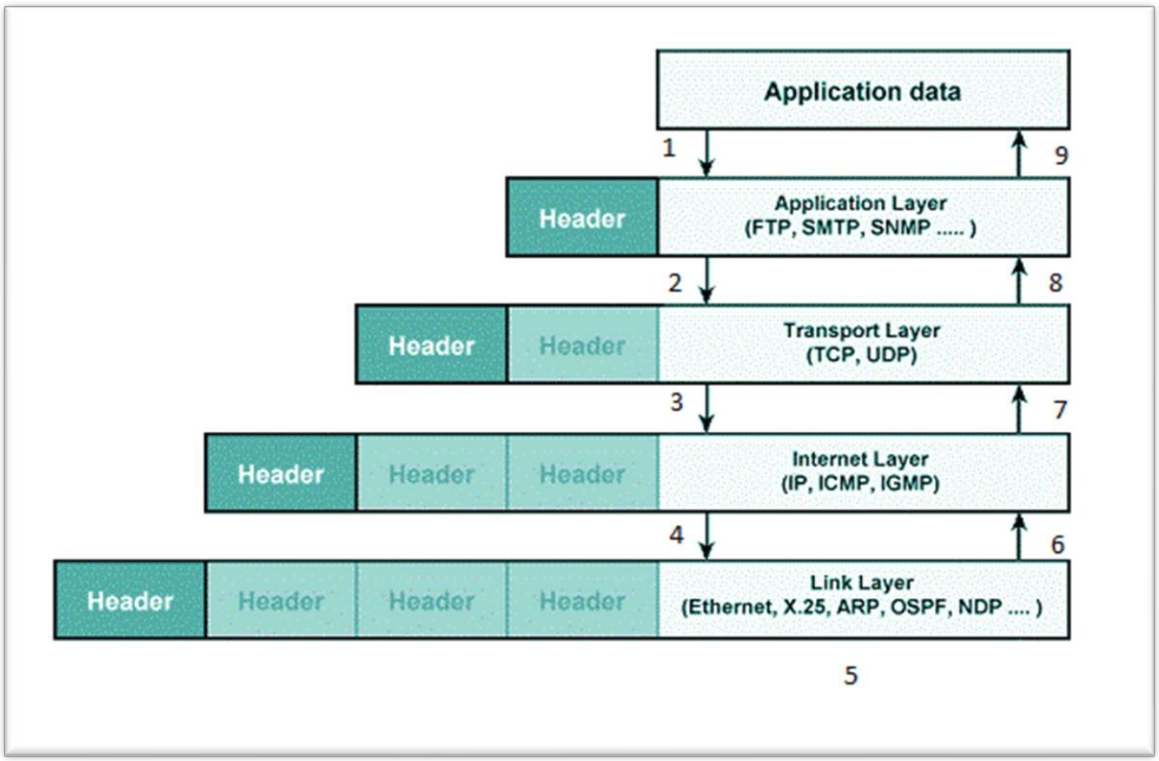
Είναι γενικά παραδεκτό ότι το πρωτόκολλο ελέγχου μετάδοσης (TCP) και το πρωτόκολλο διαδικτύου (IP) αποτελούν δύο από τα πιο σημαντικά πρωτόκολλα στο Διαδίκτυο. Οι επικοινωνίες TCP / IP αποτελούνται από πέντε αλληλοσυνεργαζόμενα επίπεδα, τα οποία φαίνονται στον Πίνακας 2.1**:** Τα επίπεδα TCP/IP [1]. Έτσι, όταν ένας χρήστης θέλει να αποστείλει δεδομένα μέσω κάποιου δικτύου, γίνεται μεταφορά των δεδομένων από το υψηλότερο επίπεδο μέσω ενδιάμεσων επιπέδων στο χαμηλότερο επίπεδο, όπου σε κάθε επίπεδο προστίθενται επιπλέον πληροφορίες με μορφή ετικετών (headers). Το χαμηλότερο επίπεδο αποστέλλει τα συσσωρευμένα δεδομένα μέσω του φυσικού δικτύου και εν συνεχεία τα δεδομένα μεταφέρονται στον τελικό προορισμό τους. Ουσιαστικά, τα δεδομένα που παράγονται από ένα επίπεδο ενθυλακώνονται σε ένα μεγαλύτερο στοιχείο δεδομένων, όπου σε αυτό προστίθενται τα δεδομένα του αμέσως επόμενου επιπέδου (Σχήμα 2.1: Ενθυλάκωση πακέτων (Πηγή: http://rupasundar.blogspot.com/2014/12/protocol-its-like-language-through.html)[1] [1].

---

[1] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77. p. 2-1

Όνομα Επιπέδου	***Λειτουργία Επιπέδου***
Επίπεδο Εφαρμογής (Application Layer)	*Σε αυτό το επίπεδο, στέλνονται και λαμβάνονται δεδομένα για συγκεκριμένες εφαρμογές, όπως το Domain Name System (DNS), το HyperText Transfer Protocol (HTTP) και το Simple Mail Transfer Protocol (SMTP).*
Επίπεδο Μεταφοράς (Transport Layer)	*Σε αυτό το επίπεδο παρέχονται υπηρεσίες προσανατολισμένες στη μεταφορά υπηρεσιών επιπέδου εφαρμογών μεταξύ δικτύων. Το επίπεδο μεταφοράς μπορεί προαιρετικά να διασφαλίσει την αξιοπιστία των επικοινωνιών. Το πρωτόκολλο ελέγχου μετάδοσης (TCP) και το πρωτόκολλο δεδομένων χρήστη (UDP) είναι συνήθως χρησιμοποιούμενα πρωτόκολλα επιπέδου μεταφοράς.*
Επίπεδο Δικτύου (Network Layer)	*Αυτό το επίπεδο δρομολογεί πακέτα μεταξύ δικτύων. Το Internet Protocol (IP) είναι το βασικό πρωτόκολλο επιπέδου δικτύου στη σουϊτα TCP / IP. Άλλα κοινά χρησιμοποιούμενα πρωτόκολλα στο επίπεδο δικτύου είναι το Internet Control Message Protocol (ICMP) και το Internet Group Management Protocol (IGMP).*
Επίπεδο Συνδέσμου Δεδομένων (Data Link Layer)	*Αυτό το επίπεδο χειρίζεται τις επικοινωνίες στο φυσικό δίκτυο. Το πιο γνωστό πρωτόκολλο επιπέδου σύνδεσης δεδομένων είναι το Ethernet.*

Πίνακας 2.1: Τα επίπεδα TCP/IP [1]



Σχήμα 2.1: Ενθυλάκωση πακέτων (Πηγή: http://rupasundar.blogspot.com/2014/12/protocol-its-like-language-through.html)

Υπάρχουν έλεγχοι ασφαλείας για επικοινωνίες δικτύου σε κάθε επίπεδο του μοντέλου TCP/IP. Όπως εξηγήθηκε προηγουμένως, τα δεδομένα μεταφέρονται από το υψηλότερο στο χαμηλότερο επίπεδο, με κάθε επίπεδο να προσθέτει περισσότερες πληροφορίες. Εξαιτίας αυτού, ένας έλεγχος ασφαλείας σε υψηλότερο επίπεδο δεν μπορεί να παρέχει πλήρη προστασία για τα κατώτερα επίπεδα, επειδή τα κατώτερα επίπεδα εκτελούν λειτουργίες την ύπαρξη των οποίων τα ανώτερα επίπεδα δεν γνωρίζουν[2] [1]. Για παράδειγμα, εάν χρησιμοποιηθεί ένας έλεγχος ασφαλείας στο επίπεδο μεταφοράς (transport layer), θα παρέχεται ασφάλεια στα δεδομένα/λειτουργίες του επιπέδου εφαρμογής και του επιπέδου μεταφοράς, αλλά όχι του επιπέδου δικτύου και του επιπέδου συνδέσμου δεδομένων (data link).

---

[2] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77. p. 2-1

Για αυτό το λόγο, οι έλεγχοι ασφάλειας επιπέδου δικτύου (network layer) χρησιμοποιούνται για την ασφάλεια των επικοινωνιών, ιδίως μέσω δημοσίων δικτύων όπως το Internet, επειδή μπορούν να παρέχουν προστασία για πολλές εφαρμογές ταυτόχρονα χωρίς να τις τροποποιήσουν. Τα πλεονεκτήματα των ελέγχων ασφαλείας επιπέδου δικτύου συνοψίζονται στα παρακάτω:

- Τα στοιχεία ελέγχου σε αυτό το επίπεδο ισχύουν για εφαρμογές κάθε τύπου και δεν εστιάζουν σε συγκεκριμένες εφαρμογές (όπως π.χ τα στοιχεία ελέγχου στο επίπεδο εφαρμογής). Για παράδειγμα, όλες οι επικοινωνίες δικτύου μεταξύ δύο κεντρικών υπολογιστών μπορούν να προστατευτούν σε αυτό το επίπεδο χωρίς να απαιτείται η τροποποίηση εφαρμογών σε clients ή servers.
- Λόγω της δυσκολίας που ενέχει η προσθήκη ελέγχων ασφαλείας σε μεμονωμένες εφαρμογές, τα στοιχεία ελέγχου επιπέδου δικτύου αποτελούν καλύτερη λύση σε πολλές περιπτώσεις.
- Με την εφαρμογή ελέγχων ασφαλείας στο network layer είναι ευκολότερο για τους διαχειριστές των δικτύων να εφαρμόζουν πολιτικές ασφαλείας.
- Δεδομένου ότι σε αυτό το επίπεδο προστίθεται η πληροφορία του IP (π.χ. διεύθυνση IP), τα στοιχεία ελέγχου μπορούν να προστατεύσουν τόσο τα δεδομένα των επιπέδων εφαρμογής και μεταφοράς όσο και τις πληροφορίες της διεύθυνσης IP για κάθε διερχόμενο πακέτο, προστατεύοντας έτσι στην ουσία την ταυτότητα του αποστολέα και του παραλήπτη[3] [1].

Παρόλα αυτά, αυτοί οι έλεγχοι ασφάλειας δεν παρέχουν δυνατότητα ευελιξίας για την εστίαση στην προστασία συγκεκριμένων εφαρμογών από ότι οι αντίστοιχοι έλεγχοι στα επίπεδα μεταφοράς και εφαρμογών. Από τα παραπάνω, είναι προφανές ότι τα στοιχεία ελέγχου και ασφάλειας τα οποία εφαρμόζονται στο αμέσως επόμενο επίπεδο (data link) μπορούν να προστατεύσουν τόσο τα δεδομένα όσο και την IP πληροφορία. Επειδή όμως τα στοιχεία ελέγχου στο επίπεδο data link μπορούν να χρησιμοποιηθούν ειδικά μόνο για έναν συγκεκριμένο φυσικό σύνδεσμο, δεν είναι κατάλληλα για την προστασία συνδέσεων

---

[3] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77. p. 2-2, 2-3

με πολλαπλούς συνδέσμους. Μια τοπολογία στο Διαδίκτυο αποτελείται συνήθως από πολλούς φυσικούς συνδέσμους που συνδέονται μεταξύ τους. Η προστασία μιας τέτοιας σύνδεσης με στοιχεία ελέγχου επιπέδου data link θα απαιτούσε την εφαρμογή χωριστά του ελέγχου σε κάθε σύνδεσμο από τον οποίο θα διερχόταν το πακέτο, κάτι που δεν είναι εφικτό σε τοπολογίες στις οποίες υπάρχουν πολλοί δρομολογητές από τους οποίους το πακέτο πρέπει να διέλθει[4] [1]. Οπότε, στις περιπτώσεις όπου απαιτείται η προστασία μιας τοπολογίας δικτύου με πολλαπλούς συνδέσμους και κόμβους, η χρήση στοιχείων ελέγχου στο επίπεδο δικτύου είναι σχεδόν επιβεβλημένη. Σε αυτή την κατηγορία στοιχείου ελέγχου ανήκει και το πρωτόκολλο IPSec, του οποίου η αρχιτεκτονική και λειτουργία μελετάται σε αυτή την ενότητα.

2.2 Ορισμός του IPSec και τύποι προστασίας

Σε ένα δίκτυο, για να θεωρηθεί ασφαλές, πρέπει να οριστεί μια ισχυρή πολιτική ασφάλειας που καθορίζει επ'ακριβώς την ελευθερία πρόσβασης σε πληροφορίες και υπαγορεύει την ανάπτυξη ασφάλειας στο δίκτυο. Το Internet Protocol Security (IPSec) αποτελεί ένα framework για τη διασφάλιση ασφαλών επικοινωνιών μέσω δημόσιων δικτύων. Με βάση τα πρότυπα που αναπτύχθηκαν από την IETF, το IPsec διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των δεδομένων που ανταλλάσσονται σε ένα δημόσιο δίκτυο. Στην ουσία, δημιουργεί μια γραμμή οριοθέτησης μεταξύ μη προστατευμένων και προστατευμένων interfaces σε έναν user ή ένα δίκτυο. Σε κάθε πακέτο που πρόκειται να διασχίσει το όριο εφαρμόζεται ένας έλεγχος πρόσβασης που καθορίζεται από τον χρήστη ή τον διαχειριστή ασφαλείας. Αυτός ο έλεγχος καθορίζει εάν τα πακέτα θα διασχίζουν το όριο χωρίς την εφαρμογή πολιτικής ασφαλείας σε αυτά, αν θα εφαρμοστούν σε αυτά πολιτικές ασφαλείας ή εάν θα απορρίπτονται. Η εφαρμογή των πολιτικών

[4] p. 2-2 – 2-3

ασφαλείας του IPsec γίνεται στο επίπεδο δικτύου μέσω επιλογής κατάλληλων πρωτοκόλλων ασφαλείας, κρυπτογραφικών αλγορίθμων και κρυπτογραφικών κλειδιών[5] [3]. Ανάλογα με τον τρόπο εφαρμογής και διαμόρφωσης του IPsec, το IPSec μπορεί να παρέχει οποιονδήποτε συνδυασμό των ακόλουθων τύπων προστασίας:

- **Εμπιστευτικότητα (Confidentiality)**: Το IPSec μπορεί να διασφαλίσει ότι τα δεδομένα που ανταλλάσσονται δεν μπορούν να διαβαστούν από μη εξουσιοδοτημένα μέρη. Αυτό μπορεί να επιτευχθεί με την κρυπτογράφηση των δεδομένων με τη χρήση ενός κρυπτογραφικού αλγορίθμου και ενός μυστικού κλειδιού, το οποίο αποτελεί μια τιμή γνωστή μόνο στα δύο μέρη που ανταλλάσσουν δεδομένα. Τα δεδομένα μπορούν να αποκρυπτογραφηθούν μόνο από κάποιον που έχει τον αλγόριθμο και το μυστικό κλειδί.
- **Ακεραιότητα (Integrity)**: Το IPsec μπορεί να προσδιορίσει εάν τα δεδομένα έχουν μεταβληθεί κατά οποιοδήποτε τρόπο (σκόπιμα ή ακούσια) κατά την κίνησή τους στο δίκτυο. Η ακεραιότητα των δεδομένων διασφαλίζεται με τη δημιουργία μίας τιμής κωδικού αυθεντικότητας μηνυμάτων (MAC), η οποία αποτελεί ένα κρυπτογραφικό άθροισμα ελέγχου (checksum) των δεδομένων. Εάν τα δεδομένα τροποποιηθούν και το MAC υπολογιστεί ξανά, το MAC των αυθεντικών δεδομένων θα διαφέρει από το MAC των τροποποιημένων δεδομένων.
- **Αυθεντικότητα (Authentication)**: Κάθε IPsec endpoint επιβεβαιώνει την ταυτότητα του άλλου IPsec endpoint με το οποίο επιθυμεί να επικοινωνήσει, διασφαλίζοντας ότι η κυκλοφορία του δικτύου και τα δεδομένα αποστέλλονται από τον αναμενόμενο κεντρικό υπολογιστή[6] [1].
- **Προστασία από replay attacks (Replay Protection)**: Η replay attack είναι μια μορφή επίθεσης στο δίκτυο στην οποία μια έγκυρη μετάδοση δεδομένων επαναλαμβάνεται ή καθυστερεί κακόβουλα ή με δόλο. Είναι μια προσπάθεια ανατροπής της ασφάλειας από κάποιον που προσπαθεί να καταγράφει κρυπτογραφημένα

---

5 Kent, S. and Seo, K. (2005). *Security Architecture for the Internet Protocol*. RFC 4301.

6 Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77. p. 2-3

πακέτα και τα επανεκπέμπει στον έγκυρο παραλήπτη τους προκειμένου να πλαστοπροσωπήσει έναν έγκυρο χρήστη και να προκαλέσει αρνητικές επιπτώσεις. Το IPSec παρέχει προστασία κατά της replay attack με την εκχώρηση ενός μονοτονικά αυξανόμενου αριθμού ακολουθίας σε κάθε κρυπτογραφημένο πακέτο[7] [2]. Ωστόσο, το IPsec δεν διασφαλίζει ότι τα δεδομένα παραδίδονται με την ακριβή σειρά με την οποία αποστέλλονται.

- **Προστασία Ανάλυσης Κυκλοφορίας (Traffic Analysis Protection):** Ένα άτομο που παρακολουθεί την κυκλοφορία του δικτύου δεν γνωρίζει ποια μέρη επικοινωνούν, πόσο συχνά πραγματοποιούνται επικοινωνίες ή πόσα δεδομένα ανταλλάσσονται. Ωστόσο, ο αριθμός των πακέτων που ανταλλάσσονται σε ένα δίκτυο είναι μετρήσιμος.
- **Έλεγχος πρόσβασης (Access Control):** Τα τελικά σημεία IPsec μπορούν να κάνουν filtering για να διασφαλίσουν ότι μόνο εξουσιοδοτημένοι χρήστες IPsec έχουν πρόσβαση σε συγκεκριμένους πόρους δικτύου. Τα τελικά σημεία IPsec μπορούν επίσης να επιτρέπουν ή να αποκλείουν συγκεκριμένους τύπους κίνησης δικτύου, όπως η πρόσβαση σε διακομιστή Web, αλλά η άρνηση κοινοποίησης αρχείων[8] [1].

---

7 Basu A., Zhang W., Naik N. (2016). IPsec Anti-Replay Check Failures, Available at: www.cisco.com.

8 Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77. p. 2-3 – 2-4

2.3 Η Κρυπτογραφία στα Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks – VPN)

Το IPSec έχει γίνει ο πιο κοινός έλεγχος ασφαλείας επιπέδου δικτύου, που χρησιμοποιείται συνήθως για τη δημιουργία ενός εικονικού ιδιωτικού δικτύου (Virtual Private Network - VPN). Το VPN αποτελεί ένα εικονικό δίκτυο που χρησιμοποιεί την υποδομή των υπαρχόντων φυσικών δικτύων για να παρέχει έναν ασφαλή μηχανισμό επικοινωνίας για δεδομένα που μεταδίδονται μέσω αυτών των δικτύων[9] [1]. Ένα εικονικό ιδιωτικό δίκτυο επεκτείνει ένα ιδιωτικό δίκτυο σε ένα δημόσιο δίκτυο και επιτρέπει στους χρήστες να στέλνουν και να λαμβάνουν δεδομένα σε κοινόχρηστα ή δημόσια δίκτυα σαν να ήταν οι υπολογιστικές τους συσκευές απευθείας συνδεδεμένες στο ιδιωτικό δίκτυο. Οι εφαρμογές που εκτελούνται μέσω ενός VPN ενδέχεται επομένως να επωφεληθούν από τη λειτουργικότητα, την ασφάλεια και τη διαχείριση του ιδιωτικού δικτύου[10] [6]. Σύμφωνα με το NIST, τα VPN χρησιμοποιούνται συχνότερα για την προστασία των επικοινωνιών που μεταφέρονται μέσω δημόσιων δικτύων όπως το Διαδίκτυο και μπορούν να παρέχουν διάφορους τύπους προστασίας δεδομένων, διευκολύνοντας έτσι την ασφαλή μεταφορά ευαίσθητων δεδομένων σε δημόσια δίκτυα. Τα VPN μπορούν επίσης να παρέχουν ευέλικτες λύσεις, όπως η διασφάλιση επικοινωνιών μεταξύ απομακρυσμένων διακομιστών ενός οργανισμού, ανεξάρτητα από το πού βρίσκονται οι διακομιστές. Ένα VPN μπορεί ακόμη και να δημιουργηθεί σε ένα μόνο ιδιωτικό δίκτυο για την προστασία ιδιαίτερα ευαίσθητων επικοινωνιών από άλλα μέρη στο ίδιο δίκτυο[11] [1]. Ένα VPN είναι εικονικό, επειδή δεν υπάρχει πραγματική απευθείας σύνδεση δικτύου μεταξύ των δύο (ή περισσότερων) συνεργατών επικοινωνίας, αλλά μόνο μια εικονική σύνδεση που παρέχεται από το λογισμικό VPN, η οποία πραγματοποιείται μέσω υποδομής δημόσιου δικτύου και ιδιωτική, επειδή μόνο

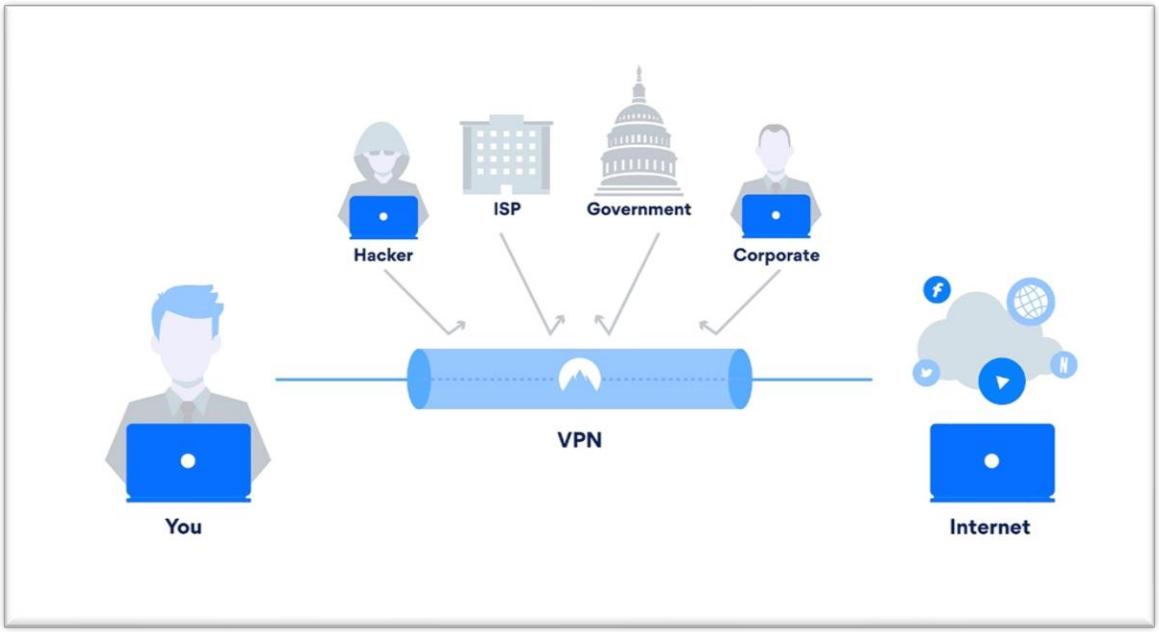
---

9 Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.p. 2-4

10 Mason, A. G. (2002). Cisco Secure Virtual Private Network. Cisco Press, p. 7

11 Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.p. 2-4

τα συμβαλλόμενα μέρη που συνδέονται με το λογισμικό VPN επιτρέπεται να διαβάζουν τα δεδομένα που μεταφέρονται[12] [5].



Σχήμα 2.1: Το Εικονικό Ιδιωτικό Δίκτυο (VPN) [87]

Η κρυπτογραφία αποτελεί ένα σημαντικό στοιχείο των VPN συνδέσεων, αν και δεν είναι εγγενώς συνυφασμένο με αυτές. Τα VPN μπορούν να χρησιμοποιούν τόσο συμμετρικές όσο και ασύμμετρες μορφές κρυπτογραφίας. Στη συμμετρική κρυπτογραφία χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και για την αποκρυπτογράφηση των δεδομένων, ενώ στην ασύμμετρη κρυπτογραφία χρησιμοποιούνται ξεχωριστά κλειδιά για κρυπτογράφηση και αποκρυπτογράφηση ή για ψηφιακή υπογραφή και επαλήθευση υπογραφής. Το NIST θεωρεί ότι η συμμετρική κρυπτογραφία γενικά θεωρείται πιο αποτελεσματική και απαιτεί λιγότερη επεξεργαστική ισχύ από την ασύμμετρη κρυπτογραφία, γι' αυτό συνήθως είναι συνήθης η χρήση της για την κρυπτογράφηση του όγκου των δεδομένων που αποστέλλονται μέσω ενός VPN. Παρόλα αυτά, το NIST τονίζει ότι για τη διασφάλιση

[12] Feilner, M. "Chapter 1 - VPN—Virtual Private Network". OpenVPN: Building and Integrating Virtual Private Networks: Learn How to Build Secure VPNs Using this Powerful Open Source Application, Packt Publishing.

της εμπιστευτικότητας, ο τρόπος με τον οποίο θα γίνει η ανταλλαγή του κλειδιού μεταξύ των συμβαλλομένων μερών (προκειμένου να μπορούν να συμμετέχουν στη διαδικασία της κρυπτογράφησης - αποκρυπτογράφησης) θα πρέπει να είναι εκτός ζώνης (out-of-band), που σημαίνει ότι θα πρέπει για την ανταλλαγή αυτή να χρησιμοποιηθεί ξεχωριστό από το υπόλοιπο δίκτυο και ασφαλές κανάλι επικοινωνίας (συνήθως η μη ηλεκτρονική μεταφορά αλλά η φυσική μεταφορά του κλειδιού ενδείκνυται σε αυτές τις περιπτώσεις)[13] [1].

Το NIST παραθέτει τους παρακάτω αλγορίθμους, ως συνήθεις αλγορίθμους αλγόριθμοι υλοποίησης της συμμετρικής κρυπτογραφίας:

- Ψηφιακό Πρότυπο Κρυπτογράφησης (DES)
- Τριπλό DES (3DES)
- Προηγμένο Πρότυπο Κρυπτογράφησης (AES)
- Blowfish
- RC4
- Διεθνής αλγόριθμος κρυπτογράφησης δεδομένων (IDEA)
- Αλγόριθμοι HMAC:
    - Message Digest 5 (MD5)
    - Secure Hash Algorithm (SHA-1).

Η ασύμμετρη κρυπτογραφία (επίσης γνωστή ως κρυπτογραφία δημόσιου κλειδιού) χρησιμοποιεί δύο ξεχωριστά κλειδιά για την ασφαλή ανταλλαγή δεδομένων σε ένα δίκτυο. Το ένα κλειδί χρησιμοποιείται για την κρυπτογράφηση ή την ψηφιακή υπογραφή των δεδομένων και το άλλο κλειδί χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων ή την επαλήθευση της ψηφιακής υπογραφής. Αυτά τα κλειδιά αναφέρονται συχνά ως συνδυασμοί δημόσιου / ιδιωτικού κλειδιού. Εάν το δημόσιο κλειδί ενός ατόμου (το οποίο μπορεί να κοινοποιηθεί σε άλλους) χρησιμοποιείται για την κρυπτογράφηση δεδομένων, τότε μόνο το ιδιωτικό κλειδί του ίδιου ατόμου (το οποίο είναι γνωστό μόνο στο άτομο)

---

[13] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77.p. 2-4

μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση των δεδομένων. Εάν το ιδιωτικό κλειδί ενός ατόμου χρησιμοποιείται για την ψηφιακή υπογραφή δεδομένων, τότε μόνο το δημόσιο κλειδί του ίδιου ατόμου μπορεί να χρησιμοποιηθεί για την επαλήθευση της ψηφιακής υπογραφής.

Το NIST παραθέτει τους παρακάτω αλγορίθμους, ως συνήθεις αλγορίθμους εφαρμογής ασύμμετρης κρυπτογραφίας:

- RSA (Rivest Shamir Adleman)
- Digital Signature Algorithm (DSA)
- Elliptic Curve DSA (ECDSA)[14] [1].

Οι περισσότερες υλοποιήσεις του IPSec υλοποιούν έναν συνδυασμό συμμετρικής και ασύμμετρης κρυπτογραφίας. Η ασύμμετρη κρυπτογραφία χρησιμοποιείται για τον έλεγχο ταυτότητας των ταυτοτήτων και των δύο μερών, ενώ η συμμετρική κρυπτογράφηση χρησιμοποιείται για την προστασία των πραγματικών δεδομένων[15] [1]. Αξίζει να σημειωθεί ότι δεν είναι όλοι οι αλγόριθμοι κατάλληλοι σε κάθε περίπτωση. Για παράδειγμα, οι ομοσπονδιακές υπηρεσίες πρέπει να χρησιμοποιούν αλγόριθμους κρυπτογράφησης εγκεκριμένους από την ομοσπονδιακή τυποποιημένη έκδοση επεξεργασίας πληροφοριών 140-2 (Federal Information Processing Standard Publication - FIPS 140-2, Παράρτημα “A”), το οποίο είναι ένα αμερικανικό κυβερνητικό πρότυπο ασφάλειας που χρησιμοποιείται γενικά για τον χαρακτηρισμό ενός υλικού ως κρυπτοϋλικού[16] [7].

---

[14] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77.p. 2-4

[15] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77.p. 2-4

[16] National Institute of Standards and Technology (2007). *FIPS PUB 140-2: Security Requirements for Cryptographic Modules.*

Τα VPN μπορούν να μειώσουν σημαντικά τους κινδύνους ασφαλείας επικοινωνιών που πραγματοποιούνται μέσω δημόσιων δικτύων, όμως δεν μπορούν να τους εξαλείψουν εντελώς. Για παράδειγμα:

- Τα ελαττώματα σε έναν αλγόριθμο κρυπτογράφησης ή το λογισμικό που εφαρμόζει τον αλγόριθμο θα μπορούσαν να επιτρέψουν στους εισβολείς να αποκρυπτογραφήσουν την παρεμποδισμένη κίνηση.
- Οι γεννήτριες τυχαίων αριθμών που δεν παράγουν επαρκώς τυχαίες τιμές θα μπορούσαν να παρέχουν επιπλέον δυνατότητες επίθεσης.
- Η ανακάλυψη ενός κλειδιού κρυπτογράφησης από έναν εισβολέα μπορεί να οδηγήσει στην αποκρυπτογράφηση της πληροφορίας αλλά και την εκμετάλλευσή της για την εμφάνιση του εισβολέα ως νόμιμου χρήστη.

Παρόλο που τα VPN επαυξάνουν την εμπιστευτικότητα και την ακεραιότητα των δεδομένων, γενικά δεν βελτιώνουν τη διαθεσιμότητα, δηλαδή τη δυνατότητα των εξουσιοδοτημένων χρηστών να έχουν πρόσβαση σε συστήματα όπως απαιτείται. Στην πραγματικότητα, η διαθεσιμότητα σε πολλές εφαρμογές του VPN τείνει στο να μειώνεται κάπως επειδή στην υπάρχουσα υποδομή δικτύου προστίθενται περισσότερα στοιχεία - υπηρεσίες. Αυτό εξαρτάται σε μεγάλο βαθμό από το επιλεγμένο μοντέλο αρχιτεκτονικής VPN και τις λεπτομέρειες της εφαρμογής του[17] [1].

2.4 Μοντέλα Αρχιτεκτονικής IPSec VPN

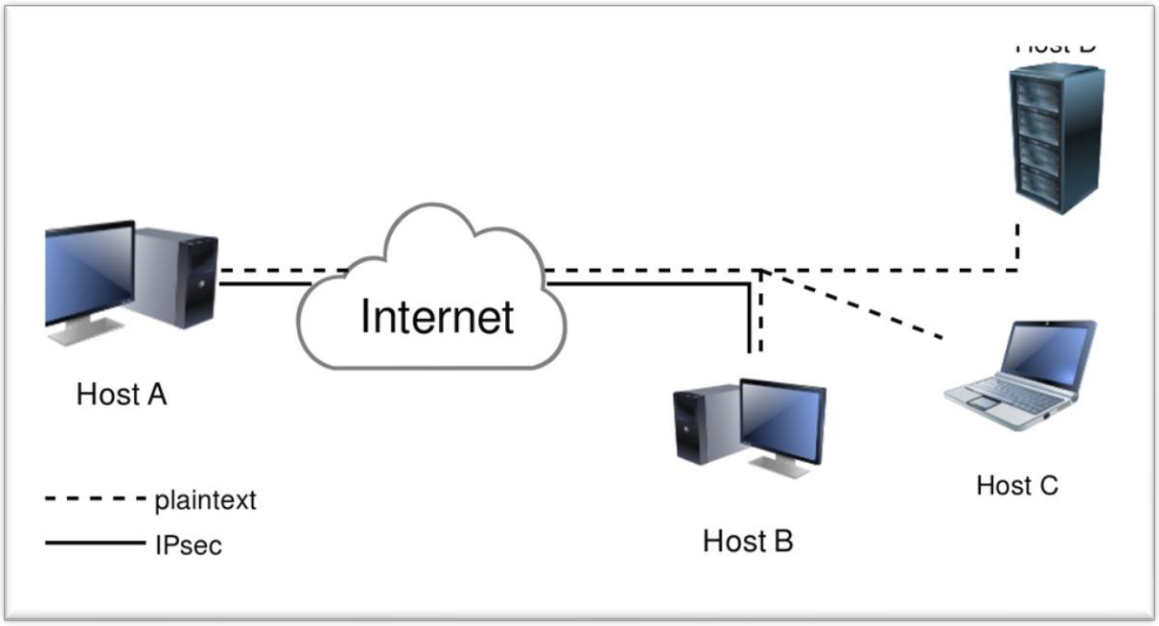
Οι τρεις κύριες αρχιτεκτονικές του IPsec VPN είναι οι παρακάτω:

- host-to-host
- host-to-gateway και
- gateway-to-gateway.

---

[17] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77.p. 2-5

2.4.1 Host-to-host

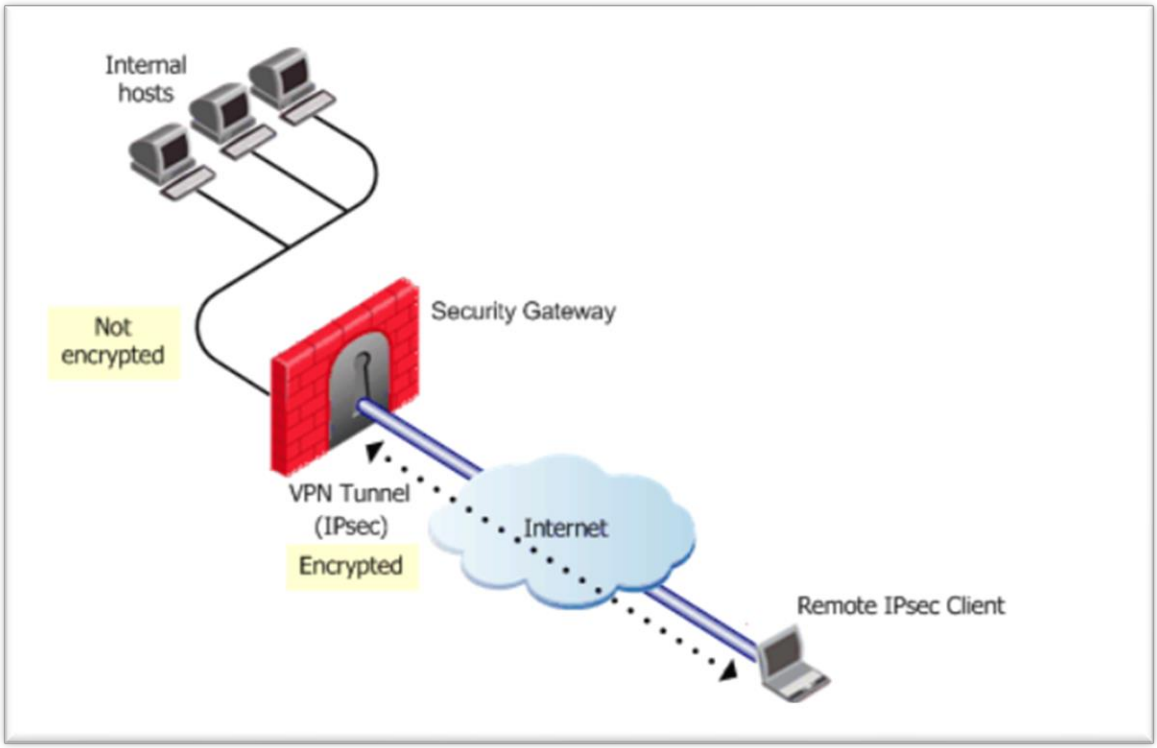


Σχήμα 2.2: Η αρχιτεκτονική host-to-host [88]

Σε αυτό το μοντέλο, δημιουργούνται ξεχωριστά συνδέσεις IPsec για κάθε μεμονωμένο χρήστη VPN. Ένας IPsec client ο οποίος επιθυμεί να ανταλλάξει πληροφορίες με έναν IPsec server σε ασφαλές κανάλι, στην αρχική τους επικοινωνία ζητά από τον IPsec server να πραγματοποιήσει έλεγχο ταυτότητας πριν τη δημιουργία της σύνδεσης. Ο server και ο client ανταλλάσσουν πληροφορίες και εάν ο έλεγχος ταυτότητας είναι επιτυχής, δημιουργείται η σύνδεση IPsec. Έπειτα από αυτό, ο client θα μπορεί να αιτηθεί τις ευαίσθητες πληροφορίες του server και η κίνηση του δικτύου μεταξύ του κεντρικού υπολογιστή του client και του server θα προστατεύεται από την IPsec σύνδεση. Το host-to-host είναι το μόνο μοντέλο που παρέχει προστασία στα δεδομένα που ανταλάσσονται καθ 'όλη τη διαδρομή τους από τον ένα τελικό χρήστη στον άλλο (end-to-end). Αυτό μπορεί να αποτελεί πρόβλημα, επειδή τα network-based firewalls, τα IDS και άλλες παρόμοιες συσκευές-λειτουργίες δεν μπορούν να επιθεωρήσουν αποτελεσματικά τα αποκρυπτογραφημένα δεδομένα εφόσον παρακάμπτουν αποτελεσματικά ορισμένα επίπεδα ασφαλείας. Γενικά τα μοντέλα VPN Host-to-Host δεν παρέχουν διαφάνεια στο χρήστη, επειδή ο ίδιος ο χρήστης αλληλεπιδρά με το λογισμικό κατά τον απαραίτητο έλεγχο ταυτότητας πριν από τη

χρήση του VPN. Επίσης, το σύνολο των users/servers που θα συμμετέχουν σε κάποιο VPN πρέπει να έχουν εγκατεστημένο λογισμικό VPN (VPN client software). Το μοντέλο host-to-host χρησιμοποιείται συχνότερα όταν ένας μικρός αριθμός αξιόπιστων χρηστών πρέπει να χρησιμοποιήσει ή να διαχειριστεί ένα απομακρυσμένο σύστημα που απαιτεί τη χρήση μη ασφαλών πρωτοκόλλων και μπορεί να παρέχει υπηρεσίες VPN[18] [1].

2.4.2 Host-to-gateway



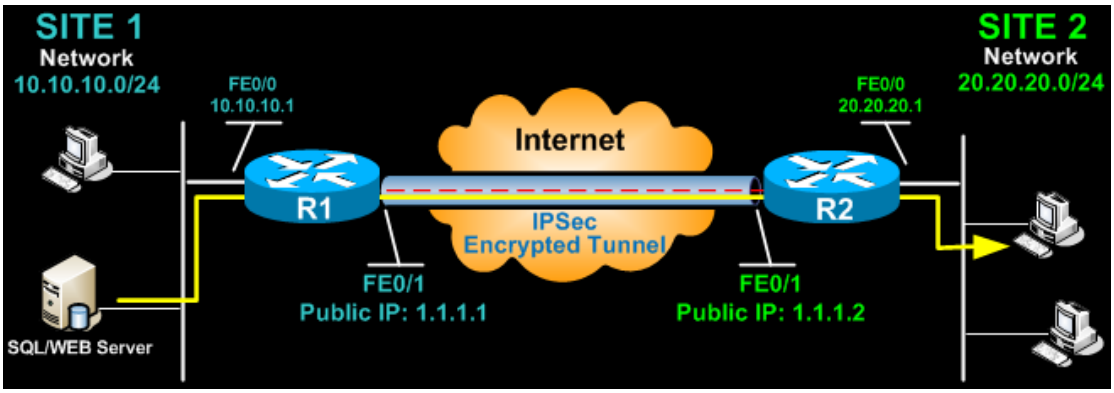
Σχήμα 2.3: Η αρχιτεκτονική host-to-gateway [89]

[18] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.p. 2-7 – 2-8

Σε αυτό το μοντέλο, ένας οργανισμός αναπτύσσει μια VPN gateway στο network edge. Στη συνέχεια δημιουργείται μια σύνδεση VPN για κάθε χρήστη απομακρυσμένης πρόσβασης μεταξύ του κεντρικού υπολογιστή του χρήστη και της VPN gateway. Η VPN gateway μπορεί να είναι μια dedicated συσκευή ή μέρος μιας άλλης συσκευής δικτύου (π.χ router). Όταν ένας user θέλει να χρησιμοποιήσει τους πόρους ενός οργανισμού, αρχικά εκκινεί την επικοινωνία με την VPN gateway του οργανισμού αφού συνήθως πρώτα πραγματοποιηθεί ένας έλεγχος ταυτότητας για να αποκτήσει ο χρήστης πρόσβαση στο VPN. Ο έλεγχος αυτός μπορεί να πραγματοποιηθεί είτε από την ίδια την πύλη είτε με τη συμβουλή ενός dedicated server για ελέγχους ταυτότητας. Αφού πιστοποιηθεί η ταυτότητα του client, ο client και η gateway ανταλλάσσουν πληροφορίες και δημιουργείται η IPsec σύνδεση. Η κίνηση δικτύου μεταξύ του χρήστη και της gateway προστατεύεται από την IPsec VPN σύνδεση και ο χρήστης μπορεί ακίνδυνα να χρησιμοποιήσει τους πόρους του οργανισμού. Ένα τέτοιο παράδειγμα αποτελεί και η σύνδεση των φοιτητών του Πανεπιστημίου Δυτικής Αττικής με την VPN Gateway του Πανεπιστημίου. Επίσης, η κίνηση δικτύου μεταξύ του χρήστη και των πόρων που δεν ελέγχονται από τον οργανισμό (άλλες θέσεις δικτύου) μπορεί επίσης να δρομολογηθεί μέσω της VPN gateway, δηλαδή στην ουσία ο χρήστης μπορεί να την χρησιμοποιεί για την προστασία της δικής του επικοινωνίας, ανεξάρτητα από τη θέση δικτύου με την οποία επικοινωνεί[19] [1].

[19] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.p. 2-7 – 2-8

2.4.3 Gateway-to-Gateway



Σχήμα 2.4: Η αρχιτεκτονική gateway-to-gateway [90]

Η συχνότερη χρήση του IPsec VPN είναι για την παροχή ασφαλών επικοινωνιών μεταξύ δύο χωριστών IP δικτύων (π.χ επικοινωνία ανάμεσα στο δίκτυο μιας Ταξιαρχίας με το δίκτυο μιας άλλης Ταξιαρχίας). Η συνηθέστερη τακτική εδώ είναι η ανάπτυξη μιας VPN gateway σε κάθε δίκτυο και τη δημιουργία ενός IPsec VPN που συνδέει τις δύο gateways. Σε αυτή την αρχιτεκτονική, η ευαίσθητη πληροφορία που χρειάζεται να προστατευτεί κατά την κίνησή της στο δίκτυο μεταξύ των δύο δικτύων περνά μέσα από την σύνδεση VPN μεταξύ των δύο VPN gateways. Η IPsec VPN Gateway μπορεί να είναι μια dedicated συσκευή που εκτελεί μόνο λειτουργίες VPN (όπως οι IP Encryptors σε στρατιωτικά δίκτυα, που θα εξεταστούν στο κεφάλαιο 2) ή μπορεί να αποτελεί λειτουργία μίας άλλης συσκευής που χρησιμοποιείται στο δίκτυο, όπως ένα router ή ένα firewall. Όσο μεγαλύτερη και ποιοτικότερη η προστασία που προσφέρουν αυτές οι συσκευές, τόσο μεγαλύτερα τα κόστη προμήθειας και συντήρησής τους.

Για την εκκίνηση του ασφαλούς καναλιού, μία από τις VPN gateways στέλνει αίτημα για τη δημιουργία σύνδεσης IPsec στην άλλη. Οι δύο VPN gateways ανταλλάσσουν τις απαραίτητες πληροφορίες μεταξύ τους για τη δημιουργία της ασφαλούς σύνδεσης και δημιουργούν μια IPsec σύνδεση. Όταν ένας user σε ένα δίκτυο πρέπει να επικοινωνήσει με έναν user στο άλλο δίκτυο, η IP κίνηση μεταξύ των δικτύων δρομολογείται αυτόματα μέσω του IPsec VPN. Όπως εύκολα γίνεται αντιληπτό, η αρχιτεκτονική αυτή παρέχει προστασία

μόνο στην κίνηση μεταξύ των δύο gateways, και όχι μέχρι τον τελικό χρήστη, σε αντίθεση με τα άλλα δύο μοντέλα VPN που περιγράφηκαν παραπάνω.

Γενικά, η αρχιτεκτονική IPsec VPN gateway-to-gateway είναι η πιο εύκολα εφαρμόσιμη όσον αφορά τη διαχείριση του VPN από τους users, καθώς δεν απαιτεί την αναδιάρθρωση των υπολογιστών των users και servers στο δίκτυο, ούτε την ύπαρξη ειδικού λογισμικού και ξεχωριστών ελέγχων ταυτότητας των χρηστών για τη χρήση του VPN. Έτσι, οι users επικοινωνούν κανονικά με το άλλο δίκτυο, χωρίς να καταλαβαίνουν ουσιαστικά κάποια αλλαγή στη συμπεριφορά του δικτύου[20] [1].

[20] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.p. 2-5 – 2-6

ΚΕΦΑΛΑΙΟ 3

ΠΡΩΤΟΚΟΛΛΑ IPSEC ΓΙΑ ΔΗΜΙΟΥΡΓΙΑ ΑΣΦΑΛΟΥΣ ΣΥΝΔΕΣΗΣ

Το IPsec χρησιμοποιεί δύο πρωτόκολλα για την δημιουργία ασφαλούς σύνδεσης, το Authentication Header (AH) και το Encapsulating Security Payload (ESP).

3.1 Authentication Header (AH)

Το AH αποτελεί ένα από τα πρωτόκολλα δημιουργίας ασφαλούς σύνδεσης IPsec. Χρησιμοποιείται για την παροχή ακεραιότητας και ελέγχου ταυτότητας προέλευσης των δεδομένων των IP datagrams και για την προαιρετική προστασία έναντι των replay attacks. Παρόλα αυτά, δεν μπορεί να παρέχει εμπιστευτικότητα των δεδομένων, καθώς δεν έχει τη δυνατότητα κρυπτογράφησης. Αρχικά, το πρωτόκολλο ESP (το οποίο θα εξεταστεί παρακάτω) είχε τη δυνατότητα παροχής μόνο κρυπτογράφησης και όχι ελέγχου ταυτότητας, οπότε τα AH και ESP χρησιμοποιούνταν κατά κόρον σε συνδυασμό για να μπορούν να παρέχουν εμπιστευτικότητα και προστασία ακεραιότητας των δεδομένων στις επικοινωνίες IP. Στη δεύτερη έκδοση του IPsec προστέθηκαν δυνατότητες ελέγχου ταυτότητας στο ESP, γεγονός που καθιστά το AH λιγότερο σημαντικό. Στην πραγματικότητα, κανένα πλέον λογισμικό IPsec δεν υποστηρίζει πλέον AH. Ωστόσο, το AH εξακολουθεί να έχει

αξία, επειδή το AH μπορεί να πιστοποιήσει την αυθεντικότητα σε τμήματα πακέτων που δεν μπορεί το ESP[21] [1].

3.1.1 Τρόποι λειτουργίας του Authentication Header

Το AH λειτουργεί με δύο τρόπους: το transport mode και το tunnel mode. Στο transport mode, το AH δεν δημιουργεί νέα κεφαλίδα IP, ενώ στο tunnel mode δημιουργείται μια νέα IP header για κάθε πακέτο. Σε αρχιτεκτονικές IPsec με gateways, η πραγματική διεύθυνση IP προέλευσης ή προορισμού για πακέτα πρέπει να αλλάξει ώστε να είναι η διεύθυνση IP της gateway. Επομένως, γίνεται αντιληπτό ότι το transport mode χρησιμοποιείται γενικά σε αρχιτεκτονικές host-to-host ακριβώς επειδή το transport mode δεν μπορεί να αλλάξει την αρχική κεφαλίδα IP ή να δημιουργήσει μια νέα κεφαλίδα IP. Γενικά, το AH μπορεί παρέχει προστασία ακεραιότητας για ολόκληρο το πακέτο, ανεξάρτητα από το ποια από τις δύο λειτουργίες χρησιμοποιείται[22] [1].

3.1.2 Η διαδικασία προστασίας ακεραιότητας

Για την προστασία της ακεραιότητας του πακέτου στο IPsec, χρησιμοποιείται μια μονοσήμαντη συνάρτηση κατακερματισμού (hash function) γνωστή και ως αλγόριθμος MAC (Message Authentication Code), που αποτελεί τύπο ασύμμετρης κρυπτογραφίας. Οι hash functions δημιουργούν έναν κωδικό hash βάσει ενός τμήματος κειμένου (ή κώδικα) ο οποίος είναι ίδιου μήκους ανεξαρτήτως του μήκους του κειμένου και είναι μοναδικός για κάθε αυτόνομο κείμενο. Στην ουσία, η παραμικρή αλλαγή στο κείμενο θα επιφέρει αλλαγή στον κωδικό hash. Υπάρχουν hash functions τα οποία δημιουργούν κωδικούς hash μόνο βάσει του εισερχομένου κειμένου (ή μηνύματος) ή hash functions που για τη δημιουργία των κωδικών hash χρησιμοποιούν και ένα μυστικό κλειδί. Σημαντικό στοιχείο αποτελεί το

---

[21] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-1

[22] p. 3-1

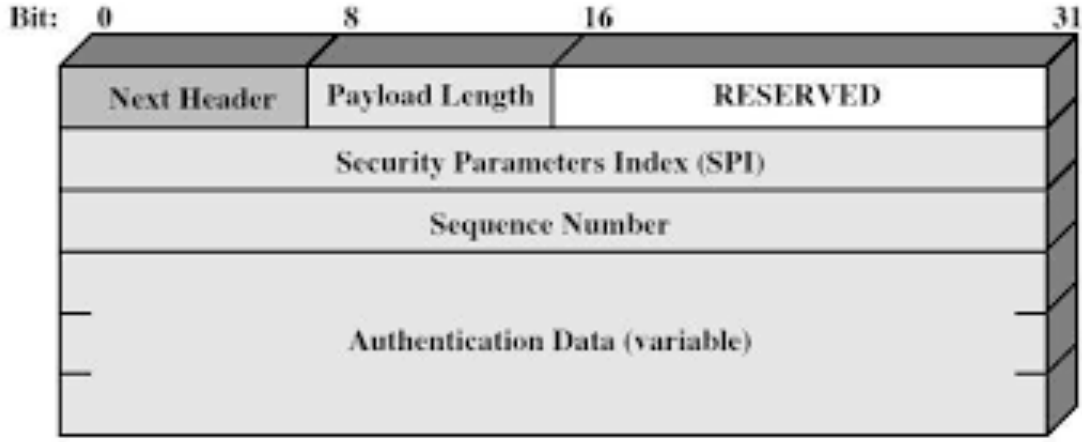
ότι η παραπάνω διαδικασία δεν αντιστρέφεται, δηλαδή αν κάποιος γνωρίζει τον κωδικό και τον αλγόριθμο, δεν μπορεί να αναπαράγει το αυθεντικό κείμενο. Για να μπορεί να πιστοποιηθεί η ακεραιότητα των δεδομένων, τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να γνωρίζουν τη hash function και το κλειδί. Έτσι, στις IPsec επικοινωνίες, για την πιστοποίηση της ακεραιότητας, μία hash function δημιουργεί ένα hash κωδικό βάσει του πακέτου που αποστέλλεται και ενός μυστικού κλειδιού (private key) το οποίο γνωρίζει μόνο ο αποστολέας. Ο hash κωδικός που δημιουργείται προστίθεται στο πακέτο και αποστέλλεται στον παραλήπτη. Ο παραλήπτης στη συνέχεια αναδημιουργεί τον hash κωδικό βάσει του πακέτου που έλαβε χρησιμοποιώντας την hash function η οποία είναι κοινή και για τα δύο μέρη καθώς και το public key του αποστολέα (διαφορετικά κλειδιά – ασσύμετρη κρυπτογραφία). Έπειτα συγκρίνει τον νέο κωδικό με τον κωδικό που απέστειλε με το πακέτο ο αποστολέας. Αν οι δύο κωδικοί ταιριάζουν, πιστοποιείται η ακεραιότητα του πακέτου. Παραδείγματα hash functions είναι οι HMAC-MD5 και HMAC-SHA-1.19 Ένας άλλος κοινός αλγόριθμος MAC είναι ο AES Cipher Block Chaining MAC (AES-XCBC-MAC-96).

Παρόλα αυτά, δεν είναι δυνατή η προστασία της ακεραιότητας ολόκληρης της IP header, καθώς ορισμένα πεδία της, όπως το time-to-live (TTL) και το IP checksum, είναι δυναμικά και ενδέχεται να αλλάξουν κατά τη διάρκεια της επικοινωνίας. Εάν ο κωδικός hash υπολογίζεται για όλη την IP header και ορισμένες από τις τιμές κάποιων πεδίων της αλλάζουν νόμιμα κατά τη μεταφορά του πακέτου, ο κωδικός hash που θα προκύψει στον παραλήπτη θα είναι διαφορετικός. Έτσι, ο παραλήπτης θα καταλήξει στο συμπέρασμα ότι το πακέτο έχει τροποποιηθεί κατά την κίνησή του και ότι η ακεραιότητά του έχει παραβιαστεί. Για να αποφευχθεί αυτό, τα πεδία της IP header που μπορούν να αλλάξουν κατά τη κίνησή τους νόμιμα αλλά και απρόβλεπτα εξαιρούνται από τον υπολογισμό του hash κωδικού για την προστασία ακεραιότητας.

Για τον παραπάνω λόγο το AH είναι συχνά ασυμβίβαστο με το Network Address Translation (NAT), καθώς στο AH τα πεδία IP source και IP destination περιλαμβάνονται στον υπολογισμό κωδικού hash προστασίας ακεραιότητας. Εάν αυτά τα πεδία τροποποιηθούν

από το NAT (π.χ. αλλαγή της IP source από private σε public), ο κωδικός hash που θα αναπαράγεται από τον προορισμό δεν θα ταιριάζει με αυτόν που στάλθηκε αρχικά[23] [1].

3.1.3 Η κεφαλίδα AH



Σχήμα 3.1: Η κεφαλίδα AH [91]

Το AH προσθέτει μια δική του κεφαλίδα σε κάθε πακέτο. Κάθε κεφαλίδα AH αποτελείται από έξι πεδία:

Επόμενη κεφαλίδα (Next Header): Καταδεικνύει τον τύπο του επόμενου payload για το πακέτο με τη χρήση ενός πρωτοκόλλου IP. Στη λειτουργία tunnel, το payload είναι ένα IP packet, οπότε η τιμή Next Header ορίζεται σε 4 για το IP-in-IP. Στη λειτουργία transport, το payload είναι συνήθως επιπέδου transport, TCP (αριθμός πρωτοκόλλου 6) ή UDP (αριθμός πρωτοκόλλου 17).

Μήκος payload (Payload Length): Δείχνει πόσο είναι το μήκος του επερχόμενου payload.

Reserved: Πεδίο μελλοντικής χρήσης, συνήθως 0.

---

[23] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-2

Δείκτης παραμέτρων ασφαλείας (Security Parameters Index - SPI): Τα endpoints μιας IPsec σύνδεσης έχουν μια αυθαίρετα επιλεγμένη τιμή SPI, η οποία λειτουργεί ως μοναδικό αναγνωριστικό για τη σύνδεση. Ο παραλήπτης χρησιμοποιεί την τιμή SPI, μαζί με τη διεύθυνση IP προορισμού και (προαιρετικά) τον τύπο πρωτοκόλλου IPsec (σε αυτήν την περίπτωση, το AH), για τον καθορισμό της Security Association (SA) η οποία δείχνει στον παραλήπτη ποια πρωτόκολλα και ποιοι αλγόριθμοι IPsec έχουν εφαρμοστεί στο εισερχόμενο πακέτο.

Αριθμός ακολουθίας (Sequence Number): Σε κάθε πακέτο εκχωρείται ένας αριθμός ακολουθίας, ο οποίος καταδεικνύει έναν αριθμό «σειράς» για το πακέτο. Για να γίνει δεκτό το πακέτο από τον παραλήπτη, πρέπει ο αριθμός αυτός να ανήκει σε ένα πεδίο τιμών το οποίο γίνεται γνωστό από το πρώτο πακέτο της ακολουθίας και να μην έχει εμφανιστεί νωρίτερα κάποιο πακέτο με τον ίδιο αριθμό ακολουθίας. Αυτό παρέχει προστασία από replay attacks, επειδή τα διπλότυπα πακέτα θα χρησιμοποιούν τον ίδιο αριθμό ακολουθίας. Επίσης, βοηθά στην αποτροπή των Denial-of-Service (DoS) attacks, επειδή παλιά πακέτα που μπορεί να αναπαράγονται για το σκοπό αυτό θα έχουν αριθμούς ακολουθίας εκτός του πεδίου τιμών και θα απορριφθούν αμέσως χωρίς περαιτέρω επεξεργασία.

Πληροφορίες ελέγχου ταυτότητας (Authentication Data): Αυτό το πεδίο περιέχει τον MAC κώδικα που περιγράφεται παραπάνω στη διαδικασία προστασίας ακεραιότητας. Ο παραλήπτης του πακέτου μπορεί να υπολογίσει εκ νέου τον κώδικα MAC για να επιβεβαιώσει ότι το πακέτο δεν έχει τροποποιηθεί κατά την κίνησή του στο δίκτυο[24] [1].

3.2 Encapsulating Security Payload (ESP)

Το ESP είναι το δεύτερο πρωτόκολλο ασφαλείας της σουίτας IPsec. Αρχικά, το ESP παρείχε μόνο κρυπτογράφηση για τα δεδομένα πακέτων, και η προστασία ακεραιότητας των δεδομένων, εάν ήταν απαραίτητη, μπορούσε να διατεθεί από το πρωτόκολλο AH.

---

[24] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-2 – 3-3

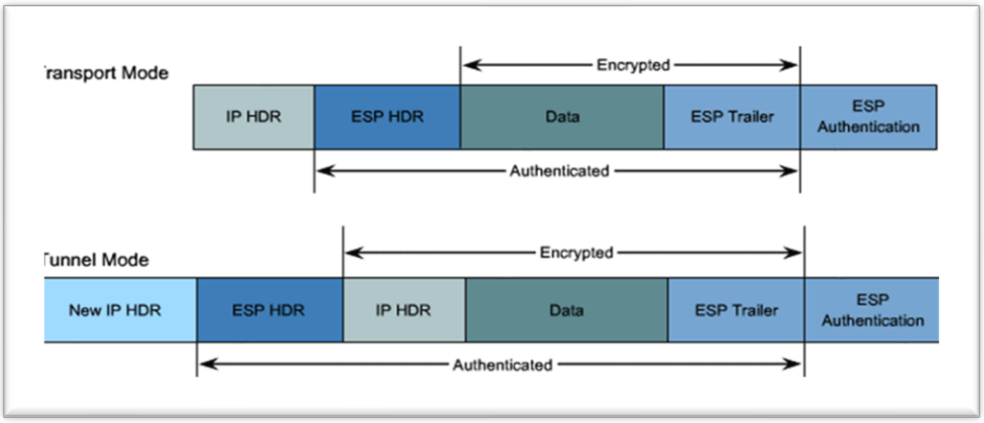
Στη δεύτερη έκδοση του IPsec, το ESP έχει τη δυνατότητα προστασίας ακεραιότητας των πακέτων, αλλά όχι για την εξωτερική κεφαλίδα IP (είτε του transport είτε του tunnel mode). Επίσης, υπάρχει η δυνατότητα μη κρυπτογράφησης των πακέτων αν επιλεγεί για την κρυπτογράφηση αντί για κάποιον αλγόριθμο κρυπτογράφησης ο Null ESP Encryption Algorithm.

3.2.1 Λειτουργίες ESP

Όπως και το AH, το ESP τους ίδιους δύο τρόπους λειτουργίας (modes): transport και tunnel. Και στο ESP, στο tunnel mode, το ESP δημιουργεί μια νέα IP header για κάθε πακέτο. Η νέα IP header καταδεικνύει τα endpoints της ESP tunnel (π.χ οι δύο IPsec gateways ανάμεσα στις οποίες σχηματίζεται το ESP tunnel) ως την πηγή και τον προορισμό του πακέτου. Έτσι, το tunnel mode μπορεί να χρησιμοποιηθεί και με τα τρία μοντέλα αρχιτεκτονικής VPN που περιγράφηκαν στην ενότητα 1.4. Το tunnel mode μπορεί να κρυπτογραφήσει και / ή να προστατεύσει την ακεραιότητα τόσο των δεδομένων όσο και της αρχικής IP header για κάθε πακέτο. Η κρυπτογράφηση των δεδομένων παρέχει εμπιστευτικότητα στα δεδομένα, καθώς τα προστατεύει από την μη εξουσιοδοτημένη πρόσβαση ή την τροποποίηση τους. Η κρυπτογράφηση της αρχικής IP header αποκρύπτει την ταυτότητα της πραγματική πηγής και προορισμού του πακέτου. Εάν ο έλεγχος ταυτότητας χρησιμοποιείται και για την προστασία της ακεραιότητας, κάθε πακέτο θα έχει μια ενότητα ESP Authentication Section μετά το ESP trailer, όπως θα δούμε παρακάτω.

Στο transport mode, το ESP χρησιμοποιεί την αρχική κεφαλίδα IP αντί να δημιουργεί μια νέα. Από το Σχήμα 3.2 φαίνεται ότι στο transport mode, το ESP έχει τη δυνατότητα μόνο κρυπτογράφησης και προστασίας ακεραιότητας του ESP payload, αλλά όχι της IP header. Όπως με το AH, το transport mode στο ESP χρησιμοποιείται γενικά μόνο σε αρχιτεκτονικές host-to-host. Επίσης, το transport mode δεν είναι συμβατό με το NAT. Παρόλα αυτά, δεν αντιμετωπίζονται προβλήματα με το NAT στο tunnel mode, καθώς ολόκληρο το πακέτο TCP είναι κρυμμένο και το NAT δεν θα προσπαθήσει να υπολογίσει

ξανά το TCP checksum. Ωστόσο, άλλα πιθανά προβλήματα συμβατότητας με το NAT και το tunnel mode του ESP είναι ενδεχόμενα[25] [1].



Σχήμα 3.2: ESP transport και tunnel mode [92]

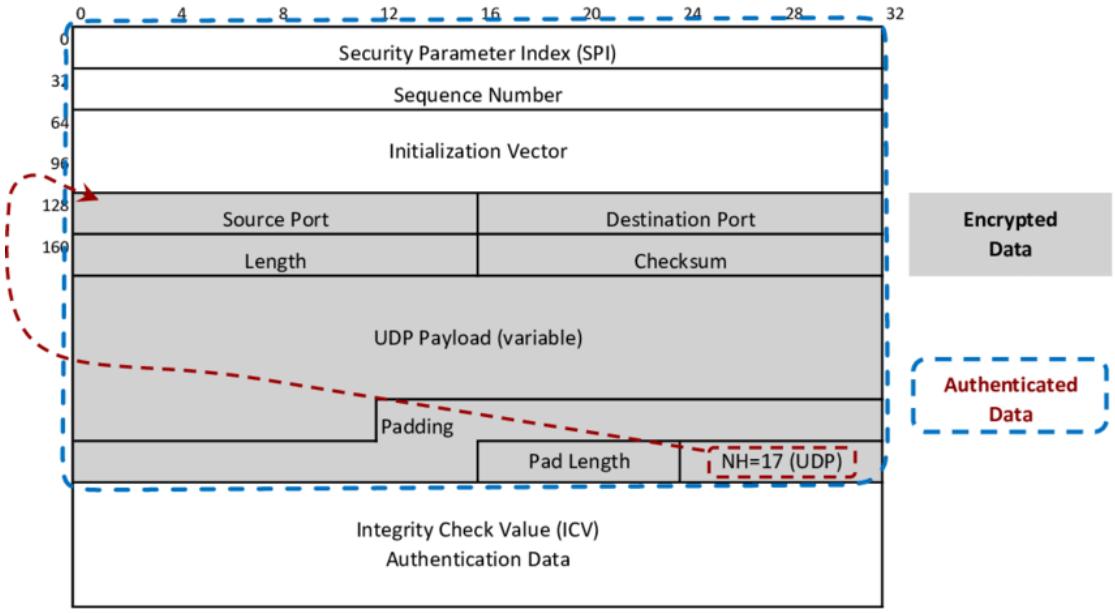
3.2.2 Η διαδικασία κρυπτογράφησης

Το ESP χρησιμοποιεί συμμετρική κρυπτογραφία για να παρέχει κρυπτογράφηση για πακέτα IPsec. Συνεπώς, δύο endpoints μιας IPsec σύνδεσης που προστατεύονται από ESP κρυπτογράφηση πρέπει να χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των πακέτων. Όταν ένα endpoint κρυπτογραφεί δεδομένα, διαιρεί τα δεδομένα σε μικρά μπλοκ (για τον αλγόριθμο AES, 128 ή 256 bits το καθένα) και, στη συνέχεια, εκτελεί πολλαπλά σύνολα κρυπτογραφικών λειτουργιών (γνωστά ως rounds) χρησιμοποιώντας τα μπλοκ δεδομένων και το κλειδί. Οι αλγόριθμοι κρυπτογράφησης που λειτουργούν με αυτόν τον τρόπο είναι γνωστοί ως block cipher algorithms. Όταν το άλλο endpoint λαμβάνει τα κρυπτογραφημένα δεδομένα, εκτελεί αποκρυπτογράφηση χρησιμοποιώντας το ίδιο κλειδί και μια παρόμοια ανεστραμμένη διαδικασία αποκρυπτογράφησης. Παραδείγματα αλγορίθμων κρυπτογράφησης που χρησιμοποιούνται

[25] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.p. 3-5 – 3-6

από το ESP είναι AES-Cipher Block Chaining (AES-CBC), AES Counter Mode (AES-CTR) και Triple DES (3DES)[26] [1].

3.2.3 Το ESP Packet



Σχήμα 3.3: Το ESP packet [93]

Όπως φαίνεται και στο παραπάνω σχήμα, το ESP προσθέτει δύο πεδία στο payload του IP πακέτου, ένα header και ένα trailer. κεφαλίδα και ένα τρέιλερ γύρω από το ωφέλιμο φορτίο κάθε πακέτου.

Κάθε ESP header αποτελείται από δύο πεδία, το **Security Parameter Index (SPI)** και το **Sequence Number**, τα οποία έχουν ακριβώς τις ίδιες ιδιότητες με αυτές του AH. Αμέσως μετά το header ακολουθεί το IP payload, το οποίο είναι κρυπτογραφημένο, και τον φορέα αρχικοποίησης (Initialization Vector), ο οποίος δεν είναι κρυπτογραφημένος. Το IV χρησιμοποιείται κατά την κρυπτογράφηση. Η τιμή του είναι διαφορετική σε κάθε πακέτο,

---

[26] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.p. 3-6

οπότε αν δύο πακέτα έχουν το ίδιο περιεχόμενο, η συμπερίληψη του IV θα έχει ως αποτέλεσμα η κρυπτογράφηση των δύο πακέτων να έχει διαφορετικά αποτελέσματα. Αυτό καθιστά το ESP λιγότερο ευαίσθητο στην κρυπτοανάλυση, σύμφωνα με τους S. Frankel, K. Kent, R. Lewkowski, A.D. Orebaugh, R.W. Ritchey και S.R. Sharma.

Το τρίτο μέρος του πακέτου είναι το ESP trailer, το οποίο εμπεριέχει τα εξής πεδία:

Padding: Ένα πακέτο ESP μπορεί προαιρετικά να περιέχει padding. Το πεδίο padding εμπεριέχει κάποια πρόσθετα byte δεδομένων που κάνουν το πακέτο μεγαλύτερο και απορρίπτονται από τον παραλήπτη του πακέτου. Επειδή το ESP χρησιμοποιεί block ciphers για κρυπτογράφηση, το πακέτο μπορεί να χρειαστεί πλήρωση (padding) με δεδομένα έτσι ώστε τα κρυπτογραφημένα δεδομένα να αποτελούν ακέραιο πολλαπλάσιο του μεγέθους του μπλοκ που χρησιμοποιείται. Μπορεί επίσης να χρειαστεί πλήρωση με δεδομένα για να διασφαλιστεί ότι το ESP trailer τελειώνει σε πολλαπλάσια των 4 byte. Επιπρόσθετο padding μπορεί επίσης να χρησιμοποιηθεί για να αλλάξει το μέγεθος κάθε πακέτου, αποκρύπτοντας τον πραγματικό αριθμό των bytes των πραγματικών δεδομένων που το πακέτο περιέχει. Αυτό είναι χρήσιμο στην αποτροπή της ανάλυσης της κυκλοφορίας.

Μήκος padding (Padding Length): Υποχρεωτικό πεδίο. Αριθμός που υποδεικνύει πόσα bytes είναι το padding σε μέγεθος.

Next header: Λειτουργεί όπως και στο AH. Στο tunnel mode, το payload είναι ένα IP packet, οπότε η τιμή Next Header ορίζεται σε 4 (IP-in-IP). Στο transport mode, το payload είναι συνήθως ένα πρωτόκολλο επιπέδου transport, συχνά TCP (αριθμός πρωτοκόλλου 6) ή UDP (αριθμός πρωτοκόλλου 17). Κάθε ESP trailer περιέχει ένα πεδίο Next Header.

Integrity Check Value (ICV): Εάν είναι ενεργοποιημένη η προστασία ακεραιότητας ESP, το ESP ακολουθείται από ένα πεδίο ICV το οποίο περιέχει ένα MAC κωδικό, ο οποίος λειτουργεί όπως και στο AH. Όμως, υπάρχει μια ουσιαστική διαφορά. Το MAC στο

ESP δεν περιλαμβάνει την εξωτερική IP header στους υπολογιστμούς του. Ο παραλήπτης μπορεί ως εκ τούτου να υπολογίσει εκ νέου το MAC για να επιβεβαιώσει την ακεραιότητα του πακέτου, πλην της εξωτερικής IP header[27] [1].

[27] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-7

ΚΕΦΑΛΑΙΟ 4

ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΑΝΤΑΛΛΑΓΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΚΛΕΙΔΙΩΝ – ΤΟ ΠΡΩΤΟΚΟΛΛΟ IKE

Το πρωτόκολλο Internet Key Exchange - IKE αποτελεί πρωτόκολλο της σουίτας IPsec που χρησιμοποιείται για τη διαπραγμάτευση, δημιουργία και διαχείριση των συσχετισμών ασφαλείας (Security Association) που αναφέρθηκαν παραπάνω. Το NIST ορίζει το συσχετισμό ασφαλείας (SA) ως ένα γενικό όρο που εμπεριέχει ένα σύνολο τιμών που καθορίζουν τις δυνατότητες και τους τύπους προστασίας του IPsec που εφαρμόζονται σε μια IPsec σύνδεση. Υπάρχει επίσης η δυνατότητα δημιουργίας SA χειροκίνητα, δηλαδή χρήση συμφωνημένων εκ των προτέρων και προκαθορισμένων τιμών για την SA από τα δύο μέρη της σύνδεσης, χωρίς τη δυνατότητα αλλαγής ή ενημέρωσής τους. Για τη δημιουργία συσχετισμών ασφαλείας, την αποσαφήνιση της κατάστασης/σφαλμάτων και τον ορισμό ομάδων Diffie-Hellman, το IKE υλοποιεί πέντε διαφορετικούς τύπους διαπραγμάτευσης και ανταλλαγής δεδομένων:

- Ανταλλαγή Πρώτης Φάσης (Phase One Exchange)
    a. Κύρια λειτουργία (Main Mode)
    b. Επιθετική Λειτουργία (Aggressive Mode)
- Ανταλλαγή Δεύτερης Φάσης (Phase Two Exchange)
- Ανταλλαγή Πληροφοριών (Informational Exchange)
- Ανταλλαγή Ομάδων Diffie-Helman (Group Exchange)

Γενικά, στο IPsec, το IKE χρησιμοποιείται για την παροχή ενός ασφαλούς μηχανισμού για τη δημιουργία συνδέσεων με προστασία IPsec [1].

4.1 Ανταλλαγή πρώτης φάσης (Phase 1 Exchange)

Σε αυτή τη φάση, ο σκοπός του IKE είναι η επιτυχής διαπραγμάτευση ενός ασφαλούς καναλιού μεταξύ των δύο IPsec endpoints, το οποίο θα χρησιμοποιηθεί από τα δύο μέρη στην επόμενη φάση για την ασφαλή διαπραγμάτευση μιας IPsec SA. Το ασφαλές κανάλι που δημιουργείται κατά τη διάρκεια αυτής της πρώτης φάσης είναι κοινώς γνωστό ως Internet Security Exchange Security Association (IKE SA). Ο σκοπός της IKE SA είναι να παρέχει αμφίδρομη κρυπτογράφηση και έλεγχο ταυτότητας για τους άλλους τύπους ανταλλαγών του IKE: τις διαπραγματεύσεις που περιλαμβάνει η δεύτερη φάση, τη μεταφορά πληροφοριών κατάστασης και σφαλμάτων και τη δημιουργία πρόσθετων ομάδων Diffie-Hellman. Η ολοκλήρωση της ανταλλαγής πρώτης φάσης του IKE είναι υποχρεωτική πριν την υλοποίηση των άλλων τύπων ανταλλαγών IKE. Ένα IKE SA μπορεί να δημιουργηθεί μέσω ενός από τους δύο τρόπους: main mode και aggressive mode[28] [1].

4.1.1 Κύρια λειτουργία (Main mode)

Με το main mode γίνεται η διαπραγμάτευση της IKE SA που θα εγκαθιδρυθεί μεταξύ των δύο endpoints, μέσω τριών ζευγαριών μηνυμάτων, που χρησιμοποιούν την port 400 ή 4500[29] [8].

Στο πρώτο ζεύγος μηνυμάτων, κάθε endpoint προτείνει παραμέτρους που θα χρησιμοποιηθούν για το SA. Το endpoint που εκκινεί τη σύνδεση μπορεί να προτείνει διάφορες

---

[28] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.p. 3-10

[29] Barker, E., Dang, Q., Frankel, S., Scarfone, K., Wouters, Paul (2020). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77 (1st Revision)

τιμές για διάφορες παραμέτρους και να επιτρέψει στο άλλο endpoint να επιλέξει από αυτές τις τιμές. Τέσσερις από τις παραμέτρους αυτές πρέπει υποχρεωτικά να περιλαμβάνονται στη διαπραγμάτευση (σύμφωνα με το NIST, αυτές αναφέρονται συλλογικά ως *protection suite*):

1. **Αλγόριθμος κρυπτογράφησης (Encryption Algorithm):** Η παράμετρος αυτή καθορίζει τον αλγόριθμο που θα χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων. Παραδείγματα αλγορίθμων κρυπτογράφησης είναι DES, 3DES, CAST, RC5, IDEA, Blowfish και AES.
2. **Αλγόριθμος προστασίας ακεραιότητας (Integrity Protection Algorithm):** Αυτό υποδεικνύει ποιος αλγόριθμος κατακερματισμού (hash function) με χρήση κλειδιού πρέπει να χρησιμοποιηθεί για προστασία ακεραιότητας. Παραδείγματα αλγορίθμων προστασίας ακεραιότητας είναι οι HMAC-MD5 και HMAC-SHA-1.
3. **Μέθοδος αυθεντικότητας (Authentication Method):** Υπάρχουν πολλές μέθοδοι για τον έλεγχο ταυτότητας των δύο endpoints, με δημοφιλέστερους τους κάτωθι:
   - **Προ-διαμοιρασμένο κλειδί (Pre-Shared Key):** Το ίδιο μυστικό κλειδί έχει προκαταβολικά διαμοιραστεί σε κάθε endpoint. Με αυτό το κλειδί, τα endpoints δημιουργούν μια τιμή που χρησιμοποιείται στη διαπραγμάτευσή τους για τη δημιουργία των μυστικών κλειδιών της προστασίας του ασφαλούς καναλιού της Phase 1, αλλά και για την τελική IPsec SA. Προκειμένου η διαπραγμάτευση να είναι επιτυχής, η προκαθορισμένη τιμή πρέπει να είναι ίδια και για τα δύο endpoints. Εφόσον η IKE Phase 1 διαπραγμάτευση μεταξύ των endpoints ολοκληρωθεί, αυτό αποδεικνύει ότι οι συμμετέχοντες στην επικείμενη IPsec σύνδεση κατέχουν το ίδιο μυστικό κλειδί, γεγονός που επαληθεύει την κατοχή του προκαθορισμένου κλειδιού από τα συμβαλλόμενα μέρη.
   - **Ψηφιακές υπογραφές (Digital Signatures):** Αποτελούν ψηφιακά πιστοποιητικά που κατέχουν τα endpoints και εμπεριέχουν ένα δημόσιο κλειδί. Το endpoint που εκκινεί τη σύνδεση χρησιμοποιεί το αντίστοιχο ιδιωτικό κλειδί για την ψηφιακή υπογραφή των δεδομένων πριν τα στείλει στο παραλαβών endpoint. Το παραλαμβάνων endpoint επαληθεύει την γνησιότητα της υπογραφής χρη-

σιμοποιώντας το δημόσιο κλειδί του εκκινών τη σύνδεση. Οι επιλογές αλγορίθμου ψηφιακής υπογραφής είναι το RSA και το Digital Signature Standard (DSS).

- **Κρυπτογράφηση δημόσιου κλειδιού (Public-key encryption):** Τα endpoints που αποστέλλουν δεδομένα τα κρυπτογραφούν με το δικό τους ιδιωτικό κλειδί και τα παραλαμβάνοντα endpoints τα αποκρυπτογραφούν με τη χρήση του δημοσίου κλειδιού του αποστολέα. Η διαφορά από τη χρήση της ψηφιακής υπογραφής είναι ότι το ζεύγος δημοσίου/ιδιωτικού κλειδιού δεν χρησιμοποιείται για την ψηφιακή υπογραφή των δεδομένων, αλλά για την κρυπτογράφηση – αποκρυπτογράφησή τους. Ο αλγόριθμος που χρησιμοποιείται συνήθως για κρυπτογράφηση δημόσιου κλειδιού είναι ο RSA. Ο έλεγχος ταυτότητας με κρυπτογράφηση δημόσιου κλειδιού βασίζεται συνήθως στην καθιέρωση μιας Public Key Infastructure (PKI) και στην έκδοση ψηφιακών πιστοποιητικών.
- **Έλεγχος ταυτότητας από εξωτερικό διακομιστή:** Ορισμένες υλοποιήσεις του IPsec υποστηρίζουν τη χρήση εξωτερικών servers ελέγχου ταυτότητας όπως ο Kerberos v5. Με αυτή τη μέθοδο, ένας διακομιστής Kerberos διατηρεί όλα τα κλειδιά για όλες τις συσκευές στον domain του. Ο Kerberos μπορεί επίσης να χρησιμοποιηθεί για τον έλεγχο ταυτότητας των κεντρικών υπολογιστών των χρηστών. Ωστόσο, η ταυτότητα των endpoints δεν θα είναι μυστική έως το τρίτο σύνολο μηνυμάτων, σε αντίθεση με τη μέθοδο των προ-εγκατεστημένων κλειδιών ή των ψηφιακών υπογραφών.

4. **Diffie-Hellman Group (DH):** Η παράμετρος αυτή χρησιμοποιείται για την ασφαλή δημιουργία ενός «κοινού μυστικού» για τα endpoints, έτσι ώστε ένας μη επιφανής παρατηρητής της IKE Phase 1 Exchange να μην μπορεί να το αναγνωρίσει. Αυτό το «κοινό μυστικό» στη συνέχεια χρησιμοποιείται για τη δημιουργία μια τιμής που χρησιμοποιείται ως είσοδος στους υπολογισμούς για τα μυστικά κλειδιά της IKE Phase Exchange 1 και 2. Κάθε αριθμός DH Group αντιστοιχεί σε ένα συγκεκριμένο

μήκος κλειδιού και έναν τύπο γεννήτριας κρυπτογράφησης (π.χ MODP ή EC2N)[30] [1].

Group Number	Generator	Modulus or Field Size
1	MODP	768-bit modulus
2	MODP	1024-bit modulus
3	EC2N	155-bit field size
4	EC2N	185-bit field size
5	MODP	1536-bit modulus
14	MODP	2048-bit modulus
15	MODP	3072-bit modulus
16	MODP	4096-bit modulus
17	MODP	6144-bit modulus
18	MODP	8192-bit modulus

Σχήμα 4.1: Diffie-Helman Groups [1]

Στο δεύτερο ζεύγος μηνυμάτων του main mode γίνεται η ανταλλαγή των κλειδιών μέσω του αλγορίθμου Diffie-Helman, χρησιμοποιώντας τις παραμέτρους που συμφωνήθηκαν από τη διαπραγμάτευση στο πρώτο ζεύγος μηνυμάτων. Το μεγαλύτερο μέρος του πακέτου αποτελείται από τα βασικά δεδομένα της ανταλλαγής, καθώς και ένα nonce. Σύμφωνα με το NIST, *το nonce είναι μια μη επαναλαμβανόμενη τιμή που χρησιμοποιείται ως είσοδος σε διάφορους τύπους κρυπτογραφικών υπολογισμών, συμπεριλαμβανομένης της υποστήριξης της ακεραιότητας της διαπραγμάτευσης. Για παράδειγμα, ο κεντρικός υπολογιστής Α στέλνει ένα nonce στον κεντρικό υπολογιστή Β. Ο κεντρικός υπολογιστής Β εκτελεί υπολογισμούς και στέλνει τα αποτελέσματα στον κεντρικό υπολογιστή Α. Ο κεντρικός υπολογιστής Α χρησιμοποιεί στη συνέχεια την αρχική τιμή nonce για την επικύρωση των αποτελεσμάτων από τον κεντρικό υπολογιστή Β. Οι nonces χρησιμοποιούνται επίσης για*

[30] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-10 – 3-11

να εγγυηθούν ότι κάθε ανταλλαγή είναι νέα, αντί για επανάληψη προηγούμενης ανταλλαγής IKE.

Υπάρχει διαφορά στο ακριβές περιεχόμενο του δεύτερου ζεύγους μηνυμάτων, ανάλογα με τη μέθοδο αυθεντικότητας που χρησιμοποιείται. Τα μηνύματα που περιλαμβάνουν στη παράμετρο της μεθόδου προεγκατεστημένο κλειδί ή ψηφιακή υπογραφή έχουν ακριβώς τα ίδια πεδία. Τα μηνύματα που περιλαμβάνουν στην μέθοδο την παράμετρο κρυπτογράφησης δημόσιου κλειδιού κρυπτογραφούν το nonce με το δημόσιο κλειδί του άλλου τελικού σημείου και το ID της μεθόδου ανταλλαγής (το οποίο είναι επίσης κρυπτογραφημένο με το δημόσιο κλειδί). Όταν χρησιμοποιείται η μέθοδος του προεγκατεστημένου κλειδιού ή οι ψηφιακές υπογραφές, τα ID της μεθόδου ανταλλαγής δεν ανταλλάσσονται μέχρι το τρίτο ζεύγος μηνυμάτων, έτσι ώστε τα IDs να προστατευτούν από τα κλειδιά της Diffie-Helman Group ανταλλαγής[31] [1].

Στο τρίτο ζεύγος μηνυμάτων, τα endpoints ελέγχουν την αυθεντικότητα των μηνυμάτων που παρέλαβαν. Το περιεχόμενο των πεδίων των μηνυμάτων εξαρτάται και αυτό από τη διαπραγματευόμενη μέθοδο ελέγχου ταυτότητας. Εάν έχει καθοριστεί η μέθοδος των προκαθορισμένων κλειδιών, γίνεται ανταλλαγή των κωδικών hash. Εάν έχουν καθοριστεί ψηφιακές υπογραφές, χρησιμοποιούνται αυτές. Τα μηνύματα αυτά κρυπτογραφούνται με βάση τις παραμέτρους που ανταλλάσσονται στο δεύτερο ζεύγος μηνυμάτων, ανεξάρτητα από τη μέθοδο που έχει καθοριστεί, (η κρυπτογράφηση αυτή δεν εφαρμόζεται στην IKE header[32] [1].

4.1.2 «Επιθετική» λειτουργία (Aggressive mode)

Σύμφωνα με το NIST, η διαφορά του aggressive mode από το main mode είναι ότι το aggressive mode διαπραγματεύεται την ίδρυση της IKE SA μέσω τριών μηνυμάτων αντί

---

31 Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-14

32 p. 3-14 – 3-15

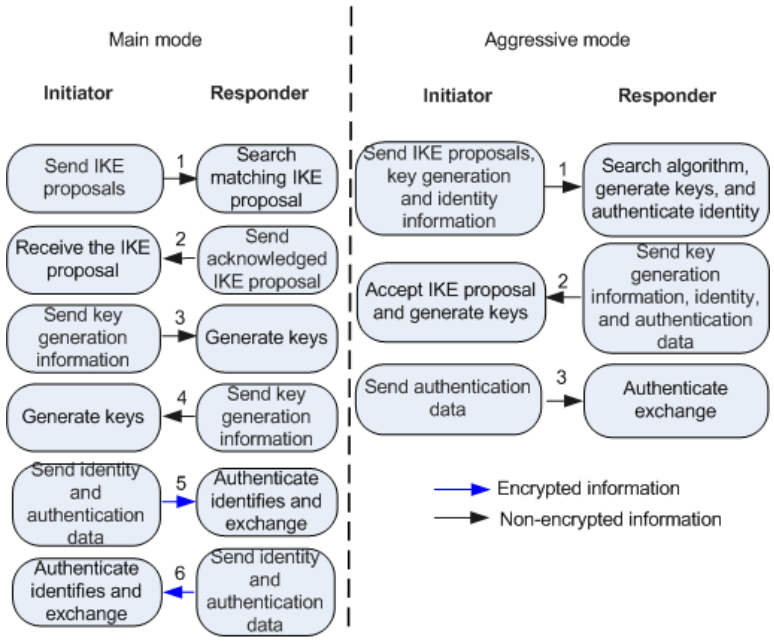
τριών ζευγών μηνυμάτων, γεγονός που καθιστά την εγκαθίδρυση της IKE SA ταχύτερη (3 μηνύματα αντί για 6 συνολικά). Στο πρώτο μήνυμα, το εκκινών τη σύνδεση endpoint (endpoint A) στέλνει όλες τις παραμέτρους της protection suite, καθώς και την δική του παράμετρο για την ανταλλαγή Diffie-Hellman, ένα nonce και την ταυτότητά του. Στο δεύτερο μήνυμα, το άλλο endpoint (endpoint B) στέλνει στο endpoint A τις παραμέτρους της protection suite, την παράμετρο ανταλλαγής Diffie-Hellman, ένα nonce, την ταυτότητά του και το payload της μεθόδου αυθεντικότητας (μέσω ψηφιακής υπογραφής ή κωδικού hash). Στο τρίτο μήνυμα, το endpoint A στέλνει στο B το δικό του payload μεθόδου αυθεντικότητας.

Με την επιθετική λειτουργία γίνεται διαπραγμάτευση των ιδίων παραμέτρων που διαπραγματεύονται με την κύρια λειτουργία, αλλά με τη χρήση λιγότερων μηνυμάτων. Επίσης, η επιθετική λειτουργία μπορεί να χρησιμοποιηθεί με τη χρήση της μεθόδου του προεγκατεστημένου κλειδιού ως ελέγχου αυθεντικότητας για κεντρικούς υπολογιστές χωρίς σταθερές διευθύνσεις IP, εν αντιθέσει με την κύρια λειτουργία.. Παρόλα αυτά, το μειονέκτημα της επιθετικής λειτουργίας είναι η μειωμένη ασφάλεια. Σύμφωνα με το NIST*, εφόσον η ανταλλαγή κλειδιών Diffie-Hellman ξεκινά στο πρώτο πακέτο, τα δύο μέρη δεν έχουν την ευκαιρία να διαπραγματευτούν τις παραμέτρους Diffie-Hellman. Επίσης, οι πληροφορίες της ταυτότητας των endpoints δεν κρύβονται πάντα στην επιθετική κατάσταση, έτσι ένας παρατηρητής θα μπορούσε να καθορίσει ποια μέρη πραγματοποιούσαν τη διαπραγμάτευση. (Η επιθετική λειτουργία μπορεί να αποκρύψει πληροφορίες ταυτότητας σε ορισμένες περιπτώσεις όταν έχουν ήδη ανταλλαχθεί δημόσια κλειδιά.) Οι διαπραγματεύσεις επιθετικής λειτουργίας είναι επίσης επιρρεπείς στο «σπάσιμο» των pre-shared keys, το οποίο μπορεί να επιτρέψει την απομίμηση χρηστών και τις επιθέσεις man-in-the-middle. Ένα άλλο πιθανό πρόβλημα είναι ότι ενώ όλες οι συσκευές IPsec πρέπει να υποστηρίζουν την κύρια λειτουργία, η επιθετική υποστήριξη λειτουργίας είναι προαιρετική.* Για όλους αυτούς τους λόγους, το NIST προτείνει τη χρήση γενικά του main mode για την IKE Phase 1 exchange, εκτός αν υπάρχουν προβλήματα απόδοσης του δικτύου[33] [1].

---

[33] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-15

Το Σχήμα 4.2 δείχνει μια επισκόπηση των IKE main και aggressive mode, καθώς και των διαφορών τους.



Σχήμα 4.2: Επισκόπηση των IKE main/aggressive mode [94]

4.2 Ανταλλαγή δεύτερης φάσης (Phase 2 Exchange)

Σε αυτή τη φάση, ο σκοπός του IKE είναι η δημιουργία της SA για την πραγματική IPsec σύνδεση (IPsec SA), μέσω του ασφαλούς καναλιού που προέκυψε από τη διαπραγμάτευση της Φάσης 1. Οι IPsec SA, αντίθετα με τις IKE SA, είναι μονοκατευθυντικές (σε αντίθεση με τις IKE SA). Αυτό σημαίνει ότι μια σύνδεση IPsec μεταξύ δύο endpoints απαιτεί δύο IPsec SAs. Ένα ζεύγος IPsec SA δημιουργείται μέσω του quick mode. Το quick mode είναι μια λειτουργία που χρησιμοποιεί τρία μηνύματα για τη δημιουργία της IPsec SA, τα οποία κρυπτογραφούνται με την καθορισμένη μέθοδο της Φάσης 1 και σύμφωνα με το NIST, κάνουν τα εξής:

1. Στο πρώτο μήνυμα, το endpoint A στέλνει κλειδιά, nonces και προτάσεις παραμέτρων IPsec SA.
2. Στο δεύτερο μήνυμα, το endpoint B στέλνει κλειδιά, επιλογές παραμέτρων IPsec SA, nonces και ένα κωδικό hash για έλεγχο αυθεντικότητας.

3. Στο τρίτο μήνυμα, το endpoint A στέλνει έναν κωδικό hash για έλεγχο ταυτότητας.

Αφού το endpoint B επικυρώσει το τρίτο μήνυμα, δημιουργείται το ζεύγος των IPsec SAs. Σύμφωνα με το NIST, όλες οι ενεργές SA αποθηκεύονται σε μια βάση δεδομένων σύνδεσης ασφαλείας (Security Association Database - SAD), η οποία περιγράφει τα μέτρα ασφαλείας που πρέπει να χρησιμοποιεί η IPsec για την προστασία των επικοινωνιών και περιλαμβάνει τις πληροφορίες του Πίνακα 4.1 για κάθε προστατευμένη σύνδεση.

IP διεύθυνση πηγής
IP διεύθυνση προορισμού.
Δείκτης παραμέτρων ασφαλείας (SPI)
Πρωτόκολλο δημιουργίας ασφαλούς σύνδεσης (AH/ESP)
Mode λειτουργίας (transport ή tunnel)
Αλγόριθμος κρυπτογράφησης (αν χρησιμοποιείται το ESP, π.χ AES-CBC)
Αλγόριθμος προστασίας ακεραιότητας (π.χ HMAC-SHA-1)
Μυστικά κλειδιά των επιλεγμένων αλγορίθμων και μέγεθος των κλειδιών
Διάρκεια ζωής της SA
Πληροφορίες αριθμών ακολουθίας
Πληροφορίες anti-replay
Τύποι κίνησης στους οποίους θα πρέπει να εφαρμόζεται η SA (π.χ. συγκεκριμένες θύρες ή / και πρωτόκολλα).

Πίνακας 4.1: Περιεχόμενα της βάσης δεδομένων σύνδεσης ασφαλείας (SAD) [1]

Στον παραπάνω πίνακα, με έντονη γραφή είναι οι παράμετροι που προσδιορίζουν μοναδικά κάθε SA. Όταν ένα endpoint πρέπει να γνωρίζει ποια SA ισχύει για ένα συγκεκριμένο πακέτο, το αναζητά στο SAD με βάση αυτές τις παραμέτρους. Ωστόσο, σύμφωνα με το NIST, μια SAD δεν περιγράφει πλήρως τους τύπους κυκλοφορίας που θα πρέπει

να προστατεύονται και υπό ποιες συνθήκες. Πληροφορίες αυτής της φύσεως αποθηκεύονται σε ξεχωριστή βάση δεδομένων, η οποία ονομάζεται βάση δεδομένων πολιτικής ασφαλείας (SPD), η οποία ταξινομεί τα δεδομένα που κινούνται στο δίκτυο ως:

- Δεδομένα απαιτούμενης προστασίας IPsec (protect)
- Δεδομένα μη απαιτούμενης προστασίας IPsec (bypass)
- Δεδομένα στα οποία η πρόσβαση απαγορεύεται (discard).

Το NIST αναφέρει τις πληροφορίες που συνήθως περιέχει το SPD για κάθε τύπο κίνησης δικτύου που απαιτεί προστασία (protect):

- IP διεύθυνση πηγής/προορισμού
- Πρωτόκολλα της σουίτας TCP/IP που χρησιμοποιούνται
- Αριθμός θύρας TCP ή UDP (προαιρετικά)
- Τύποι προστασίας IPsec που πρέπει να εφαρμοστούν
- Δείκτης που καταδεικνύει την αντίστοιχη SA στην βάση SAD, εάν υπάρχει ήδη καταχωρημένη μια SA για έναν συγκεκριμένο τύπο κίνησης δικτύου.

Οι διαμορφώσεις του SPD, σύμφωνα με το NIST, διαμορφώνονται από το χρήστη μέσω ενός Graphical User Interface (GUI), ενώ οι καταχωρήσεις της SAD δημιουργούνται αυτόματα από τις διαπραγματεύσεις του IKE. Σε ορισμένες εφαρμογές, δεν είναι προφανές πώς οι όροι που χρησιμοποιούνται στο εργαλείο διαμόρφωσης ταιριάζουν με τις καταχωρήσεις βάσης δεδομένων SAD και SPD. Οι δύο αυτές βάσεις δεδομένων θα πρέπει να προστατεύονται και μόνο ένας διαχειριστής ή "superuser" πρέπει να είναι σε θέση να διαμορφώσει το SPD.

Τα IPsec και IKE SAs έχουν συγκεκριμένη διάρκεια ζωής, η οποία δεν αλλάζει μετά την εγκαθίδρυσή τους. Αν η διάρκεια ζωής μιας SA τείνει στο να εξαντληθεί, τα endpoints

πρέπει να εγκαθιδρύσουν νέα SA. Συνήθως η διάρκεια ζωής μίας SA καθορίζει και πόσο συχνά αυτές ανανεώνονται, και δεν είναι μεγαλύτερη της μίας ημέρας[34] [1].

4.3 Ανταλλαγή πληροφοριών (Informational Exchange)

Σε αυτή τη φάση παρέχονται ασφαλείς τρόποι ανταλλαγής μηνυμάτων κατάστασης (status) ή σφαλμάτων (errors) μεταξύ των endpoints. Σύμφωνα με το NIST, η IKE SA είναι αυτή που παρέχει προστασία για την κατάσταση και τις πληροφορίες σφάλματος, διασφαλίζοντας τη μη διακοπή διαπραγμάτευσης ή πρόωρο τερματισμό μιας IPsec SA. Για παράδειγμα, ένα τελικό σημείο μπορεί να πει σε ένα άλλο τελικό σημείο ότι ένα συγκεκριμένο SA δεν πρέπει πλέον να χρησιμοποιείται. Όμως, το NIST τονίζει ότι *τα μηνύματα που αποστέλλονται μέσω της ανταλλαγής πληροφοριών βασίζονται στο πρωτόκολλο UDP και ο παραλήπτης δεν τα αναγνωρίζει, επομένως δεν υπάρχει καμία εγγύηση ότι τα άλλα τελικά σημεία θα τα λάβουν*[35] [1].

4.4 Ανταλλαγή Ομάδων Diffie-Helman (Diffie-Helman Group Exchange)

Οι ομάδες Diffie-Helman αναφέρθηκαν στο κεφάλαιο 3.1.1. Οι προκαθορισμένες ομάδες Diffie-Helman φαίνονται στο Σχήμα 4.1 όπου κάθε αριθμός που αντιστοιχεί σε μία ομάδα Diffie-Helman καθορίζει ένα μέγεθος συντελεστή και έναν τύπο γεννήτριας κρυπτογράφησης. Σύμφωνα με το NIST, σε αυτή τη φάση, τα δύο endpoints μπορούν να διαπραγματευτούν τη δημιουργία μιας ή περισσότερων επιπλέον ομάδων Diffie-Helman, αφού συμφωνήσουν στα χαρακτηριστικά της. Αυτές οι ομάδες μπορούν να χρησιμοποι-

---

[34] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-15 – 3-17

[35] p. 3-17

ηθούν σε μελλοντική διαπραγμάτευση Φάσης 1. Συνήθως όμως αυτή η φάση δεν χρησιμοποιείται, καθώς το NIST τονίζει ότι *ο ορισμός μιας νέας ομάδας Diffie-Hellman δεν αποτελεί ασήμαντο θέμα*, ώστε να γίνει εκτός της Φάσης 1[36] [1].

[36] p. 3-17

ΚΕΦΑΛΑΙΟ 5

ΣΕΝΑΡΙΟ ESP ΣΕ ΑΡΧΙΤΕΚΤΟΝΙΚΗ GATEWAY-TO-GATEWAY

Είδαμε στο κεφάλαιο 1.4.2 ότι το IPsec VPN χρησιμοποιείται συχνότερα για την εγκαθίδρυση ασφαλούς IP επικοινωνίας μεταξύ δύο χωριστών εταιρικών δικτύων, όπου η συνηθέστερη αρχιτεκτονική που χρησιμοποιείται είναι η Gateway-to-Gateway. Για την καλύτερη κατανόηση της λειτουργίας του πρωτοκόλλου θα παρουσιαστεί ένα σενάριο υλοποίησης IPsec (IKE/ESP) Gateway-to-Gateway, όπου στόχος είναι η δημιουργία μιας IPsec σύνδεσης που παρέχει υπηρεσίες κρυπτογράφησης και προστασίας ακεραιότητας μεταξύ των endpoints A και B. Το endpoint A χρησιμοποιεί την gateway A στο δίκτυο A και το endpoint B χρησιμοποιεί την gateway B στο δίκτυο B.

5.1 Δημιουργία IKE SA

Το πρώτο βήμα για τη δημιουργία της σύνδεσης είναι η δημιουργία μίας IKE SA (εάν δεν υπάρχει ήδη μια καταχωρημένη στην SAD), ως εξής:

1. Το endpoint A δημιουργεί και αποστέλλει ένα κανονικό (μη χρήση IPsec) πακέτο που έχει IP διεύθυνση προορισμού την διεύθυνση του endpoint B.
2. Το πακέτο φτάνει μέσω του δικτύου A στην gateway A.
3. Η gateway A δέχεται το πακέτο και υλοποιεί το NAT, αλλάζοντας την IP διεύθυνση της πηγής του πακέτου.
4. Η gateway A συγκρίνει τα χαρακτηριστικά του πακέτου με εκείνα της SPD. Εφόσον η SPD έχει καταχωρημένα πακέτα με τα συγκεκριμένα χαρακτηριστικά ως

«protect», η gateway A καθορίζει ότι στο πακέτο θα πρέπει να εφαρμοστεί προστασία κρυπτογράφησης και ακεραιότητας μέσω ESP. Επίσης καθορίζει τη διεύθυνση της gateway του προορισμού του πακέτου (από τον routing table). Υποθέτουμε ότι η αντίστοιχη καταχώρηση στην SPD που συμβουλεύτηκε η gateway δεν έχει δείκτη IKE SA, που καθιστά γνωστό στην gateway ότι δεν υπάρχει προς το παρόν IKE SA για την προστασία αυτής της συγκεκριμένης κίνησης δικτύου.

5. Η gateway A εκκινεί μια διαπραγμάτευση IKE SA με την gateway B χρησιμοποιώντας είτε κύρια είτε επιθετική λειτουργία. Στο τέλος της διαπραγμάτευσης, εγκαθιδρύεται μία IKE SA μεταξύ των gateways A και B[37] [1].

5.2 Δημιουργία IPsec SA

Το επόμενο βήμα για τη δημιουργία της σύνδεσης ESP είναι η δημιουργία IPsec SA, ως εξής:

1. Η gateway A χρησιμοποιεί τις παραμέτρους που ορίζονται στην IKE SA που εγκαθιδρύθηκε μεταξύ των gateways για να εκκινήσει μια διαπραγμάτευση IPsec SA με την πύλη B. Το IKE SA παρέχει προστασία για τη διαπραγμάτευση, η οποία πραγματοποιείται χρησιμοποιώντας το quick mode. Θεωρούμε ότι οι παράμετροι της IKE SA καθορίζουν ότι θα χρησιμοποιηθεί η λειτουργία ESP tunnel και ότι θα παρέχει προστασία κρυπτογράφησης και ακεραιότητας. Στο τέλος της διαπραγμάτευσης, δημιουργείται ένα ζευγάρι από μονόδρομες IPsec SAs για τη σύσταση του ESP tunnel. Κάθε SA παρέχει προστασία μόνο για κίνηση δικτύου που κινείται προς μία μόνο κατεύθυνση.

---

[37] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-20

2. Μόλις δημιουργηθούν οι δύο IPsec SA, η gateway A μπορεί να ολοκληρώσει την επεξεργασία του πακέτου που αποστέλλεται από το endpoint A και η οποία ξεκίνησε στο βήμα 1 της δημιουργίας IKE SA. Το πακέτο θα κρυπτογραφηθεί πρώτα και στη συνέχεια θα υποβληθεί σε επεξεργασία για προστασία ακεραιότητας[38] [1].

5.3 Τελική διευθυνσιοδότηση του πακέτου

Τα ακόλουθα βήματα περιγράφουν πώς τα δεδομένα φτάνουν πραγματικά στον προορισμό τους, μετά την εγκαθίδρυση του ζεύγους των IPsec SAs:

1. Το gateway A, με το πέρας της δημιουργίας του ζεύγους των IPsec SA, τροποποιεί το πακέτο έτσι ώστε να προστατεύεται σύμφωνα με τις παραμέτρους SA. Αυτό περιλαμβάνει:
   - την προσθήκη μιας νέας IP header που χρησιμοποιεί τη διεύθυνση IP της gateway A ως τη διεύθυνση IP προέλευσης και τη διεύθυνση IP της gateway B ως διεύθυνση προορισμού,
   - την κρυπτογράφηση των δεδομένων του πακέτου (payload) και
   - την προσθήκη των πληροφοριών αυθεντικότητας.

   Στη συνέχεια, η gateway A στέλνει το πακέτο στην πύλη B.
2. Η gateway B λαμβάνει το πακέτο και χρησιμοποιεί την τιμή στο μη κρυπτογραφημένο πεδίο SPI από την ESP header για να προσδιορίσει ποια IPsec SA θα πρέπει να εφαρμοστεί στο πακέτο.
3. Μετά την εύρεση της IPsec SA, η gateway B βρίσκει τις παραμέτρους που χρειάζονται για προστασία ακεραιότητας – αποκρυπτογράφηση του πακέτου (μυστικά κλειδιά) και επεξεργάζεται και επικυρώνει το πακέτο. Αυτό περιλαμβάνει:
   - την αφαίρεση της πρόσθετης IP header,
   - τον έλεγχο της ακεραιότητας των κρυπτογραφημένων δεδομένων,

---

[38] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.p. 3-20

- την προαιρετική εκτέλεση ελέγχου διπλότυπων πακέτων (για πιθανότητα re-play attack) και
- την αποκρυπτογράφηση του αρχικού payload του πακέτου.

4. Η gateway B ελέγχει το SPD για να διασφαλίσει ότι εφαρμόστηκαν οι απαιτούμενες προστασίες στο πακέτο, έπειτα εφαρμόζει το NAT για να αλλάξει η NAT IP διεύθυνσης προορισμού στο πακέτο στην πραγματική IP διεύθυνση του δικτύου B και έπειτα στέλνει το πακέτο στον πραγματικό του προορισμό, το endpoint B, μέσω του δικτύου B.

Η διαδικασία αυτή επαναλαμβάνεται αντίστροφα στην περίπτωση που το endpoint B επιθυμεί να απαντήσει στο πακέτο ή να στείλει στο endpoint A ένα άλλο πακέτο. Σε αυτή την περίπτωση, το πακέτο θα έφτανε μέσω του δικτύου B στην gateway B, η οποία θα το τροποποιήσει κατάλληλα (εφόσον υπάρχει ήδη μια ανεξάντλητη IPsec SA, δε χρειάζεται να δημιουργηθεί ξανά) και θα το αποστείλει στην gateway A, η οποία αφού το επεξεργαστεί και το επικυρώσει, θα εφαρμόσει το NAT για να επαναφέρει την αρχική διεύθυνση IP και θα το αποστείλει στο endpoint A, μέσω του δικτύου A.

Αν υποθέσουμε ότι η σύνδεση IPsec μεταξύ των gateways διατηρείται, τελικά η IKE SA ή οι IPsec SAs θα προσεγγίσουν ένα από τα όρια διάρκειας ζωής SA. Η πρώτη gateway που καταλαβαίνει ότι η διάρκεια ζωής μιας SA φτάνει στο τέλος της εκκινεί τη διαδικασία εκ νέου ενεργοποίησης της SA. Αυτό αναγκάζει ορισμένα από τα βήματα που αναφέρθηκαν να εκτελεστούν ξανά, ανάλογα με τον τύπο SAs (IKE ή IPsec) που πρέπει να αναδημιουργηθεί. Μόλις δημιουργηθούν οι νέες SA, οι gateways στέλνουν όλη τη νέα κίνηση μέσω των νέων SA, και τελικά οι παλιές SA διαγράφονται[39] [1].

---

[39] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77. p. 3-20 – 3-21

ΚΕΦΑΛΑΙΟ 6

Η ΣΥΣΚΕΥΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ IP (IP ENCRYPTOR) - ΤΟ ΠΡΩΤΟΚΟΛΛΟ IPSEC ΣΤΙΣ ΕΝΟΠΛΕΣ ΔΥΝΑΜΕΙΣ

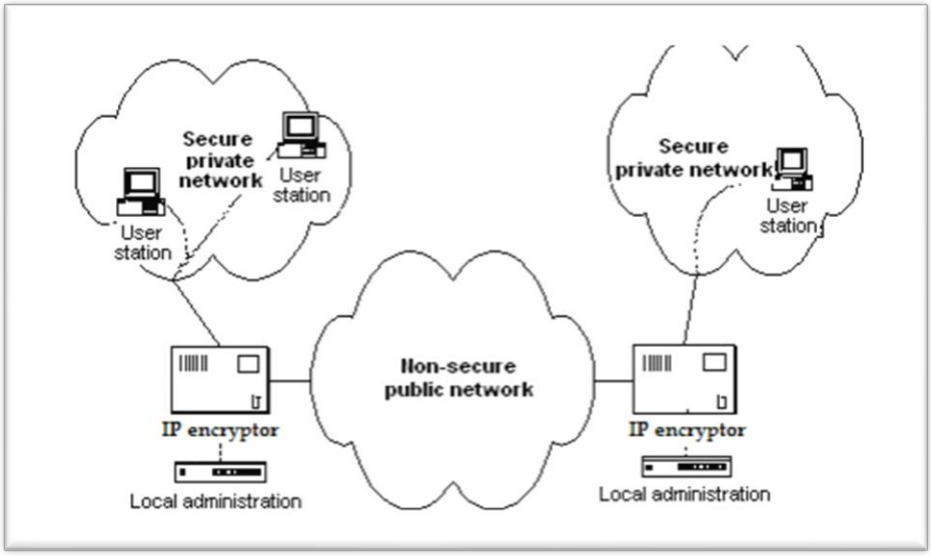
Τα δίκτυα IPv4 τα οποία προορίζονται για χρήση από ένοπλες δυνάμεις έχουν το χαρακτηριστικό ότι συνήθως χρησιμοποιούν υποδομές που χρησιμοποιούνται αποκλειστικά από τις ένοπλες δυνάμεις, και ως εκ τούτου δεν αποτελούν δικτυακές υποδομές στις οποίες έχει πρόσβαση ο απλός πολίτης. Αυτό τα καθιστά ιδιωτικά δίκτυα που χρησιμοποιούνται από έναν και μόνο οργανισμό. Εξ'ορισμού, τα δίκτυα αυτού του είδους αποτελούν τα λεγόμενα ενδοδίκτυα (intranets) [19].

Οι συσκευές κρυπτογράφησης IP (IP Encryptors) αποτελούν ειδικά σχεδιασμένες συσκευές, των οποίων η λειτουργία στηρίζεται στο πρωτόκολλο IPsec, με πρόσθετους περιορισμούς και βελτιώσεις. Οι συσκευές αυτές δημιουργούν ένα IPsec VPN, κρυπτογραφώντας τα δεδομένα που ανταλλάσσονται μεταξύ των υποδικτύων που προστατεύουν. Αποτελούν συνήθως ασφαλείς πύλες (gateways) που επιτρέπουν την ασφαλή ανταλλαγή δεδομένων μεταξύ δύο ιδιωτικών δικτύων μέσω ενός μη αξιόπιστου ή χαμηλότερης διαβάθμισης δικτύου.

Σχήμα 6.1: Ο IP Encryptor KG-255X της Viasat [95]

6.1 Υλοποίηση του IPsec με IP Encryptors

Οι IP Encryptors δημιουργούν IPsec VPNs κρυπτογραφώντας τα δεδομένα που ανταλλάσσονται από τα προστατευόμενα υποδίκτυα. Τα υποδίκτυα συνδέονται μεταξύ τους μέσω δικτύων IP. Η χρήση των IP Encryptors αποτελεί υλοποίηση Bump-In-The-Wire, στην οποία το IPsec εφαρμόζεται σε μια συσκευή (IP Encryptor), σε αντίθεση με την εγγενή εφαρμογή στους δρομολογητές, όπου το IPsec ενσωματώνεται στον εκάστοτε δρομολογητή. Η συσκευή συνδέεται με τη φυσική διεπαφή του δρομολογητή και εξασφαλίζει την κρυπτογράφηση πακέτων IP που προέρχονται από το εξωτερικό δίκτυο. Το παράδειγμα του σχήματος περιέχει δύο συσκευές κρυπτογράφησης IP, ελάχιστο αριθμό που απαιτείται για τη δημιουργία μιας σύνδεσης VPN μεταξύ δύο ιδιωτικών δικτύων. Ο αριθμός των συσκευών κρυπτογράφησης που θα χρησιμοποιηθούν εξαρτάται από τον αριθμό των ιδιωτικών δικτύων τα οποία επικοινωνούν μεταξύ τους μέσω ενός μη-ασφαλούς δημοσίου δικτύου [11].



Σχήμα 6.2: Σχηματική παράσταση VPN διάταξης με τη χρήση κρυπτομηχανής [11]

Στην παραπάνω διάταξη, δημιουργείται ένα IPsec VPN tunnel ανάμεσα στις δύο συσκευές IP Encryptors. Η κρυπτογράφηση εδώ γίνεται στο Layer 3, δηλαδή ενθυλακώνεται ολόκληρο το IP Header (μαζί με τη διεύθυνση IP του source και του destination). Τα πακέτα IP που θα μεταδοθούν από το αξιόπιστο στο μη αξιόπιστο δίκτυο ενθυλακώνονται σε ένα νέο πακέτο IP (IPSec encapsulation). Έτσι, όλες οι επικοινωνίες πραγματοποιούνται σε υψηλότερα πρωτόκολλα (TCP / IP, UDP κ.λπ.) και παρέχεται ασφάλεια στις σχετικές υπηρεσίες (Mail, Telnet, FTP κ.λπ.).

6.2 Αρχιτεκτονική της συσκευής κρυπτογράφησης IP

Οι συσκευές κρυπτογράφησης IP στρατιωτικών προδιαγραφών είναι σχεδιασμένες για να είναι ανθεκτικές σε παραβιάσεις (tamper-proof). Συνήθως είναι διαστάσεων 19” rack-unit. Το περίβλημα (shell) των συσκευών συνήθως είναι μεταλλικής ή πλαστικής κατασκευής. Μπορεί να διαθέτουν κάποια οπτική οθόνη (visual display) τύπου LCD για ενδείξεις παραμέτρων λειτουργίας ή χειρισμού. Ορισμένες από αυτές έχουν τη δυνατότητα ηχητικών μηνυμάτων, για την ένδειξη κάποιας παραμέτρου (π.χ διακοπή κρυπτασφάλισης). Πολλές από αυτές επίσης υποστηρίζουν διαγραφή έκτακτης ανάγκης με μηχανικό

διακόπτη (επίσης προαπαιτούμενο για τη στρατιωτική χρήση). Οι συσκευές αυτές παρέχουν συνήθως **Ethernet interfaces**, με τα δεδομένα IP να μεταφέρονται εντός Ethernet data frames που κυμαίνονται σε μήκος μεταξύ 64 και 1.518 bytes. Κάθε συσκευή κρυπτογράφησης IP παρουσιάζει συνήθως τρεις λογικές και ξεχωριστές εξωτερικές διεπαφές:

-διεπαφή προς το ιδιωτικό δίκτυο (secure network interface)

-διεπαφή προς το δημόσιο δίκτυο (non-secure network interface) και

-διεπαφή διαχείρισης (administration interface)

Σχήμα 6.3: Η συσκευή κρυπτογράφησης SITLine της Rohde&Schwarz [96]

Έτσι, παρέχουν μια πλατφόρμα επικοινωνίας με δύο τομείς ασφαλείας που διαχωρίζονται φυσικά (red και black δίκτυα) που επικοινωνούν μέσω της μονάδας κρυπτογράφησης. Μια συνήθης αρχιτεκτονική των μονάδων κρυπτογράφησης που χρησιμοποιούνται σε ευαίσθητα δίκτυα (όπως των ενόπλων δυνάμεων) διαθέτει συνήθως **3 εσωτερικές**

υπομονάδες: δύο ενσωματωμένους προγραμματιζόμενους δρομολογητές που διαχωρίζονται από έναν ασφαλή πυρήνα κρυπτογράφησης **(secure cryptoprocessor).** Ένας secure cryptoprocessor αποτελεί έναν αποκλειστικός υπολογιστής με τη μορφή ολοκληρωμένου κυκλώματος (chip) ή μικροεπεξεργαστή ο οποίος χρησιμοποιείται για την εκτέλεση κρυπτογραφικών εργασιών, ενσωματωμένος σε μια συσκευή με πολλαπλά μέτρα φυσικής ασφάλειας, τα οποία του παρέχουν έναν βαθμό αντίστασης παραβίασης (όπως ο IP Encryptor). Σε αντίθεση με τους cryptoprocessors που εξάγουν αποκρυπτογραφημένα δεδομένα σε έναν δίαυλο σε ένα ασφαλές περιβάλλον, ένας secure cryptoprocessor δεν εξάγει αποκρυπτογραφημένα δεδομένα ή αποκρυπτογραφημένες οδηγίες προγράμματος σε ένα περιβάλλον όπου η ασφάλεια δεν μπορεί πάντα να διατηρείται.

Για τη λειτουργία του secure cryptoprocessor ενός IP Encryptor συνήθως απαιτείται και η παρουσία ενός κλειδιού έναρξης κρυπτογράφησης (**Crypto Ignition Key - CIK**). Μια συσκευή CIK γενικά αποτελεί τη συσκευή ή το ηλεκτρονικό κλειδί που χρησιμοποιείται για το ξεκλείδωμα της ασφαλούς λειτουργίας μιας συσκευής κρυπτογράφησης και τον έλεγχο της ταυτότητας του χρήστη που τη χρησιμοποιεί [18]. Συνήθως είναι ενσωματωμένη σε μια αφαιρούμενη κασέτα δεδομένων, ειδικά σχεδιασμένη για να είναι συμβατή με την εκάστοτε συσκευή κρυπτογράφησης, η οποία χρησιμοποιείται για τη μεταφορά πληροφοριών για κρυπτογραφική επεξεργασία σε ένα κεντρικό σύστημα κρυπτογράφησης. Όταν η αφαιρούμενη κασέτα δεδομένων είναι διασυνδεδεμένη με τη συσκευή κρυπτογράφησης, η συσκευή CIK επικοινωνεί με μία άλλη συσκευή CIK (εντός του δικτύου που κρυπτογραφείται – συνήθως είναι η CIK του διαχειριστή του intranet) που χρησιμοποιείται για τον έλεγχο ταυτότητας του χρήστη, έτσι ώστε τα δεδομένα που υπόκεινται σε κρυπτογραφική επεξεργασία να μπορούν να μεταφερθούν ή να υποβληθούν σε επεξεργασία από το σύστημα κρυπτογράφησης. Μόλις πραγματοποιηθεί ο έλεγχος ταυτότητας χρήστη, η αφαιρούμενη κασέτα δεδομένων μπορεί να μεταφέρει δεδομένα στον IP Encryptor, όπως οι αλγόριθμοι κρυπτογράφησης [18].

Σχήμα 6.4: Η χρήση του CIK [97]

Οι συσκευές κρυπτογράφησης IP υιοθετούν ένα αυτοσχέδιο λειτουργικό σύστημα ασφαλείας και παρέχουν ολοκληρωμένες λειτουργίες ασφαλείας για την κάλυψη αναγκών προστασίας δεδομένων σε διάφορα περιβάλλοντα δικτύου. Εκτός από την κρυπτογράφηση δεδομένων, μπορεί επίσης να παρέχουν ορισμένες παραδοσιακές λειτουργίες ασφαλείας, όπως φιλτράρισμα πακέτων, DDOS anti-attack, anti-virus, hot standby κ.λπ [15].

6.3 Διαχείριση κλειδιών – Key Management

Μία από τις επιπλέον λειτουργίες που περιλαμβάνει τη δυνατότητα κρυπτογράφησης multicast δεδομένων χρησιμοποιώντας ένα "προεγκατεστημένο κλειδί" (Pre-Placed Key). Αυτό απαιτεί τη φόρτωση του ίδιου κλειδιού σε όλες τις συσκευές IP Encryptor που θα συμμετάσχουν σε μια multicast session πριν από τη μετάδοση των δεδομένων [18]. Για παράδειγμα, σε ένα intranet μίας χώρας το οποίο προορίζεται για στρατιωτική χρήση, θα πρέπει να φορτωθεί το ίδιο κλειδί σε όλους τους IP Encryptors προκειμένου να μπορούν να επικοινωνήσουν μεταξύ τους και να ανταλλάξουν δεδομένα. Για την μεγιστοποίηση της

ασφάλειας, υπάρχουν IP Encryptors που υποστηρίζουν την εισαγωγή κλειδιών από διάτρητες ταινίες ή από ηλεκτρονικές συσκευές μεταφοράς (fill guns). Τα κλειδιά αυτά δημιουργούνται από συσκευές παραγωγής τυχαίων αριθμών.

Στις σύγχρονες συσκευές κρυπτογράφησης IP, υπάρχει συνήθως η δυνατότητα κεντρικής διαχείρισης των κλειδιών και των access-lists μέσω λογισμικών κεντρικής διαχείρισης τα οποία αναπτύσσουν οι εταιρείες παραγωγής των συσκευων. Η επικοινωνία του κεντρικού server διαχείρισης των IP Encryptors γίνεται μέσω προστατευμένων συνδέσεων από το δίκτυο IP. Παρόλα αυτά, ενώ οι κατασκευαστές υποστηρίζουν την κεντρική διαχείριση των συσκευών τους μέσω ιδιόκτητου λογισμικού, σε κάποιες συσκευές, κυρίως για λόγους διαβάθμισης πληροφορίας, δεν προσφέρεται η δυνατότητα διαχείρισης μέσω ανοιχτών πρωτοκόλλων ή προτύπων, και η διαχείριση γίνεται μόνο τοπικά από τον τοπικό υπεύθυνο.

6.4 Τυπικές υπηρεσίες και λειτουργίες ενός IP Encryptor

Το κύριο χαρακτηριστικό μιας συσκευής κρυπτογράφησης IP είναι ότι παρέχει σε ένα δίκτυο πληροφοριών ασφαλείς συνδέσεις επικοινωνίας μεταξύ πολλών ιδιωτικών δικτύων. Οι πολιτικές ασφάλειας VPN καθορίζουν τους κανόνες ασφαλείας που καθορίζουν την επεξεργασία που θα εφαρμοστεί στα δεδομένα τα οποία ανταλάσσονται μεταξύ των IP Encryptors και τα οποία μπορεί να είναι:

• Δεδομένα που προκύπτουν από τις εφαρμογές πληροφοριακών συστημάτων (υπολογιστών) και μεταφέρονται από το δίκτυο (δεδομένα εφαρμογής).

• Δεδομένα που προστίθενται από τους μηχανισμούς δικτύου που επιτρέπουν κυρίως τη δρομολόγηση πακέτων IP (τοπολογικά δεδομένα).

Γενικά, οι IP Encryptors εφαρμόζουν τη λειτουργία του «**σιωπηρού φιλτρατρίσματος**» (implicit filtering). Εάν δηλαδή δεν έχει καθοριστεί πολιτική ασφαλείας VPN σε έναν δεδομένο σύνδεσμο VPN, απορρίπτονται τα εισερχόμενα ή εξερχόμενα πακέτα μέσω του συγκεκριμένου συνδέσμου. Οι υπηρεσίες ασφαλείας VPN που εφαρμόζονται στα δεδομένα σε μια συσκευή κρυπτογράφησης IP γενικά είναι οι παρακάτω [11]:

Προστασία της εμπιστευτικότητας των δεδομένων (data confidentiality)

Η διασφάλιση της εμπιστευτικότητας των δεδομένων εφαρμογής παρέχει τη δυνατότητα αποτροπής της αποκάλυψης αυτών των δεδομένων όταν αυτά ρέουν μέσω ενός μη ασφαλούς δημόσιου δικτύου. Για το σκοπό αυτό, αυτά τα δεδομένα μπορούν να κρυπτογραφηθούν πριν περάσουν από το δημόσιο δίκτυο και να αποκρυπτογραφηθούν κατά την είσοδο του παραλήπτη του ιδιωτικού δικτύου, όπως στο Σχήμα 6.2.

Προστασία της αυθεντικότητας των δεδομένων (data integrity)

Για να διασφαλιστεί η αυθεντικότητα των δεδομένων, είναι απαραίτητο να διασφαλιστεί ταυτόχρονα η ακεραιότητα αυτών των δεδομένων κατά την «κίνησή» τους στο δίκτυο, καθώς και ο έλεγχος ταυτότητας της προέλευσης αυτών (διεύθυνση προορισμού – διεύθυνση αποστολέα). Η διασφάλιση της ακεραιότητας των δεδομένων παρέχει τη δυνατότητα διακρίβωσης ότι τα δεδομένα δεν τροποποιήθηκαν, επιτηδευμένα ή μη, κατά την μετακίνησή τους από έναν IP Encryptor σε έναν άλλο. Η διασφάλιση της αυθεντικότητας των δεδομένων διασφαλίζει ότι η προέλευση των δεδομένων είναι η σωστή. Ο αλγόριθμος για τη δημιουργία γνήσιων πληροφοριών και για την επαλήθευση της γνησιότητας αυτών, καθώς και τα χαρακτηριστικά των κλειδιών που χρησιμοποιούνται ορίζονται στο στην επιλεγμένη πολιτική ασφάλειας VPN που καθορίζεται σε έναν δεδομένο σύνδεσμο επικοινωνίας. Στις τεχνικές προδιαγραφές των κρυπτοσυσκευών και στο νομικό πλαίσιο γύρω από τη χρήση τους, θα αναλυθούν περαιτέρω οι αλγόριθμοι που επιλέγονται για αυτό το σκοπό.

Προστασία της εμπιστευτικότητας των τοπολογικών δεδομένων των ιδιωτικών δικτύων

Η διασφάλιση της εμπιστευτικότητας των τοπολογικών δεδομένων των ιδιωτικών δικτύων παρέχει τη δυνατότητα αποτροπής της αποκάλυψης των εσωτερικών διευθύνσεων IP (διεύθυνση πηγής και προορισμού) εξοπλισμού σε ιδιωτικά δίκτυα. Όσον αφορά τα

δεδομένα εφαρμογής, οι αλγόριθμοι κρυπτογράφησης/αποκρυπτογράφησης χρησιμοποιούνται και ορίζονται σε περιβάλλοντα ασφαλείας.

Προστασία της αυθεντικότητας των τοπολογικών δεδομένων ιδιωτικών δικτύων

Η διασφάλιση της αυθεντικότητας των τοπολογικών δεδομένων των ιδιωτικών δικτύων παρέχει τη δυνατότητα εντοπισμού οποιασδήποτε τροποποίησης των εσωτερικών διευθύνσεων IP (διεύθυνση πηγής και προορισμού) του εξοπλισμού που βρίσκεται σε ιδιωτικά δίκτυα. Όσον αφορά τα δεδομένα εφαρμογής, οι αλγόριθμοι για τη δημιουργία πληροφοριών γνησιότητας ή για την επαλήθευσή τους χρησιμοποιούνται και ορίζονται σε περιβάλλον ασφαλείας.

Διαχωρισμός ροών IP

Κάθε ιδιωτικό δίκτυο μπορεί να χωριστεί σε πολλά υποδίκτυα IP για να επιτρέψει τον διαχωρισμό των ροών IP εντός ενός ιδιωτικού δικτύου. Το IP flows partitioning επιτρέπει την επιβολή διαφορετικών πολιτικών ασφαλείας VPN ακολουθώντας τα υποδίκτυα που επικοινωνούν. Αυτή η υπηρεσία παρέχει επίσης τη δυνατότητα φιλτραρίσματος εισερχόμενων πακέτων IP και αποστολής τους στο κατάλληλο υποδίκτυο.

Διαχείριση πολιτικών ασφαλείας VPN

Ορισμός πολιτικών ασφαλείας VPN: Οι πολιτικές ασφαλείας VPN πρέπει να μπορούν να καθορίζονται για κάθε εξουσιοδοτημένο σύνδεσμο επικοινωνίας VPN (VPN communication link). Ένας τέτοιος σύνδεσμος επικοινωνίας δημιουργείται μεταξύ δύο υποδικτύων IP. Μπορεί να υπάρχει μια πολιτική με κατεύθυνση επικοινωνίας. Μόνο ο διαχειριστής ασφαλείας πρέπει να έχει τη δυνατότητα να ορίσει αυτού του είδους τις πολιτικές. Επίσης, ο διαχειριστής ασφαλείας πρέπει να μπορεί να καθορίζει τον κανόνα του σιωπηρού φιλτραρίσματος (implicit filtering) για την αποστολή ή τη λήψη δεδομένων: αποδοχή, απόρριψη ή επιβολή υπηρεσιών ασφαλείας. Στην τελευταία περίπτωση, θα πρέπει να μπορεί

να ορίζει επίσης τις υπηρεσίες ασφαλείας που θα εφαρμοστούν στα δεδομένα που αποστέλλονται ή λαμβάνονται, καθώς και το πλαίσιο ασφαλείας που σχετίζεται με αυτήν την πολιτική. Το πλαίσιο ασφαλείας περιέχει, μεταξύ άλλων, χρησιμοποιημένους κρυπτογραφικούς αλγόριθμους, μεγέθη κλειδιών και τη συσχέτιση με κλειδιά που θα χρησιμοποιηθούν.

Διαβαθμισμένη πρόσβαση στις πολιτικές ασφαλείας VPN: Αυτή η υπηρεσία παρέχει τη δυνατότητα ελέγχου διαφορετικών τύπων πρόσβασης (τροποποίηση, προβολή) στις πολιτικές ασφάλειας VPN και στα περιβάλλοντα ασφαλείας σύμφωνα με την πιστοποίηση του χειριστή.

Διαχείριση κρυπτογραφικών κλειδιών

Ασφάλεια πρόσβασης στα κρυπτογραφικά κλειδιά: Αυτή η υπηρεσία παρέχει τη δυνατότητα αποτροπής της εξαγωγής μυστικών και ιδιωτικών κλειδιών με μη εξουσιοδοτημένο τρόπο. Επιτρέπει επίσης την εξακρίβωση ότι ένα δεδομένο κλειδί είναι χρήσιμο (προσβάσιμο) μόνο από υπηρεσίες που το χρειάζονται.

Έγχυση κρυπτογραφικών κλειδιών (Crypto keys injection): Αυτή η υπηρεσία παρέχει τη δυνατότητα έγχυσης των κρυπτογραφικών κλειδιών με ασφαλή τρόπο, που δημιουργούνται έξω από τον κρυπτογράφο IP, σε κρυπτογραφητές IP ή εξοπλισμό διαχείρισης. Κατά τη διανομή, αυτή η υπηρεσία προστατεύει τα κλειδιά με ακεραιότητα ή / και εμπιστευτικότητα ανάλογα με τον τύπο των κλειδιών.

Ορθή χρήση κρυπτογραφικών κλειδιών: Αυτή η υπηρεσία παρέχει τη δυνατότητα σωστής διαχείρισης του κύκλου ζωής των κρυπτογραφικών κλειδιών: παράκαμψη, τακτική ανανέωση, καταστροφή.

Έλεγχος και εποπτεία

Έλεγχος / καταγραφή των δραστηριοτήτων σε VPN links: Αυτή η υπηρεσία παρέχει τη δυνατότητα καταγραφής όλων των λειτουργιών που πραγματοποιούνται από IP Encryptors σχετικά με την επικοινωνία σε VPN links, όπως για παράδειγμα τη δημιουργία των

sessions και το κλείδωμα τους. Παρέχει επίσης τη δυνατότητα καθορισμού των συμβάντων που θα καταγράφονται.

Έλεγχος / καταγραφή των εργασιών διαχείρισης: Αυτή η υπηρεσία παρέχει τη δυνατότητα καταγραφής όλων των λειτουργιών που πραγματοποιούνται από τον διαχειριστή στον IP Encryptor σχετικά με τη διαχείριση αυτής της μονάδας κρυπτογράφησης, όπως για παράδειγμα την τροποποίηση των πολιτικών ασφαλείας VPN. Παρέχει επίσης τη δυνατότητα καθορισμού των συμβάντων που θα καταγράφονται.

Δημιουργία συναγερμών ασφαλείας: Αυτή η υπηρεσία παρέχει τη δυνατότητα δημιουργίας συναγερμών ασφαλείας για να υποδείξει οποιαδήποτε σημαντική λειτουργική αστοχία των IP Encryptors, όπως για παράδειγμα απώλεια ακεραιότητας των κλειδιών. Επιτρέπει επίσης σε έναν διαχειριστή ασφαλείας να ορίζει συναγερμούς που θα δημιουργούνται και τη λειτουργία εκπομπής τους και να ελέγχει αυτούς τους συναγερμούς. Οι συναγερμοί δεν ελέγχονται μέσω του IP Encryptor, αλλά αποστέλλονται από αυτόν σε κάποιο υπολογιστικό σύστημα το οποίο έχει διαβαθμισμένη χρήση.

Επίβλεψη IP Encryptor: Αυτή η υπηρεσία επιτρέπει σε έναν διαχειριστή συστήματος και δικτύου να ελέγχει την κατάσταση διαθεσιμότητας κάθε IP Encryptor (κατάσταση λειτουργίας, επίπεδα χρήσης πόρων κλπ).

Προστασία λειτουργιών διαχείρισης

Τοπική πιστοποίηση των διαχειριστών: Αυτή η υπηρεσία παρέχει τη δυνατότητα ελέγχου ταυτότητας όλων των διαχειριστών που εκτελούν λειτουργίες τοπικής διαχείρισης σε έναν IP Encryptor. Οι IP Encryptors τελούν υπό τοπική διαχείριση, δηλαδή διαχείριση που γίνεται απευθείας στο μηχάνημα που περιέχει τις υπηρεσίες του IP Encryptor.

Ασφάλεια πρόσβασης στις παραμέτρους διαμόρφωσης

Αυτή η υπηρεσία προστατεύει (από επίθεση στο δίκτυο) τις παραμέτρους διαμόρφωσης εμπιστευτικότητας και ακεραιότητας των IP Encryptors. Αυτές οι παράμετροι περιλαμβάνουν τις παραμέτρους διαμόρφωσης δικτύου (τοπολογικά δεδομένα σε ιδιωτικά δίκτυα), δεδομένα ελέγχου ταυτότητας και δικαιώματα πρόσβασης.

ΚΕΦΑΛΑΙΟ 7

ΟΙ ΚΡΥΠΤΟΜΗΧΑΝΕΣ ΤΗΣ ΒΟΡΕΙΟ-ΑΤΛΑΝΤΙΚΗΣ ΣΥΜΜΑΧΙΑΣ

7.1 Ο Κατάλογος Προϊόντων Διασφάλισης Πληροφοριών του ΝΑΤΟ (NIAPC)

Σε αυτή την ενότητα, θα μελετηθούν οι συσκευές κρυπτογράφησης IP οι οποίες παράγονται από χώρες της Βορειο-Ατλαντικής Συμμαχίας (North-Atlantic Treaty Organization – NATO) και χρησιμοποιούνται από αυτές για την κρυπτογράφηση των IP δικτύων τους (IP Encryption). Οι συσκευές που θα εξετάσουμε ανήκουν σε έναν κατάλογο πιστοποιημένων από το NATO προϊόντων, ο οποίος ονομάζεται Κατάλογος Προϊόντων Διασφάλισης Πληροφοριών του NATO (NATO Information Assurance Product Catalogue – NIAPC[40]). Ο NIAPC εφαρμόστηκε την 22 Σεπ 2010 με την Τεχνική Οδηγία Υλοποίησης της Ασφάλειας Πληροφοριών (INFOSEC Technical and Implementation Directive) υπ' αριθμόν AC/322-D(2010)0042 και σκοπός του είναι, σύμφωνα με την επίσημη ιστοσελίδα του NIAPC, *να παρέχει στα έθνη του NATO, καθώς και στους πολιτικούς και στρατιωτικούς φορείς του NATO έναν κατάλογο από προϊόντα διασφάλισης πληροφοριών (Information Assurance - IA), προφίλ προστασίας (Protection Profiles) και πακέτα που*

---

[40] NCI Agency (2010). *NATO Information Assurance Product Catalogue (NIAPC)* [online] Introduction. Available at https://www.ia.nato.int/niapc/Information/Introduction [Accessed 19 Oct 2020].

χρησιμοποιούνται ή είναι διαθέσιμα για προμήθεια για την κάλυψη επιχειρησιακών απαιτήσεων. Η παραπάνω οδηγία δημοσιεύθηκε από το Συμβούλιο NATO-C3[41] για την υποστήριξη της Πολιτικής Διαχείρισης Πληροφοριών του NATO (NATO Information Management Policy - NIMP)[42], των Πολιτικών Ασφαλείας του NATO για την προστασία διαβαθμισμένων και μη διαβαθμισμένων πληροφοριών και της Κύριας Οδηγίας (Primary Directive) για την Ασφάλεια Πληροφοριών (Information Security – INFOSEC) και καθορίζει τις διαδικασίες για τη δημιουργία, την ενημέρωση και τη συντήρηση του NIAPC. Η παραπάνω οδηγία είναι αυτή που καθορίζει στην ουσία αν κάποια συσκευή πληροί τις προδιαγραφές που θέτει το NATO για να ανήκει σε αυτό τον κατάλογο των πιστοποιημένων υλικών, άρα για να θεωρηθεί ένα υλικό (ή λογισμικό) συσκευή κρυπτογράφησης IP, πρέπει να πιστοποιηθεί βάσει αυτής της οδηγίας. Η εφαρμογή αυτής της οδηγίας, σύμφωνα με την επίσημη ιστοσελίδα του NIAPC, είναι δεσμευτική και υποχρεωτική για τον Κλάδο της Ασφάλειας Πληροφοριών (IA Branch) του Γενικού Επιτελείου Διαβουλεύσεων, Διοίκησης και Ελέγχου του NATO (NATO Headquarters Consultation, Command and Control (C3) Staff (NHQC3S))[43], για τον Οργανισμό Ασφάλειας και Αξιολόγησης του NATO

---

41 Το Συμβούλιο C3 του NATO είναι *το ανώτερο πολυεθνικό όργανο πολιτικής στον τομέα της Διαβούλευσης, της Διοίκησης και του Ελέγχου (C3), το οποίο υπάγεται διοικητικά και παρέχει εισηγήσεις στο Συμβούλιο Βόρειου Ατλαντικού (North-Atlantic Council) και την Επιτροπή Αμυντικού Σχεδιασμού (Defence Planning Committee) για όλα τα θέματα που αφορούν την πολιτική C3. Οι τομείς εστίασης του C3 είναι η ανταλλαγή πληροφοριών και η διαλειτουργικότητα, που περιλαμβάνουν θέματα όπως η υπεράσπιση στον κυβερνοχώρο, η διασφάλιση πληροφοριών, οι συλλογικές πληροφορίες, η επιτήρηση και η αναγνώριση* [21].

42 Η Πολιτική Διαχείρισης Πληροφοριών του NATO (NIMP) *καθορίζει τις βασικές αρχές της διαχείρισης πληροφοριών που πρέπει να εφαρμόζονται από τα έθνη του NATO και τους πολιτικούς και στρατιωτικούς φορείς του NATO* [20].

43 Το NHQC3S παρέχει υποστήριξη σε θέματα C3 στο Συμβούλιο Βορείου-Ατλαντικού (North-Atlantic Council) , στη Στρατιωτική Επιτροπή (Military Committee), στο Συμβούλιο C3 (C3 Board), στη Διάσκεψη των Διευθυντών Εθνικών Εξοπλισμών (Conference of National Armaments Directors), στο Συμβούλιο Σχεδιασμού Πόρων και Πολιτικής (Resource Planning and Policy Board), σε άλλες επιτροπές με αρμοδιότητες σχετικά με θέματα C3 και σε Μεραρχίες και Διευθύνσεις του Διεθνούς Επιτελείου και του Διεθνούς Στρατιωτικού Επιτελείου [21].

(Security and Evaluation Agency NATO - SECAN)[44] και για τις χώρες του NATO που υποβάλλουν προϊόντα IA ή προφίλ προστασίας στον NIAPC, οι οποίες είναι υπεύθυνες για την παροχή των απαιτούμενων πληροφοριών για αυτά τα προϊόντα, καθώς και για την ενημέρωση των πληροφοριών αυτών σε τακτά χρονικά διαστήματα.

7.2 Νομικό πλαίσιο ένταξης μιας συσκευής κρυπτογράφησης στον NIAPC

Οι βασικές προϋποθέσεις ένταξης μιας συσκευής στον NIAPC ως συσκευή IP Encryption είναι οι παρακάτω:

- Να χρηματοδοτούνται, να αναπτύσσονται και να παράγονται από κράτος-μέλος που ανήκει στο NATO, καθώς και να ελέγχονται από την Εθνική Αρχή Ασφάλειας Επικοινωνιών του κράτους αυτού.
- Να έχουν λάβει αναγνωρισμένη από το NATO εθνική ή διεθνή αξιολόγηση ή πιστοποίηση.

---

[44] Ο Οργανισμός Ασφάλειας και Αξιολόγησης του NATO (SECAN) αποτελεί υπηρεσία που υπάγεται διοικητικά στην Στρατιωτική Επιτροπή του NATO και παρέχει τεχνική υποστήριξη στην υποεπιτροπή Ασφάλειας Πληροφοριών. Είναι οργανωμένο και στελεχωμένο από τις Ηνωμένες Πολιτείες και είναι ο οργανισμός του NATO που αξιολογεί τα συστήματα κρυπτογράφησης και τον εξοπλισμό ασφαλείας επικοινωνιών που προτείνεται για χρήση στη διερχόμενη κυκλοφορία πληροφοριών του NATO και συνιστά την έγκρισή τους ή την απόρριψή τους στη Στρατιωτική Επιτροπή. Όταν ζητηθεί, το SECAN πιστοποιεί την ασφάλεια των χρηματοδοτούμενων από το NATO CIS και των Computer Controlled Systems. Επίσης, όταν ζητηθεί από κάποια άλλη αρχή διαπίστευσης και υπάρχει αμοιβαία συμφωνία, υπάρχει η δυνατότητα αξιολόγησης τέτοιων συστημάτων. Τέλος, ο SECAN αξιολογεί την ευπάθεια των επικοινωνιών και των CIS στην τεχνική εκμετάλλευση και προτείνουν τεχνικές πολιτικές, πρότυπα και διαδικασίες τύπου COMSEC και COMPUSEC [22].

- Να υπόκεινται σε επιπρόσθετη εθνική έγκριση σύμφωνα με την Τεχνική Οδηγία Υλοποίησης της INFOSEC για την κρυπτογραφική ασφάλεια και τους κρυπτογραφικούς μηχανισμούς από την εκάστοτε Εθνική Αρχή Ασφάλειας Επικοινωνιών της χώρας προέλευσης[45].
- Να θεωρούνται εμπορικά κατάλληλα για τις συνθήκες της αγοράς του NATO.

Σύμφωνα με την επίσημη ιστοσελίδα του NIAPC, τα παραπάνω προϊόντα θα πρέπει να έχουν λάβει εθνική ή διεθνή πιστοποίηση που είναι αναγνωρισμένη από το NATO. Ένας διεθνής τύπος πιστοποίησης αναγνωρισμένος από το NATO είναι και τα Κοινά Κριτήρια για την Αξιολόγηση της Ασφάλειας της Τεχνολογίας Πληροφοριών (αναφέρονται ως Common Criteria ή CC) τα οποία αποτελούν ένα διεθνές πρότυπο (ISO / IEC 15408) για την πιστοποίηση της ασφάλειας των υπολογιστικών συστημάτων. Το παραπάνω πρότυπο επιτρέπει τη γενική σύγκριση μεταξύ των αποτελεσμάτων των ανεξάρτητων (συνήθως εθνικών) αξιολογήσεων ασφαλείας, καθώς παρέχει ένα κοινό σύνολο απαιτήσεων για τη λειτουργικότητα ασφάλειας των προϊόντων πληροφορικής και για τα μέτρα διασφάλισης που πρέπει να εφαρμόζονται σε αυτά τα προϊόντα κατά την αξιολόγηση ασφάλειάς τους. Αποτελούν ένα πλαίσιο στο οποίο οι χρήστες που θέλουν να αξιολογήσουν ένα υπολογιστικό σύστημα (το οποίο εκφράζεται ως Στόχος Αξιολόγησης – Target Of Evaluation (TOE)[46]) μπορούν να καθορίσουν τις λειτουργικές απαιτήσεις ασφαλείας και τις απαιτήσεις διασφάλισης (SFR[47] και SAR[48] αντίστοιχα) ως έναν Στόχο Ασφαλείας (Security

---

45 NCI Agency (2010). *NATO Information Assurance Product Catalogue (NIAPC).* [online] Vendor Information. Available at https://www.ia.nato.int/niapc/Information/NIAPC-vendor-info [Accessed 20 Oct 2020].

46 Ο Target Of Evaluation (TOE), σε όρους CC, αποτελεί το προϊόν το οποίο αποτελεί το αντικείμενο της CC αξιολόγησης.

47 Οι Security Functional Requirements (SFR) καθορίζουν τους κανόνες με τους οποίους ένας Στόχος Αξιολόγησης (Target of Evaluation – TOE) διέπει την πρόσβαση και τη χρήση των πόρων του, και επομένως τις πληροφορίες και τις υπηρεσίες που ελέγχονται από τον TOE.

48 Οι Security Assurance Requirements (SAR) αποτελούν περιγραφές των μέτρων που ελήφθησαν κατά την ανάπτυξη και αξιολόγηση του προϊόντος για να διασφαλιστεί η συμμόρφωση με τη διεκδικούμενη

Target - ST)[49] και μπορεί να ληφθούν από ένα Προφίλ Προστασίας (Protection Profile - PP)[50].

Η σημαντικότητα του προτύπου αυτού φαίνεται και από το γεγονός ότι σύμφωνα με την επίσημη ιστοσελίδα του NIAPC, εάν η πιστοποίηση των συσκευών δεν έχει γίνει βάσει των CC, θα πρέπει να υπάρχει γραπτή δήλωση από την Εθνική Αρχή Ασφάλειας Επικοινωνιών της χώρας προέλευσης του υλικού ότι η πιστοποίησή τους είναι ισοδύναμη με αυτή των CC[51]. Παρόλα αυτά, η NCI Agency θέτει ως προϋπόθεση για τα προϊόντα με πιστοποίηση CC ότι *μόνο τα προϊόντα που χρηματοδοτούνται εντός κράτους-μέλους του ΝΑΤΟ και θεωρούνται κατάλληλα για χρήση εντός αυτού του έθνους για την προστασία των εθνικών πληροφοριών μπορούν να ενταχθούν στο NIAPC.*[52]

λειτουργικότητα ασφαλείας. Για παράδειγμα, μια αξιολόγηση μπορεί να απαιτεί να διατηρείται όλος ο πηγαίος κώδικας σε ένα σύστημα ή να πραγματοποιείται πλήρης λειτουργικός έλεγχος [62].

[49] Οι Security Targets (ST) αποτελούν έγγραφα που προσδιορίζουν τις ιδιότητες ασφαλείας ενός στόχου αξιολόγησης. Ο ST μπορεί να αξιώσει συμμόρφωση με ένα ή περισσότερα Προφίλ Προστασίας (Protection Profiles – PP). Το TOE αξιολογείται βάσει των SFRs (Security Functional Requirements) που έχουν καθιερωθεί στο ST του. Αυτό επιτρέπει στους πωλητές να προσαρμόσουν την αξιολόγηση ώστε αυτή να ταιριάζει με ακρίβεια στις προβλεπόμενες δυνατότητες του προϊόντος τους [25].

[50] Τα Protection Profiles (PP) αποτελούν έγγραφα που ορίζουν ένα σύνολο απαιτήσεων και στόχων ασφάλειας για μια κατηγορία προϊόντων ή συστημάτων, τα οποία ικανοποιούν τις ανάγκες μιας κοινότητας χρηστών για ασφάλεια πληροφοριακών συστημάτων. Ένα PP προορίζεται για να επαναχρησιμοποιηθεί και να καθορίσει απαιτήσεις που είναι γνωστό ότι είναι χρήσιμες και αποτελεσματικές για την επίτευξη των καθορισμένων στόχων [26].

[51] NCI Agency (2010). *NATO Information Assurance Product Catalogue (NIAPC).* [online] Vendor Information. Available at https://www.ia.nato.int/niapc/Information/NIAPC-vendor-info [Accessed 20 Oct 2020].

[52] NCI Agency (2010). *NATO Information Assurance Product Catalogue (NIAPC).* [online] Vendor Information. Available at https://www.ia.nato.int/niapc/Information/NIAPC-vendor-info [Accessed 20 Oct 2020].

7.3 Απαιτήσεις ασφάλειας εκπομπών – η πιστοποίηση TEMPEST

7.3.1 Ορισμός του TEMPEST

Σύμφωνα με την Εθνική Αρχή Ασφάλειας Επικοινωνιών των Ηνωμένων Πολιτειών της Αμερικής (NSA), ο όρος TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions)[53] αφορά τεχνικές έρευνες σε ραδιοεκπομπές από ηλεκτρικό εξοπλισμό επεξεργασίας πληροφοριών οι οποίες μπορεί να εκθέσουν ευαίσθητες πληροφορίες[54]. Οι ραδιοεκπομπές αυτές ορίζονται ως Compromising Emanations – CE και είναι σήματα τα οποία, εάν υποκλαπούν και αναλυθούν, αποκαλύπτουν τις πληροφορίες εθνικής ασφάλειας που μεταδίδονται, λαμβάνονται, διαχειρίζονται ή επεξεργάζονται με άλλο τρόπο από οποιοδήποτε εξοπλισμό επεξεργασίας πληροφοριών. Η θεωρία γύρω από το TEMPEST συνοψίζεται στο ότι τα ηλεκτρομαγνητικά πεδία συνοδεύουν οποιοδήποτε κύκλωμα που έχει μεταβαλλόμενες τάσεις και ρεύματα. Αυτά τα πεδία βρίσκονται στο διάστημα που περιβάλλει τα κυκλώματα και τα πλάτη τους εξαρτώνται από παράγοντες όπως (α) τάση και πλάτος ρεύματος στο κύκλωμα. (β) τάση και τρέχοντες ρυθμοί μεταβολής (γ) διαστάσεις του κυκλώματος ·και (δ) απόσταση από το κύκλωμα. Επομένως, κάθε κύκλωμα και τα συστατικά του μπορούν να θεωρηθούν ως κεραίες που παράγουν ηλεκτρομαγνητικά πεδία που διαδίδονται μέσω του χώρου - καθένα από τα οποία μπορεί να προκαλέσει CE.[55].

---

53 Mark Ciampa (2018). *CompTIA Security+ Guide to Network Security Fundamentals.*6th Edition.

54 National Security Agency (NSA) - National Communications Security Committee (NCSC) - Subcommittee on Compromising Emanations (SCOCE) (2001). *Tempest Glossary*. [online] Available at http://cryptome.org/0001/ncsc-3.htm.

55 Cryptome.org (2003). *National Security Agency (NSA). NACSIM 5000 Tempest Fundamentals.* [online] Available at http://cryptome.org/jya/nacsim-5000/nacsim-5000.htm [Accessed 20 Oct 2020].

7.3.2 Η έννοια της Κόκκινης και Μαύρης πλευράς (RED/BLACK)

Θεμελιώδης έννοια για την εφαρμογή της αρχιτεκτονικής μιας συσκευής που προσφέρει προστασία TEMPEST είναι η έννοια της Κόκκινης/Μαύρης πλευράς (RED/BLACK). Η έννοια RED/BLACK υπαγορεύει ότι τα ηλεκτρικά και ηλεκτρονικά κυκλώματα, τα εξαρτήματα, ο εξοπλισμός, τα συστήματα κ.λπ., τα οποία χειρίζονται μη κρυπτογραφημένες πληροφορίες εθνικής ασφάλειας σε μορφή ηλεκτρικού σήματος (RED), πρέπει να διαχωρίζονται από εκείνα που χειρίζονται κρυπτογραφημένες ή μη ταξινομημένες πληροφορίες (BLACK). Σύμφωνα με αυτήν την έννοια, η ορολογία RED/BLACK χρησιμοποιείται για την αποσαφήνιση συγκεκριμένων κριτηρίων που σχετίζονται με τη διαφορά μεταξύ τέτοιων κυκλωμάτων, εξαρτημάτων, εξοπλισμών. συστημάτων κ.λπ. και τις περιοχές στις οποίες περιλαμβάνονται[56]. Το πλαίσιο RED/BLACK εφαρμόζεται σε δύο μέρη: στο φυσικό διαχωρισμό και τον ηλεκτρικό διαχωρισμό:

- **Φυσικός διαχωρισμός:** Όλος ο εξοπλισμός, τα καλώδια, τα εξαρτήματα και τα συστήματα που επεξεργάζονται πληροφορίες εθνικής ασφάλειας ορίζονται ως RED. Όλος ο εξοπλισμός, όπως καλωδιώσεις. συστατικά και συστήματα που επεξεργάζονται κρυπτογραφημένες πληροφορίες εθνικής ασφάλειας ή αδιαβάθμητες πληροφορίες ορίζονται ως BLACK. Ο σκοπός του πλαισίου RED / BLACK είναι να καθιερώσει την ελάχιστη απαίτηση φυσικού διαχωρισμού για τη μείωση της πιθανότητας της σύνδεσης των ηλεκτρομαγνητικών εκπομπών από ηλεκτρονικό εξοπλισμό RED με ηλεκτρονικό εξοπλισμό BLACK.
- **Ηλεκτρικός διαχωρισμός:** Ο ηλεκτρικός διαχωρισμός διασφαλίζει ότι κάθε αγωγός σήματος από εξοπλισμό τύπου RED δρομολογείται μόνο σε άλλο εξοπλισμό τύπου RED ή κρυπτογραφείται πριν από τη σύνδεση με εξοπλισμό τύπου BLACK. Ο ηλεκτρικός διαχωρισμός αφορά τη διανομή σήματος, τη διανομή ισχύος και τη γείωση. Σύμφωνα με το Συμβουλευτικό Μνημόνιο για την Ασφάλεια των Τηλεπικοινωνιών και Πληροφοριακών Συστημάτων Εθνικής Ασφάλειας των Ηνωμένων Πολιτειών Αμερικής (USA National Security Telecommunications and Information

---

[56] Cryptome.org (2003). *National Security Agency (NSA). NACSIM 5000 Tempest Fundamentals.* [online] Available at http://cryptome.org/jya/nacsim-5000/nacsim-5000.htm [Accessed 20 Oct 2020].

Systems Security Advisory Memorandum (NSTISSAM)),[57] οι μεταγωγείς (switches) ή/και άλλες συσκευές που χρησιμοποιούνται για τη διασύνδεση μεταξύ κυκλωμάτων/εξοπλισμού RED και BLACK (όπως η συσκευή κρυπτογράφησης IP, η οποία δέχεται μη κρυπτογραφημένα δεδομένα και τα δρομολογεί ως κρυπτογραφημένα) θα πρέπει να παρουσιάζουν τα ακόλουθα χαρακτηριστικά απομόνωσης από θύρα σε θύρα, ανάλογα με την περίπτωση:

- 100 dB πάνω από το εύρος συχνοτήτων ήχου βασικής ζώνης μεταξύ 0,3 και 15 kHz.
- 80 dB σε εύρος συχνοτήτων βίντεο βασικής ζώνης έως 5 MHz.

- 60 dB πάνω από το εύρος συχνοτήτων από μία φορά (Rd) έως δέκα φορές το βασικό ρυθμό δεδομένων (10Rd) του ψηφιακού σήματος (ή σημάτων) που υποβάλλονται σε επεξεργασία.

7.3.3 Πρότυπα TEMPEST

Μια συσκευή κρυπτογράφησης IP μπορεί να είναι κατασκευασμένη με αρχιτεκτονική που παρέχει ασφάλεια εκπομπών τύπου TEMPEST. Αυτές οι συσκευές ανήκουν σε μια κατηγορία προϊόντων του καταλόγου NIAPC με τον όρο Emission Security, όπως είναι και οι συσκευές κρυπτογράφησης με τον όρο IP Encryption. Οι συσκευές αυτές είναι κατά τέτοιο τρόπο κατασκευασμένες ώστε να παρέχουν, ανάλογα με το επίπεδο ασφάλειας, κάλυψη των εκούσιων ραδιοεκπομπών από τον ηλεκτρονικό εξοπλισμό τους. Αυτό γίνεται με διάφορους τρόπους όπως η υποχρεωτική απόσταση του εξοπλισμού από τους τοίχους, η θωράκιση των κτιρίων, των καλωδίων και του εξοπλισμού, τα καλώδια για το διαχωρισμό της κρυπτογραφημένης από τη μη κρυπτογραφημένη πληροφορία ή ακόμη

---

[57] Cryptome.org (2000). *National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST 2-95: Red/Black Installation Guidance*. [online] Available at http://cryptome.org/jya/tempest-2-95.htm [Accessed 20 Oct 2020].

η απόσταση – θωράκιση μεταξύ καλωδίων.[58] Οι συσκευές οι οποίες είναι κατασκευασμένες με αυτό τον τρόπο, για να συμπεριληφθούν στον NIAPC, πρέπει να έχουν μια πιστοποίηση TEMPEST. Τα διεθνή πρότυπα που ορίζουν τις προδιαγραφές κατασκευής των συσκευών αυτών είναι κατά κύριο λόγο το NATO SECAN and Information Publication (SDIP) – 27/1 (σε συνδυασμό με το NATO SECAN Doctrine and Information Publication (SDIP) – 28/1 το οποίο ορίζει τις ζώνες TEMPEST) [59] και το ισοδύναμο USA NSTISSAM/1-92[60]. Τα πρότυπα αυτά ορίζουν τα επίπεδα TEMPEST, δηλαδή κατά πόσο είναι μία συσκευή προστατευμένη από τις εκπομπές τύπου TEMPEST, και πρέπει να εφαρμόζονται αναλογικά με τη ζώνη TEMPEST.

7.3.4 Ζώνες και Επίπεδα TEMPEST

Οι ζώνες TEMPEST ορίζονται από το NATO SECAN Doctrine and Information Publication (SDIP) – 28/1.[61] Αυτή η οδηγία καθορίζει μια μέθοδο μέτρησης της εξασθένησης των εκπομπών σύμφωνα με την οποία τα μεμονωμένα δωμάτια εντός μιας περιμέτρου ασφαλείας ταξινομούνται ως δωμάτια Ζώνης 0, Ζώνης 1, Ζώνης 2 ή Ζώνης 3. Στην ουσία, όσο πιο κοντά βρίσκεται κάποιος στη συσκευή που επεξεργάζεται ευαίσθητες πληροφορίες και εκπέμπει ηλεκτρομαγνητική ακτινοβολία, τόσο πιο πιθανό είναι να υποκλέψει τις

---

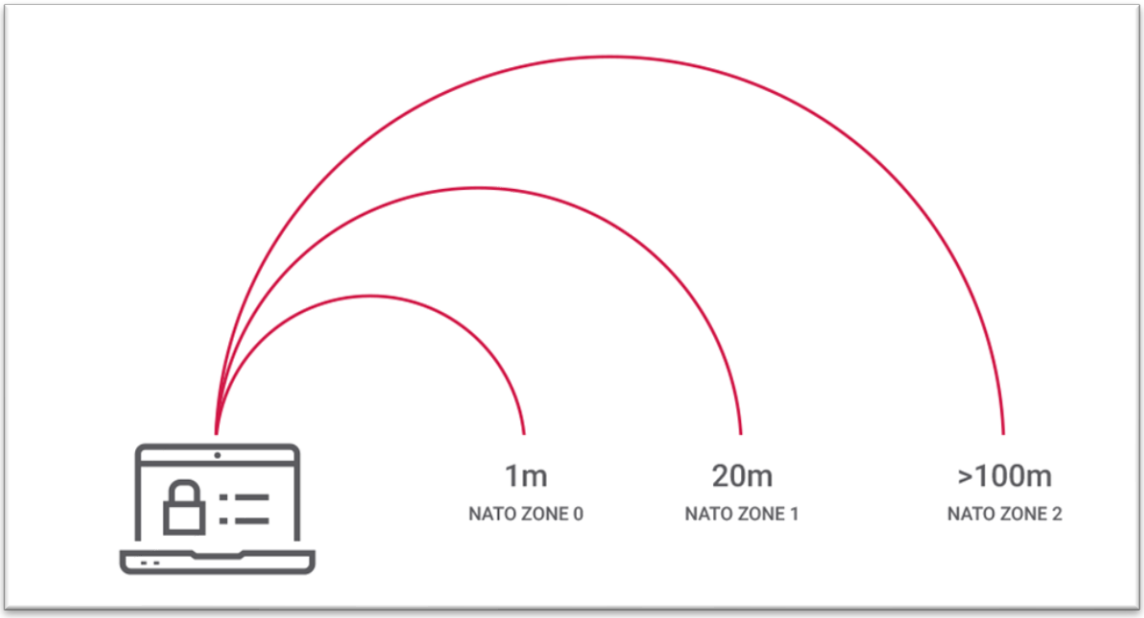
58 Internet Archive Wayback Machine (2009). National Security Agency (NSA). *TEMPEST: A Signal Problem*. [online] [30].

59 NCI Agency (2010). *NATO Information Assurance Product Catalogue (NIAPC)* [online] TEMPEST Equipment Selection Process. Available at https://www.ia.nato.int/niapc/tempest/certification-scheme [Accessed 20 Oct 2020].

60 Secure Systems and Technologies. *Tempest Introduction*. Available at https://www.apitech.com/globalassets/documents/products/secure-systems--information-assurance/sst/tempest-introduction-iss-3.pdf [Accessed 20 Oct 2020].

61 NCI Agency (2010). *NATO Information Assurance Product Catalogue (NIAPC)* [online] TEMPEST Equipment Selection Process. Available at https://www.ia.nato.int/niapc/tempest/certification-scheme [Accessed 20 Oct 2020].

εκπομπές αυτές. Άρα, όσο πιο μεγάλη η πιθανότητα να συμβεί μια υποκλοπή σε μικρότερη απόσταση, τόσο μεγαλύτερη πρέπει να είναι η προστασία που απαιτείται. Το παρακάτω σχήμα δείχνει την έκταση των ζωνών TEMPEST, βάσει της SDIP 27/1.



Σχήμα 7.1: Οι ζώνες TEMPEST [34]

4. NATO Zone 0: Αφορά την απόσταση 1 m από το αντικείμενο ενδιαφέροντος
5. NATO Zone 1: Αφορά την απόσταση 20 m από το αντικείμενο ενδιαφέροντος
6. NATO Zone 2: Αφορά την απόσταση έως 100m από το αντικείμενο ενδιαφέροντος.

Το παρακάτω σχήμα δείχνει συνοπτικά τα επίπεδα TEMPEST, βάσει των προτύπων που αναφέρθηκαν στην παραπάνω ενότητα:

Descriptive	**Full**	**Intermediate**	**Tactical**
SDIP-27 NATO Standard	Level A	Level B	Level C
previous NATO Laboratory test Standards	AMSG-720B	AMSG-788A	AMSG-784
NATO Zoning Standards	ZONE 0	ZONE 1	ZONE 2
USA NSTISSAM /1-92 Standards	LEVEL I	LEVEL II	LEVEL III
SST Example Products	SC1000TF SC8200TF SN9200TF	SN230TIR SC8200TI SS8270TI	SN790TTR SC8338TTRM SP280TTR

Σχήμα 7.2: Τα επίπεδα TEMPEST βάσει των επίσημων προτύπων [34]

5. SDIP-27 Level A (USA NSTISSAM Level I): Το τυποποιημένο επίπεδο TEMPEST Level A είναι το αυστηρότερο πρότυπο NATO και εφαρμόζεται σε περιβάλλοντα και συσκευές όπου μπορεί να προκύψει άμεση υποκλοπή, από όσο κοντά στο διπλανό δωμάτιο (απόσταση περίπου 1 μέτρων). Αυτό το πρότυπο εφαρμόζεται σε συσκευές που λειτουργούν εντός της NATO Zone 0. Αναφέρεται και ως «Full».
6. SDIP-27 Level B (USA NSTISSAM Level II): Το επίπεδο TEMPEST Level B εφαρμόζεται συνήθως σε συσκευές όπου υποτίθεται ότι η υποκλοπή δεν μπορεί να συμβεί σε απόσταση μικρότερη από 20 μέτρα. Αυτό το πρότυπο TEMPEST εφαρμόζεται σε συσκευές που λειτουργούν εντός της NATO Zone 1 και προστατεύει συσκευές τόσο από την ανεμπόδιστη απόσταση των 20 μέτρων είτε από μια συγκρίσιμη απόσταση η οποία συμπίπτει με δομικά στοιχεία – εμπόδια. Αναφέρεται και ως Intermediate ή Immediate.
7. SDIP-27 Level C (USA NSTISSAM Level II): Το επίπεδο TEMPEST Level C εφαρμόζεται σε περιβάλλοντα και συσκευές εντός της NATO Zone 2 (όπου οι υποκλοπείς υποτίθεται ότι έχουν απόσταση τουλάχιστον 100 μέτρων). Αυτό το πρότυπο προστατεύει τις συσκευές τόσο από την ανεμπόδιστη απόσταση των 100 μέτρων,

είτε από μια συγκρίσιμη απόσταση η οποία συμπίπτει με δομικά στοιχεία – εμπόδια. Αναφέρεται και ως Tactical[62].

7.3.5 Νομικό πλαίσιο ένταξης μιας συσκευής κρυπτογράφησης στην κατηγορία "Emission Security" του NIAPC

Μια συσκευή, για να ενταχθεί στον NIAPC ως συσκευή "Emission Security" πρέπει, πέραν των αναφερομένων για τον NIAPC στο κεφάλαιο 1.2 (παράγραφοι 1,2 και 4), να υπόκειται σε επιπρόσθετη εθνική έγκριση σύμφωνα με την Τεχνική Οδηγία Υλοποίησης Ασφάλειας Εκπομπών (AC / 322-D (2007) 0036) από την εκάστοτε Εθνική Αρχή TEMPEST (NTA) της χώρας προέλευσης. Η οδηγία αυτή, σύμφωνα με την NSA Agency, είναι υποχρεωτικό να εφαρμόζεται *για όλες τις οντότητες που συμμετέχουν στις διαδικασίες πιστοποίησης για τους προμηθευτές TEMPEST*. Είναι επίσης υποχρεωτική για *τα έθνη του ΝΑΤΟ, τις εντολές και τις υπηρεσίες που χρησιμοποιούν προϊόντα τεχνολογίας πληροφοριών σε συστήματα επικοινωνιών και πληροφοριών για την επεξεργασία, αποθήκευση ή μετάδοση πληροφοριών του ΝΑΤΟ που έχουν διαβάθμιση ασφαλείας ΝΑΤΟ-CONFIDENTIAL ή παραπάνω.*[63] Από τα παραπάνω γίνεται κατανοητό ότι οι κρυπτομηχανές τύπου IP, οι οποίες είναι διαβαθμισμένες από το ΝΑΤΟ ως NATO-CONFIDENTIAL[64] ή παραπάνω, πρέπει να έχουν και την ανάλογη πιστοποίηση TEMPEST από την εκάστοτε Εθνική Αρχή TEMPEST, βάσει της παραπάνω οδηγίας. Η NSA Agency ορίζει συγκεκριμένα για τις συσκευές πλήρωσης κλειδιών (όπως το CIK) ότι *"μόνο συσκευές κρυπτογράφησης πλήρωσης κλειδιών οι οποίες αξιολογούνται και εγκρίνονται σύμφωνα με την «Τεχνική Οδηγία Υλοποίησης της INFOSEC για την κρυπτογραφική ασφάλεια και*

---

62 Fibersystem AB. *Tempest.* Available at https://www.fibersystem.com/tempest/ [Accessed 21 Oct 2020].

63 NCI Agency (2010). NATO Information Assurance Product Catalogue (NIAPC) [online] TEMPEST Equipment Selection Process. Available at https://www.ia.nato.int/niapc/tempest/certification-scheme [Accessed 20 Oct 2020].

64 NATO Allied Command Transformation. *NATO Security Indoctrination.* [online] Available at https://www.act.nato.int/images/stories/structure/reserve/hqrescomp/nato-security-brief.pdf

τους κρυπτογραφικούς μηχανισμούς» και την «Τεχνική Οδηγία Υλοποίησης Ασφάλειας Εκπομπών» είναι επιλέξιμες για ένταξη στον NIAPC."[65].

7.4 Οι βαθμοί ασφαλείας των υλικών του NIAPC

Κάθε συσκευή ή υλικό του NIAPC έχει και μία ένδειξη «NATO Classification», η οποία αντιπροσωπεύει την κατηγορία διαβάθμισης ασφαλείας των πληροφοριών – δεδομένων που το υλικό μπορεί να χειριστεί, δηλαδή του βαθμού ασφαλείας με τον οποίο χαρακτηρίζεται η ευαισθησία των χειριζόμενων πληροφοριών ως προς τις συνέπειες που θα προκαλέσει η ενδεχόμενη μη εξουσιοδοτημένη πρόσβαση σε αυτές. Το ΝΑΤΟ έχει τα παρακάτω πέντε επίπεδα διαβάθμισης πληροφοριών:

- COSMIC TOP SECRET (CTS): εφαρμόζεται σε πληροφορίες των οποίων η μη εξουσιοδοτημένη αποκάλυψη θα προκαλούσε εξαιρετικά σοβαρή ζημιά στο ΝΑΤΟ. Η σήμανση "COSMIC" εφαρμόζεται σε υλικό TOP SECRET για να δηλώσει ότι είναι ιδιοκτησία του ΝΑΤΟ.
- NATO SECRET (NS): εφαρμόζεται σε πληροφορίες των οποίων η μη εξουσιοδοτημένη αποκάλυψη θα προκαλούσε σοβαρή ζημιά στο ΝΑΤΟ.
- NATO CONFIDENTIAL (NC): εφαρμόζεται σε πληροφορίες των οποίων η μη εξουσιοδοτημένη αποκάλυψη θα ήταν επιζήμια για τα συμφέροντα του ΝΑΤΟ.
- NATO RESTRICTED (NR): εφαρμόζεται σε πληροφορίες των οποίων η μη εξουσιοδοτημένη αποκάλυψη θα ήταν δυσμενής για τα συμφέροντα του ΝΑΤΟ.
- NATO UNCLASSIFIED (NU): εφαρμόζεται σε επίσημες πληροφορίες που αποτελούν ιδιοκτησία του ΝΑΤΟ, αλλά δεν πληρούν τα κριτήρια ένταξης σε κάποιον από

---

[65] NCI Agency (2010). NATO Information Assurance Product Catalogue (NIAPC). [online] Vendor Information. Available at https://www.ia.nato.int/niapc/Information/NIAPC-vendor-info [Accessed 20 Oct 2020].

τους παραπάνω βαθμούς ασφαλείας. Η πρόσβαση στις πληροφορίες από οντότητες που δεν ανήκουν στο NATO επιτρέπεται μόνο όταν αυτή η πρόσβαση δεν είναι επιζήμια για το NATO.[66]

Γίνεται εύκολα αντιληπτό ότι, όσο υψηλότερος είναι ο βαθμός ασφάλειας, τόσο πιο ισχυροί πρέπει να είναι οι μηχανισμοί ασφαλείας που παρέχει η συσκευή κρυπτογράφησης ασφαλείας, όπως π.χ ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται ή ο βαθμός της προστασίας TEMPEST που προσφέρει η αρχιτεκτονική του υλικού.

7.5 Οι κρυπτομηχανές τύπου IP του NIAPC

Σε αυτή την ενότητα, θα γίνει μία ανασκόπηση μερικών από τις συσκευές κρυπτογράφησης IP του καταλόγου NIAPC οι οποίες χρηματοδοτούνται, αναπτύσσονται και παράγονται από κατασκευαστές που εδρεύουν σε κράτος-μέλος του NATO και ελέγχονται από την Εθνική Αρχή Ασφάλειας Επικοινωνιών του κράτους αυτού, δίνοντας έμφαση στις πιστοποιήσεις που αυτές οι συσκευές διαθέτουν και αναφέρθηκαν παραπάνω, έτσι ώστε να δημιουργήσουμε ένα άτυπο μοντέλο των προδιαγραφών που θα πρέπει να έχει ένα υλικό ώστε να μπορεί να λειτουργήσει ως κρυπτομηχανή. Η ανασκόπηση θα επικεντρωθεί στα παρακάτω στοιχεία:

- **Επίπεδο διαβάθμισης** (π.χ, COSMIC TOP SECRET. Θα παρουσιαστούν κρυπτομηχανές κάθε είδους διαβάθμισης για να παρατηρηθούν οι διαφορές τους.)
- **Χαρακτηριστικά φυσικής σχεδίασης συσκευής**, όπως:
  - Μέγεθος, βάρος, τροφοδοσία
  - Συνθήκες περιβάλλοντος στις οποίες μπορεί να λειτουργήσει (π.χ θερμοκρασία, υγρασία, πιστοποίηση MIL-STD-810 E)
- **Επικοινωνιακές δυνατότητες**, όπως:
  - Δημιουργία IPSec VPN και τύποι IPSec που υλοποιεί (συνήθως IKE - ESP)

---

[66] NATO Allied Command Transformation. *NATO Security Indoctrination.* [online] Available at https://www.act.nato.int/images/stories/structure/reserve/hqrescomp/nato-security-brief.pdf

- Πρωτόκολλα επικοινωνίας που υποστηρίζονται (π.χ TCP, IP, HTTP, DNS, SNMP, ARP)
- Απόδοση στο δίκτυο (π.χ Full-duplex 100 Mbps σε Ethernet interface)
- Είδη και αριθμός διεπαφών (interfaces) που υποστηρίζονται
- Αριθμός ταυτόχρονων συσχετίσεων ασφαλείας (SAs) που υποστηρίζει
- Δυνατότητες NAT
- Ύπαρξη κεντρικού συστήματος διαχείρισης
- **Χαρακτηριστικά λογικής ασφάλειας δικτύου που παρέχει η συσκευή, όπως:**
  - Αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται (π.χ AES)
  - Δυνατότητες και τρόποι εισαγωγής κλειδών
  - Επίπεδα διαχείρισης συσκευής (π.χ administrator)
  - Δυνατότητες καταγραφής ενεργειών (logging)
- **Χαρακτηριστικά φυσικής ασφάλειας συσκευής**, όπως:
  - Αρχιτεκτονική RED/BLACK
  - Δυνατότητα αυτοελέγχου BITE
  - Επίπεδο TEMPEST στο οποίο είναι πιστοποιημένη
  - Δυνατότητες ασφάλειας από ηλεκτρομαγνητικές παρεμβολές της συσκευής (π.χ πιστοποίηση κατά MIL-STD 461/462)
  - Χαρακτηριστικά επιχειρησιακής ασφάλειας (π.χ ύπαρξη του Crypto Ignition Key, προστασία από φυσικές παραβιάσεις (tamper protection), ύπαρξη διακόπτη επείγουσας διαγραφής δεδομένων κ.α)
- **Χαρακτηριστικά αξιοπιστίας, όπως:**
  - Mean Time Between Failures, MTBF
  - Δυνατότητες hot-standby
- **Πιστοποιήσεις Common Criteria** ή άλλων επίσημων φορέων.

7.5.1 Οι κρυπτομηχανές TCE 621 – Νορβηγία

Οι Cryptel IP High Capacity Encryption Devices TCE 621 είναι Νορβηγικής προέλευσης, με κατασκευάστρια εταιρεία την Thales Norway.

Σχήμα 7.3: Οι κρυπτομηχανές TCE 621/B και TCE 621/C [36]

Επίπεδο διαβάθμισης

Σύμφωνα με την NCI Agency, οι κρυπτομηχανές της οικογένειας TCE 621 τύπου N, B, και C (NICE) είναι διαβαθμισμένες με την μεγαλύτερη δυνατή διαβάθμιση, δηλαδή ως COSMIC TOP SECRET (CTS). Οι όμοιες κρυπτομηχανές τύπου C (AES)/(BLACK), M, και V/V (AES) είναι διαβαθμισμένες ως NATO SECRET.[67] Η διαφορά ανάμεσα στην TCE 621 C (NICE) και στην C (AES) είναι ο αλγόριθμος κρυπτογράφησης που χρησιμοποιεί. Εάν ο αλγόριθμος αυτός είναι ο AES, ο οποίος γενικά υπάρχει στο εμπόριο και σε άλλα συστήματα που υλοποιούν το IPSec, όπως π.χ ένα Cisco ASA Firewall, η κρυπτομηχανή διαβαθμίζεται ως NATO SECRET. Ειδάλλως, αν ο αλγόριθμος είναι σχεδιασμένος από

---

[67] NCI Agency (2010). NATO Information Assurance Product Catalogue (NIAPC) [online] Selected Category: IP Encryption. Available at https://www.ia.nato.int/niapc/Category/IP-Encryption_25

το NATO, όπως ο NICE, ο οποίος δεν διατίθεται ελεύθερος σε άλλα συστήματα που υλοποιούν το IPSec, η συσκευή αναβαθμίζεται σε COSMIC TOP SECRET.[68]

Φυσικά χαρακτηριστικά

Οι συσκευές TCE 621 B και C λειτουργούν σε θερμοκρασία 0 έως 40 °C και αποθηκεύονται σε περιβάλλον θερμοκρασίας -20 έως 70 °C. Καταναλώνουν μέση ενέργεια της τάξεως των 20 W και τροφοδοτούνται με ρεύμα 110VAC ή 230VAC. Μπορούν να τοποθετηθούν σε rack 19'', και έχουν διαστάσεις 440 x 250 x 44 mm (μήκος x πλάτος x ύψος). Το βάρος τους είναι 4,1 kg και πληρούν τις περιβαλλοντικές προδιαγραφές των προτύπων IEC 68-2 και DEF-STAN 07-55[69].

Επικοινωνιακές δυνατότητες

Οι κρυπτοσυσκευές TCE 621/B και C δημιουργούν VPN με τη χρήση του IPsec ESP. Υποστηρίζουν τα πρωτόκολλα επικοινωνίας IP (v4 και v6), UDP και SMTP (ίσως και περισσότερα, αλλά δεν αναφέρονται στο brochure της εταιρείας). Διαθέτουν και οι δύο, τόσο στην red όσο και στην black πλευρά, ethernet interfaces ταχύτητας 10/100 Mbit/s. Η TCE 621 C διαθέτει επιπλέον από μια gigabit ethernet interface στην red και στην black πλευρά. Η κρυπτοσυσκευή TCE 621/B προσφέρει ένα data rate της τάξης των 200 Mbit/s, ενώ η αντίστοιχη TCE 621/C προσφέρει data rate της τάξης των 600 Mbit/s. Η ταχύτητα μεταφοράς δεδομένων που προσφέρει είναι 200.000 πακέτα το δευτερόλεπτο, και το latency στο δίκτυο που χρησιμοποιεί αυτού του είδους τις κρυπτομηχανές, σύμφωνα με τον κατασκευαστή, είναι < 5 μs. Οι κρυπτοσυσκευές αυτές έχουν τη δυνατότητα υποστήριξης

---

[68] Thales TCE 621/B and TCE 621/C Cryptel®-IP High Capacity Encryption Devices [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/e9f5dce5-1e5f-49e2-b291-53557b604289/TCE-621-B-Product%20sheet

[69] p. 2

έως και 15.000 SAs, ενώ ο χρόνος που χρειάζεται για την εγκαθίδρυση της SA είναι μηδαμινός. Εκτός από την χειροκίνητη λειτουργία της κρυπτοσυσκευής, λειτουργίες όπως η αυτόματη δημιουργία των κλειδιών, η διανομή τους και η απομακρυσμένη διαχείριση όλων των κρυπτοσυσκευών στο δίκτυο μπορούν να επιτελεσθούν μέσω ενός κεντρικού συστήματος διαχείρισης, του TCE 671 SMC. Οι λειτουργίες του συστήματος διαχείρισης περιλαμβάνουν τη διαχείριση των κλειδιών, τη διαχείριση του ελέγχου πρόσβασης, την παρακολούθηση της ασφάλειας στο δίκτυο και διαχείριση των ρυθμίσεών του. Προκειμένου να υπάρχει μεγαλύτερη διαθεσιμότητα (δηλαδή για περιπτώσεις όπου για κάποιο λόγο η λειτουργία του κύριου SMC αποτυγχάνει), υπάρχει η δυνατότητα σύνδεσης στο δίκτυο πολλαπλών SMC σε διαμόρφωση master/slave. Εάν αποτύχουν όλα τα SMCs, υπάρχει πάντα η δυνατότητα της χειροκίνητης διαμόρφωσης των ρυθμίσεων και της εισαγωγής των κλειδιών. Σημαντικό είναι επίσης ότι οι κρυπτοσυσκευές αυτές υποστηρίζουν τη λειτουργία NAT, μέσω UDP ενθυλάκωσης των πακέτων, ενώ επίσης μπορούν να τεθούν σε λειτουργία στην οποία θα λαμβάνουν μόνο και δεν θα αποστέλλουν δεδομένα.[70]

Λογική ασφάλεια

Τόσο η κρυπτοσυσκευή TCE 621/B όσο και η C διατίθενται σε 3 διαφορετικές εκδόσεις, βάσει των αλγορίθμων κρυπτογράφησης που χρησιμοποιούν. Αυτές είναι:

- **NICE**, όπου εφαρμόζεται στα IPsec πακέτα ο απόρρητος και μη διαθέσιμος κρυπταλγόριθμος NICE, ο οποίος χρησιμοποιείται από το NATO. Βάσει αυτού, οι κρυπτοσυσκευές αυτές διαβαθμίζονται ως COSMIC TOP SECRET.

---

[70] Thales TCE 621/B and TCE 621/C Cryptel®-IP High Capacity Encryption Devices [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/e9f5dce5-1e5f-49e2-b291-53557b604289/TCE-621-B-Product%20sheet

- **AES**, όπου χρησιμοποιείται ο διαθέσιμος εμπορικά αλγόριθμος AES (μήκος κλειδιού 256 bits), τον οποίο, αν θέλει η εκάστοτε υπηρεσία που χρησιμοποιεί την κρυπτοσυσκευή, μπορεί να μεταβάλλει κατά την δική της βούληση. Βάσει αυτού, οι κρυπτοσυσκευές αυτές διαβαθμίζονται ως SECRET.
- **DUAL**, όπου διατίθενται και οι δύο παραπάνω επιλογές, και η επιλογή του αλγορίθμου γίνεται στην αρχική ρύθμιση της συσκευής.

Η εισαγωγή των κλειδών, όπως αναφέρθηκε και παραπάνω, γίνεται είτε χειροκίνητα μέσω του εμπρόσθιου πίνακα επιλογών είτε μέσω του κεντρικού συστήματος διαχείρισης. Επίσης, υπάρχουν δύο επίπεδα διαχείρισης της συσκευής και αυτό φαίνεται από το γεγονός ότι υπάρχουν δύο επίπεδα προστασίας με κωδικό[71].

Φυσική ασφάλεια

Από τις interfaces που παρέχονται από τη συσκευή, υπάρχουν interfaces που αναφέρονται ως “Red Network Interfaces” και όμοιες που αναφέρονται ως “Black Network Interfaces”. Επομένως, γίνεται εύκολα αντιληπτό ότι η αρχιτεκτονική της συσκευής είναι τύπου RED/BLACK, με τμήματα ασφαλούς και μη ασφαλούς δικτύου τα οποία διαχωρίζονται και χρησιμοποιούν ξεχωριστές διεπαφές. Επίσης, βάσει του κατασκευαστή, η κρυπτομηχανή διαθέτει πιστοποίηση TEMPEST βάσει του προτύπου SDIP-27, σε επίπεδο Α. Όσον αφορά την ηλεκτρομαγνητική ακτινοβολία που εκπέμπεται από τη συσκευή, σύμφωνα με τον κατασκευαστή, υπάρχει εναρμόνιση της συσκευής με την Οδηγία 89/336/ΕΟΚ του Συμβουλίου της 3ης Μαΐου 1989 για την προσέγγιση των νομοθεσιών των κρατών μελών σχετικά με την ηλεκτρομαγνητική συμβατότητα, και συμμόρφωση με

---

[71] Thales TCE 621/B and TCE 621/C Cryptel®-IP High Capacity Encryption Devices [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/e9f5dce5-1e5f-49e2-b291-53557b604289/TCE-621-B-Product%20sheet

την κατηγορία Class B του διεθνούς προτύπου EN 55022[72][73]. Όσον αφορά τα χαρακτηριστικά της επιχειρησιακής ασφάλειας της συσκευής, παρατηρείται ότι για να είναι επιχειρησιακή η κρυπτοσυσκευή, θα πρέπει να βρίσκεται σε αυτή το Crypto Ignition Key, το οποίο όσον αφορά τη συγκεκριμένη συσκευή παρέχεται σε τύπο Smart-card. Εάν το CIK απουσιάζει, η συσκευή δεν παρέχει καμία προστασία και άρα η διαβάθμιση που προσφέρει κατακερματίζεται. Επίσης, υπάρχει η δυνατότητα επείγουσας διαγραφής δεδομένων με ειδικό διακόπτη. Ο κατασκευαστής επίσης ισχυρίζεται πως η συσκευή παρέχει προστασία από φυσικές παραβιάσεις (tamper protection) χωρίς όμως να δίνονται επιμέρους λεπτομέρειες επί αυτού. Τέλος, οι διαθέσιμες interfaces της συσκευής αυτής για εισαγωγή κλειδών από ειδική συσκευή πλήρωσης είναι οι:

- DS-101 (πρότυπο RS-485), για συσκευές AN/CYZ-10

Σχήμα 7.4: Η συσκευή AN/CYZ-10 και η interface DS-101 [98,99]

---

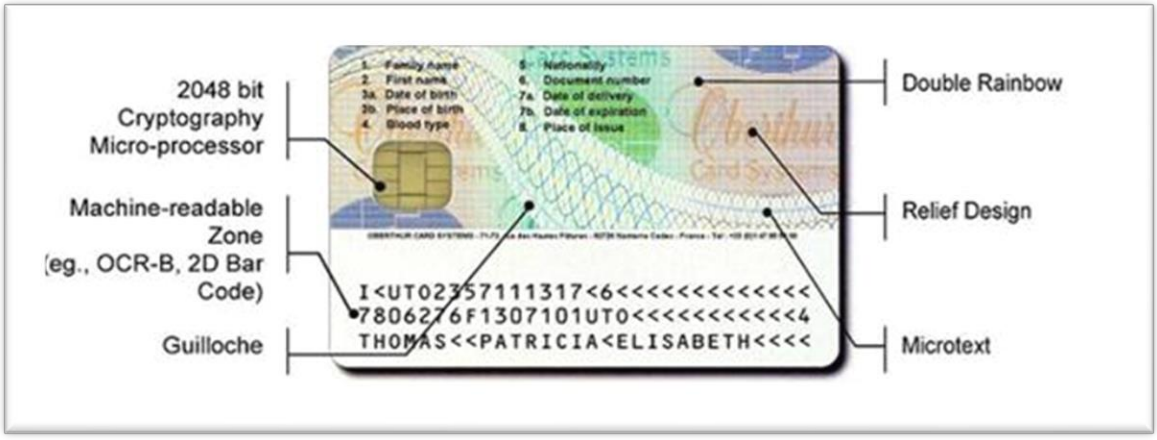
[72] Το πρότυπο EN 55022 αποτελεί ένα τροποποιημένο παράγωγο του προτύπου CISPR 22 από τη CENELEC, η οποία αποτελεί την Ευρωπαϊκή Επιτροπή Ηλεκτροτεχνικής Τυποποίησης. Το CISPR 22 αποτλεί πρότυπο CISPR για εξοπλισμό τεχνολογίας πληροφοριών όσον αφορά τα χαρακτηριστικά των ραδιοδιαταραχών και τις μεθόδους μέτρησής τους [38].

[73] Valavan, S., Texas Instruments. *Understanding electromagnetic compliance tests in digital isolators* (2014) [online] Available at https://www.tij.co.jp/jp/lit/wp/slyy064/slyy064.pdf (Accessed 13 Nov 2020)

- DS-102, για συσκευές KOI-18

Σχήμα 7.5: Η συσκευή KOI-18 [100]

- RS-232C (σειριακή θύρα)
- Smart Card interface (πρότυπο ISO 7816)



Σχήμα 7.6: ID-One PIV Smart Card [102]

Αξιοπιστία

Σύμφωνα με τον κατασκευαστή, έχει υπολογιστεί ότι η συσκευή παρέχει Mean Time To Failure (MTTF) μεγαλύτερο από 100.000 ώρες, και ο υπολογισμός αυτός έγινε βάσει του

προτύπου MIL-HDBK-217F, το οποίο είναι ένα στρατιωτικό πρότυπο που παρέχει δεδομένα ποσοστών αστοχίας για πολλά στρατιωτικά ηλεκτρονικά εξαρτήματα[74]. Το Mean Time To Failure (MTTF) υποδηλώνει τον αναμενόμενο χρόνο έως ότου ένα σύστημα επέλθει σε μη επισκευάσιμη κατάσταση[75].

Πιστοποιήσεις Common Criteria

Σε αυτού του τύπου τις κρυπτομηχανές δεν γίνεται γνωστές τυχόν πιστοποιήσεις CC ή παρόμοιες από τον κατασκευαστή.

7.5.2 Η κρυπτομηχανή CM-109 IP – Ιταλία

Η CM-109 IP είναι Ιταλικής προέλευσης, με κατασκευάστρια εταιρεία την Selenia Communications (Selex ES)[76].

---

[74] U.S. Department of Defense, (1991) Military Handbook, Reliability Prediction of Electronic Equipment (1991) [online] Available at http://www.mwftr.com/CS2/Mil-Hdbk-217F.pdf (Accessed 13 Nov 2020)

[75] Lienig, J., Bruemmer, H. (2017). Reliability Analysis. Fundamentals of Electronic Systems Design. Springer International Publishing. pp. 45–73

[76] Selenia Communications. *CM 109 IP Crypto Device* [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/e1d337b8-db92-4662-b95a-1c60041eed2a/CM-109-IP-Manufacturer's%20Brochure

Σχήμα 7.7: Η κρυπτομηχανή CM-109 IP της Selenia Communications [16]

Επίπεδο διαβάθμισης

Σύμφωνα με την NCI Agency, η CM-109 IP είναι διαβαθμισμένη με την μεγαλύτερη δυνατή διαβάθμιση, δηλαδή ως COSMIC TOP SECRET (CTS), καθώς μπορεί να υλοποιήσει κρυπτογράφηση είτε με τον αλγόριθμο AES-256 προσαρμοσμένο κατά το δοκούν του πελάτη, είτε με μυστικό αλγόριθμο του NATO είτε με customized αλγορίθμους εθνικής χρήσης που δεν είναι διαθέσιμοι στο εμπόριο. Το όνομα των αλγορίθμων NATO που οι κρυπτομηχανές υλοποιούν δεν γνωστοποιείται από τον κατασκευαστή [42, 44].

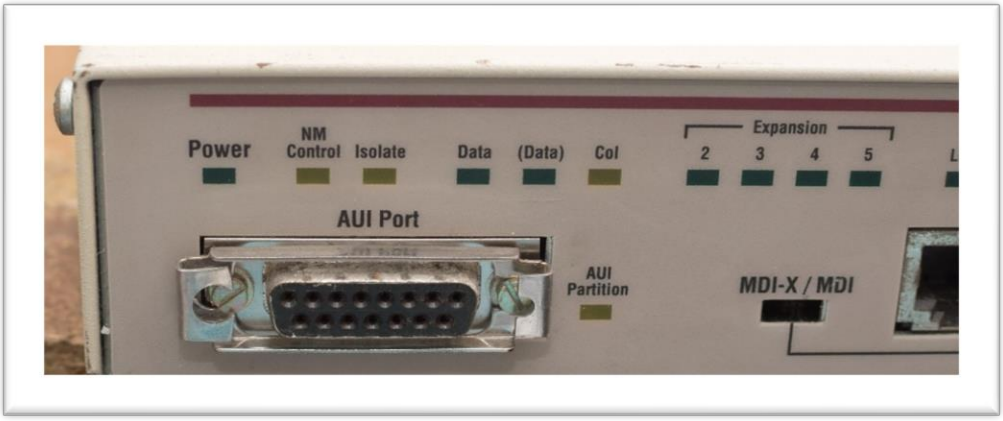
Φυσικά χαρακτηριστικά

Οι κρυπτοσυσκευές CM-109 IP λειτουργούν σε θερμοκρασία -10 °C έως 45 °C και αποθηκεύονται σε περιβάλλον θερμοκρασίας -40 έως 70 °C, γεγονός που τις καθιστά ελαφρώς πιο ανθεκτικές από τις αντίστοιχες TCE-621. Τροφοδοτούνται με τάση 115/220 VAC και έχουν μέγιστη κατανάλωση 60W. Έχουν διαστάσεις 448 x 395 x 92 mm (μήκος x πλάτος x ύψος), μέγεθος που τις καθιστά προσαρμόσιμες σε rack 19''. Το βάρος τους είναι 13 kg (CM-109 IP), σημαντικά βαρύτερες από τις αντίστοιχες TCE-621. Τέλος, η μέγιστη τιμή της σχετικής υγρασίας στην οποία η συσκευή μπορεί να παραμείνει λειτουργική είναι 90% στους 45 °C. [42, 44].

Επικοινωνιακές δυνατότητες

Η CM-109 IP δημιουργεί VPN σε tunnel mode με τη χρήση του IPsec ESP, όμως υπάρχει και η δυνατότητα υποστήριξης του AH. Υποστηρίζει τα πρωτόκολλα επικοινωνίας

IP (v4 και v6), ARP, ICMP, TCP, και UDP. Επίσης, υποστηρίζει στατική και δυναμική δρομολόγηση (OSPF, GRE). Υποστηρίζεται επίσης και η λειτουργία VRRP (Virtual Router Redundancy Protocol)[77]. Η CM-109 IP διαθέτει τόσο στην red όσο και στην black πλευρά, από μία Ethernet interface (UTP) τύπου 100Base-TX (υποστηρίζουν ταχύτητες έως και 100 Mbps) καθώς και από μία AUI (Attachment Unit Interface) ταχύτητας έως 10 Mbit/s. Για την φόρτωση των κλειδιών από ειδική συσκευή, υπάρχει και η αντίστοιχη DS-102 interface (για τις συσκευές FG-101 ή TR-101)[78].



Σχήμα 7.8: Παράδειγμα μίας AUI Interface (https://goughlui.com/wp-content/uploads/2013/09/DSC_0033.jpg)

[77] Το Virtual Router Redundancy Protocol (VRRP) είναι ένα πρωτόκολλο δικτύωσης υπολογιστών που παρέχει αυτόματη εκχώρηση διαθέσιμων δρομολογητών Internet Protocol (IP) σε συμμετέχοντες κεντρικούς υπολογιστές [44].

[78] Selex ES. IP Encryption System CM109IP and CM2000IP Families [online] Available at http://usa.selex-comms.com/internet/localization/IPC/media/docs/IP-ENCRYPTION-SYSTEM---CM109IP---CM-2000_selex.pdf [Accessed 16 Nov 2020].

Σχήμα 7.9: Οι συσκευές φόρτωσης κλειδιών FG-101 και TR-101 [44]

Το μέγιστο data rate της CM-109 IP είναι περίπου 100 Mbit/s (βάσει της απόδοσης των interfaces), ενώ δεν υπάρχουν άλλα διαθέσιμα δεδομένα από πλευράς απόδοσης, αλλά ούτε και για τον αριθμό των SAs που μπορεί η συσκευή να εγκαθιδρύσει ταυτόχρονα. Εκτός από την χειροκίνητη λειτουργία της κρυπτοσυσκευής, λειτουργίες όπως η αυτόματη δημιουργία των κλειδιών, η διανομή τους και η απομακρυσμένη διαχείριση όλων των κρυπτοσυσκευών στο δίκτυο μπορούν να επιτελεσθούν μέσω ενός κεντρικού συστήματος διαχείρισης, του KNMS 109IP. Το KNMS 109IP επιτρέπει την εύκολη διαχείριση του δικτύου συσκευών κρυπτογράφησης και την ηλεκτρονική διανομή κλειδιών μέσω κρυπτογραφημένου δικτύου διαχείρισης (ξεχωριστού δικτύου από το δίκτυο που πρόκειται να προστατευτεί, που χρησιμοποιείται μόνο για λειτουργίες διαχείρισης).

Λογική ασφάλεια

Οι αλγόριθμοι κρυπτογράφησης που μπορεί η CM-109 IP να εφαρμόσει στα IPsec πακέτα είναι οι εξής:

- **Μυστικός αλγόριθμος NATO,** όπου εφαρμόζεται στα IPsec πακέτα ένας απόρρητος και μη διαθέσιμος κρυπταλγόριθμος, ο οποίος χρησιμοποιείται από το NATO. Βάσει αυτού, οι κρυπτοσυσκευές αυτές διαβαθμίζονται ως COSMIC TOP SECRET.
- **Αλγόριθμος AES-256**, όπου χρησιμοποιείται ο διαθέσιμος εμπορικά αλγόριθμος AES (μήκος κλειδιού 256 bits), τον οποίο, αν θέλει η εκάστοτε υπηρεσία που χρησιμοποιεί την κρυπτοσυσκευή, μπορεί να μεταβάλλει κατά την δική της βούληση.

- **Άλλοι μυστικοί αλγόριθμοι (εθνικής χρήσης)**

Η εισαγωγή των κλειδών, όπως αναφέρθηκε και παραπάνω, γίνεται είτε μέσω του κεντρικού συστήματος διαχείρισης, είτε μέσω ειδικής συσκευής (tape reader ή fill gun). Υπάρχει επίσης η δυνατότητα διατήρησης των κλειδιών από διακοπή της τροφοδοσίας (τα κλειδιά παραμένουν ενεργά έως 6 μήνες). Η διαχείριση της συσκευής μπορεί να γίνει κι από τον εμπρόσθιο πίνακα (front panel). Άλλες δυνατότητες λογικής ασφάλειας της συσκευής είναι η καταγραφή ενεργειών και συμβάντων (logging) μέσω ειδικού λειτουργικού συστήματος, καθώς και η ύπαρξη συναγερμών (alarms), η φύση των οποίων δε γίνεται γνωστή από τον κατασκευαστή. Ενδιαφέρον στοιχείο αποτελεί ότι ο κατασκευαστής κάνει λόγο για λειτουργία anti-replay, όπου στην ουσία τονίζει τη δυνατότητα της κρυπτοσυσκευής για παροχή προστασίας από replay attacks.

Φυσική ασφάλεια

Οι παραπάνω αλγόριθμοι βρίσκονται εντός αφαιρούμενης ειδικής μονάδας (module) η οποία αποτελεί μέρος της κρυπτομηχανής και της επιτρέπει να αλλάζει εύκολα αλγόριθμο (με άλλους τυποποιημένους ή προσαρμόσιμους αλγόριθμους). Χωρίς τη μονάδα αυτή, η CM-109 δεν μπορεί να κρυπτογραφήσει τα δεδομένα. Στις network interfaces, γίνεται αναφορά σε “Red side” και “Black side”. Έτσι, γίνεται αντιληπτό ότι η αρχιτεκτονική της συσκευής είναι τύπου RED/BLACK, με τμήματα ασφαλούς και μη ασφαλούς δικτύου τα οποία διαχωρίζονται και χρησιμοποιούν ξεχωριστές διεπαφές. Σύμφωνα με τον κατασκευαστή, η κρυπτομηχανή διαθέτει δυνατότητα αυτοελέγχου μέσω εξοπλισμού BITE (Built-In Test Equipment), που αποτελεί δευτερεύοντα εξοπλισμό ο οποίος *εκτελεί διεξοδικό αυτοέλεγχο για την ανίχνευση της παρουσίας σφαλμάτων υλικού και απομονώνει οποιοδήποτε σφάλμα σε μια μονάδα η οποία μπορεί να αντικατασταθεί*[79]. Επίσης, βάσει

[79] Evaluation Engineering. *What Is Built-In Self Test And Why Do We Need It?* (1996) [online] Available at https://www.evaluationengineering.com/home/article/13000382/what-is-builtin-self-test-and-why-do-we-need-it [Accessed 16 Nov 2020].

του κατασκευαστή, η κρυπτομηχανή διαθέτει πιστοποίηση TEMPEST βάσει του προτύπου AMSG-720B, το οποίο είναι το αντίστοιχο του Level A του προτύπου SDIP-27 (Σχήμα 7.2), οπότε παρέχει την καλύτερη TEMPEST προστασία. Όσον αφορά την ηλεκτρομαγνητική ακτινοβολία που εκπέμπεται από τη συσκευή, σύμφωνα με τον κατασκευαστή, η συσκευή έχει κατασκευαστεί κατά τα πρότυπα MIL-STD-461 και MIL-STD-462[80]. Όσον αφορά τα χαρακτηριστικά της επιχειρησιακής ασφάλειας της συσκευής, παρατηρείται ότι για να είναι επιχειρησιακή η κρυπτοσυσκευή, θα πρέπει να εισαχθεί σε αυτή ένα PIN εκκίνησης (δεν χρησιμοποιείται CIK). Επίσης, υπάρχει η δυνατότητα επείγουσας διαγραφής δεδομένων με ειδικό διακόπτη. Ο κατασκευαστής επίσης ισχυρίζεται πως η συσκευή παρέχει λειτουργία προστασίας από φυσικές παραβιάσεις (anti-tampering function) χωρίς όμως να δίνονται επιμέρους λεπτομέρειες επί αυτού. Τέλος, οι διαθέσιμες interfaces της συσκευής αυτής για εισαγωγή κλειδών από ειδική συσκευή πλήρωσης είναι οι DS-102, για συσκευές FG-101 και TR-101.

Αξιοπιστία

Δεν διατίθενται πληροφορίες του κατασκευαστή για τυχόν MTBF ή MTTF testing.

Πιστοποιήσεις Common Criteria

Δεν διατίθενται πληροφορίες του κατασκευαστή για τυχόν πιστοποιήσεις CC ή αντίστοιχες ισοδύναμες.

---

[80] Τα πρότυπα MIL-STD-461 και MIL-STD-462 αποτελούν ευρέως αποδεκτά στρατιωτικά πρότυπα των Ηνωμένων Πολιτειών που καθορίζουν τις απαιτήσεις ηλεκτρομαγνητικής συμβατότητας ηλεκτρονικού, ηλεκτρικού και ηλεκτρομηχανικού εξοπλισμού και υποσυστημάτων που έχουν σχεδιαστεί ή προμηθεύεται για χρήση από δραστηριότητες και υπηρεσίες του Υπουργείου Άμυνας (DoD) των Ηνωμένων Πολιτειών. Οι συσκευές που συμμορφώνονται με τα πρότυπα αυτά συμμορφώνονται με τις απαιτήσεις ακτινοβολίας εκπομπών σε συσκευές στρατιωτικών προδιαγραφών [45][46][47].

7.5.3 Η κρυπτομηχανή EP430GN – Ισπανία

Η EP430GN είναι Ισπανικής προέλευσης, με κατασκευάστρια εταιρεία την DF Epicom[81].

Σχήμα 7.10: Η κρυπτομηχανή EP430GN [50]

Επίπεδο διαβάθμισης

Σύμφωνα με την NCI Agency, η EP430GN είναι διαβαθμισμένη ως NATO SECRET. Η συσχέτιση της διαβάθμισης της κρυπτομηχανής με τον αλγόριθμο κρυπτογράφησης δεν είναι δυνατή σε αυτή την περίπτωση, καθώς οι λεπτομέρειες των αλγορίθμων κρυπτογράφησης που υλοποιεί αυτή η συσκευή δεν γίνονται γνωστές [49].

Φυσικά χαρακτηριστικά

Οι κρυπτοσυσκευές EP430GN λειτουργούν σε θερμοκρασία 0 °C έως 50 °C και αποθηκεύονται σε περιβάλλον θερμοκρασίας -30 έως 65 °C. Τροφοδοτούνται με τάση 100/240 VAC. Η σχετική υγρασία στην οποία παραμένουν λειτουργικές είναι από 5 έως 95%. Οι διαστάσεις τους δεν αναφέρονται από τον κατασκευαστή, αλλά παρόλα αυτά ο κατασκευαστής δηλώνει ότι είναι προσαρμόσιμες σε rack 19'' [50].

---

81 DF Epicom. *EP430GN. IP Encryption Unit for NATO networks protection* [online] Available at https://www.zsis.hr/UserDocsImages/Sigurnost/pdfs/EP430GN.pdf [Accessed 16 Nov 2020].

Επικοινωνιακές δυνατότητες

Η CM-109 IP δημιουργεί VPN σε tunnel mode με τη χρήση του IPsec ESP. Λεπτομέρειες για τα πρωτόκολλα επικοινωνίας που υποστηρίζει, πέρα από τα πρωτόκολλα IP και UDP, δεν γίνονται γνωστές. Παρόλα αυτά, η κρυπτομηχανή υποστηρίζει στατική και δυναμική δρομολόγηση (OSPF, RIP), καθώς και DHCP. Όσον αφορά τις interfaces, η κρυπτομηχανή υποστηρίζει Gigabit Ethernet μέσω οπτικής ίνας (1000 Base SX) η οποία είναι κατάλληλη για μετάδοση δεδομένων σε μεγάλες αποστάσεις. Λεπτομέρειες για τον αριθμό των interfaces ή για άλλους τύπους interfaces, δεν γίνονται γνωστές. Η δικτυακή απόδοση (throughput) της κρυπτομηχανής κυμαίνεται στα 2 Gbps, λόγω των Gigabit Ethernet interfaces. Μία σημαντική διαφορά από τις κρυπτομηχανές που έχουμε ήδη εξετάσει είναι ότι δεν διαθέτει τη δυνατότητα μη-κρυπτογράφησης (null encryption), καθώς πρέπει πάντα να εφαρμόζει αλγόριθμο κρυπτογράφησης στα IPsec πακέτα. Ένα ακόμη στοιχείο αποτελεί ότι μπορεί να εγκαθιδρύσει ταυτόχρονα 1000 SAs. Επίσης, ενδιαφέρον αποτελεί το γεγονός ότι η διαχείριση της κρυπτοσυσκευής (ρύθμιση των υποδικτύων της “red” και “black” interface) γίνεται με φυσική πρόσβαση στην κρυπτοσυσκευή, μέσω θύρας console στον εμπρόσθιο πίνακα [68]. Αυτό δείχνει ότι δεν υπάρχει η δυνατότητα χρήσης κεντρικού συστήματος διαχείρισης των κρυπτοσυσκευών αυτών.

Λογική ασφάλεια

Λεπτομέρειες γύρω από τους αλγόριθμους κρυπτογράφησης που χρησιμοποιεί η συσκευή δεν γίνονται γνωστές. Και στη συγκεκριμένη περίπτωση, ο κατασκευαστής αναφέρει ότι η συσκευή παρέχει προστασία από replay attacks και άλλες παρόμοιες επιθέσεις. Η κρυπτομηχανή επίσης διαθέτει ένα σύστημα ελέγχου πρόσβασης που βασίζεται σε προφίλ δικαιωμάτων που καθορίζουν ενέργειες που επιτρέπονται σε συγκεκριμένο χρήστη. Ο χρήστης πρέπει να πιστοποιηθεί χρησιμοποιώντας μια ειδικά προγραμματισμένη συσκευή πλήρωσης που κι αυτή ενεργοποιείται από έναν κωδικό πρόσβασης. Σημαντικό στοιχείο αποτελεί επίσης ότι γίνεται έλεγχος ταυτότητας του λογισμικού σε κάθε εκκίνηση, που συντελεί στο να προλαμβάνονται καταστάσεις στις οποίες το λογισμικό της κρυπτο-

συσκευής έχει υποστεί αλλοιώσεις. Επίσης, γίνεται αναφορά σε δυνατότητα της κρυπτοσυσκευής για καταγραφή αρχείου συναγερμών, που δείχνει ότι υπάρχει η δυνατότητα της κρυπτοσυσκευής για logging.

Φυσική ασφάλεια

Ο κατασκευαστής ισχυρίζεται πως η συσκευή είναι σχεδιασμένη έτσι ώστε να διαθέτει μηχανισμούς προστασίας από φυσικές παραβιάσεις (antitamper mechanisms) οι οποίοι αξιολογούνται ως Level 4 από το πρότυπο FIPS 140-2[82]. Επίσης, βάσει του κατασκευαστή, η κρυπτομηχανή διαθέτει πιστοποίηση TEMPEST Level A βάσει του προτύπου SDIP-27 (Σχήμα 7.2), οπότε παρέχει την καλύτερη TEMPEST προστασία. Η κρυπτοσυσκευή παρέχει επίσης τη δυνατότητα επείγουσας διαγραφής δεδομένων με ειδικό κομβίο το οποίο βρίσκεται στον εμπρόσθιο πίνακα. Η αναφορά στις “Red side” και “Black side” εδώ γίνεται στον τρόπο ρύθμισης της κρυπτομηχανής, καθώς αναφέρεται ότι οι δύο πλευρές (δηλαδή τα υποδίκτυά τους) μπορούν να ρυθμιστούν μέσω ανεξάρτητης console port. Έτσι, γίνεται αντιληπτό ότι η αρχιτεκτονική της συσκευής είναι τύπου RED/BLACK. Όσον

---

[82] Το Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφοριών 140-2, (FIPS PUB 140-2), είναι ένα πρότυπο ασφάλειας υπολογιστών της κυβέρνησης των ΗΠΑ που χρησιμοποιείται για την έγκριση κρυπτοϋλικών. Το FIPS 140-2 καθορίζει τέσσερα επίπεδα ασφάλειας: Level 1, όπου το κρυπτοϋλικό παρέχει το χαμηλότερο επίπεδο ασφάλειας και καθορίζονται μόνο οι βασικές απαιτήσεις ασφαλείας, Level 2, το οποίο απαιτεί πρόσθετες λειτουργίες που δείχνουν στοιχεία παραβίασης, συμπεριλαμβανομένων ταινιών ή σφραγίδων που πρέπει να παραβιασθούν για να επιτευχθεί φυσική πρόσβαση στα κρυπτογραφικά κλειδιά και τις κρίσιμες παραμέτρους ασφαλείας (CSP) εντός του υλικού, Level 3, το οποίο πλέον των προηγούμενων επιχειρεί να εμποδίσει τον εισβολέα να αποκτήσει πρόσβαση στις CSP που διατηρούνται εντός της κρυπτογραφικής μονάδας με μηχανισμούς φυσικής ασφάλειας που μπορεί να περιλαμβάνουν τη χρήση ισχυρών περιβλημάτων και κυκλώματος ανίχνευσης παραβίασης που μηδενίζει όλα τα CSP όταν ανοίγουν τα αφαιρούμενα καλύμματα / θύρες του υλικού, και Level 4, στο οποίο οι μηχανισμοί φυσικής ασφάλειας παρέχουν ένα πλήρες προστατευτικό περίβλημα γύρω από την κρυπτογραφική μονάδα με σκοπό την ανίχνευση και την απόκριση σε όλες τις μη εξουσιοδοτημένες προσπάθειες φυσικής πρόσβασης. Η διείσδυση του περιβλήματος κρυπτογραφικής μονάδας από οποιαδήποτε κατεύθυνση έχει πολύ υψηλή πιθανότητα ανίχνευσης, με αποτέλεσμα την άμεση διαγραφή όλων των CSP [51].

αφορά την ηλεκτρομαγνητική ακτινοβολία που εκπέμπεται από τη συσκευή, λεπτομέρειες δεν γίνονται γνωστές. Τέλος, όσον αφορά τα χαρακτηριστικά της επιχειρησιακής ασφάλειας της συσκευής, παρατηρείται ότι δεν απαιτείται PIN ή CIK για να είναι επιχειρησιακή η κρυπτοσυσκευή, όμως κάτι που δεν έχουμε παρατηρήσει στις προηγούμενες περιπτώσεις είναι ότι η συσκευή αυτή έχει τη δυνατότητα να αποκλείσει τη συσκευή πλήρωσης εάν ανιχνευτεί ότι δεν έχει υλοποιηθεί σωστά η διαδικασία πιστοποίησης του χρήστη από αυτή [50]. Αυτό σημαίνει ότι μόνο όποιος έχει πιστοποιηθεί από τη συσκευή πλήρωσης μπορεί να επέμβει στην κρυπτομηχανή.

Αξιοπιστία

Σύμφωνα με τον κατασκευαστή, η συσκευή μπορεί να λειτουργήσει αξιόπιστα 24 ώρες το 24ωρο, χωρίς όμως να δίνονται στοιχεία τιμών MTBF/MTTF [50].

Πιστοποιήσεις Common Criteria

Σε αυτή την περίπτωση βλέπουμε ότι η κρυπτομηχανή αυτή έχει λάβει πιστοποίηση Common Criteria ως EAL4+. Αυτό σημαίνει ότι το Target Of Evaluation (δηλαδή η κρυπτομηχανή) έχει σχεδιαστεί μεθοδικά, έχει δοκιμαστεί και έχει αναθεωρηθεί.

7.5.4 Η κρυπτομηχανή KG-250 – Ηνωμένες Πολιτείες

Η Altasec KG-250 είναι Αμερικανικής προέλευσης, με κατασκευάστρια εταιρεία την ViaSat[83].

---

[83] ViaSat. *Altasec KG-250 HAIPE IP Network Encryptor (2012)* [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/9d1ff17e-cc97-4709-95cb-400588bcaf80/AltaSec-KG-250-Product%20Sheet [Accessed 18 Nov 20]

Σχήμα 7.11: Η κρυπτομηχανή KG-250 [52]

Επίπεδο διαβάθμισης

Σύμφωνα με την NCI Agency, η Altasec KG-250 είναι διαβαθμισμένη με την μεγαλύτερη δυνατή διαβάθμιση, δηλαδή ως COSMIC TOP SECRET (CTS). Όπως θα δούμε παρακάτω, η συσκευή μπορεί να προσφέρει κρυπτογράφηση με μυστικό αλγόριθμο, εγκεκριμένο από την National Security Authority (NSA) των Ηνωμένων Πολιτειών, καθώς και με εμπορικούς αλγορίθμους[84].

Φυσικά χαρακτηριστικά

Οι κρυπτοσυσκευές EP430GN λειτουργούν σε θερμοκρασία 0 °C έως 50 °C και αποθηκεύονται σε περιβάλλον θερμοκρασίας -20 έως 70 °C. Η σχετική υγρασία στην οποία παραμένουν λειτουργικές είναι 95% στους 60°C για 96 ώρες. Τροφοδοτούνται με τάση +5/+3,3 VDC. Έχουν διαστάσεις 302,2 x 190.5 x 42,7 mm (μήκος x πλάτος x ύψος), μέγεθος που τις καθιστά προσαρμόσιμες σε rack 19''. Το βάρος τους είναι 2,9 kg. Συμπε-

[84] NCI Agency. NIAPC. AltaSec KG-250 [online] Available at https://www.ia.nato.int/niapc/Product/AltaSec-KG-250_304 [Accessed 18 Nov 20].

ραίνεται από τα παραπάνω ότι η συγκεκριμένη κρυπτοσυσκευή είναι ως τώρα η μικρότερη σε διαστάσεις και βάρος, ωστόσο λειτουργεί με συνεχές ρεύμα. Επίσης, η συσκευή συμμορφώνεται με το κατασκευαστικό πρότυπο MIL-STD-810F[85] [52].

Επικοινωνιακές δυνατότητες

Η KG-250 σύμφωνα με τον κατασκευαστή αποτελεί συσκευή HAIPE (High Assurance Internet Protocol Encryptor). Ο όρος HAIPE αποτελεί προδιαγραφή η οποία ορίζεται από την NSA για να αποδώσει μια συσκευή ως συσκευή κρυπτογράφησης στο επίπεδο IP[86]. Οι συσκευές HAIPE γενικά υλοποιούν IPsec VPN με τη χρήση των πρωτοκόλλων IKE και ESP [55]. Τα πρωτόκολλα επικοινωνίας που μπορεί η συσκευή να υποστηρίξει είναι σύμφωνα με τον κατασκευαστή τα TCP, UDP, ICMP, IGMP, ARP, και DHCP. Η κρυπτοσυσκευή επίσης υποστηρίζει δυναμική δρομολόγηση μέσω OSPF (για την red πλευρά μόνο), καθώς και GRE tunneling. Όσον αφορά τις interfaces, η κρυπτομηχανή υποστηρίζει από μία Ethernet interface σε κάθε πλευρά (RED/BLACK) της τάξεως των 10/100 Mbps, και μπορεί να υποστηρίξει ταχύτητες έως 100 Mbps σε full duplex (200 Mbps συνολικά). Επίσης, διαθέτει και μία interface DS-101 για την εισαγωγή κλειδιών από ειδική συσκευή πλήρωσης. Σημαντικό στοιχείο αποτελεί ότι η συγκεκριμένη συσκευή μπορεί να υποστηρίξει και εικονικά τοπικά δίκτυα (VLANs). Ο κατασκευαστής εδώ δεν δίνει στοιχεία

---

[85] Το πρότυπο MIL-STD-810F είναι ένα Στρατιωτικό Πρότυπο των Ηνωμένων Πολιτειών που αφορά εργαστηριακές δοκιμές των ορίων δοκιμής ενός εξοπλισμού στις συνθήκες που θα βιώσει καθ 'όλη τη διάρκεια ζωής του [76].

[86] *Η HAIPE (High Assurance Protocol Encryptor) είναι μια προγραμματιζόμενη συσκευή ασφάλειας πληροφοριών IP (INFOSEC) με δυνατότητες προστασίας κυκλοφορίας, δικτύωσης και διαχείρισης που παρέχει υπηρεσίες διασφάλισης πληροφοριών για δίκτυα IPv4 και IPv6. Η συσκευή HAIPE έχει σχεδιαστεί για να παρέχει υπηρεσίες εμπιστευτικότητας, ακεραιότητας και ελέγχου ταυτότητας για την κυκλοφορία IP για εφαρμογές αναπτυσσόμενων και σταθερών δικτύων. Το HAIPE επιτρέπει την ασφαλή μετάδοση σε WAN μέσω κρυπτογράφησης πακέτων IP σε συμβατές συσκευές ασφαλείας στο δίκτυο προορισμού όπου πραγματοποιείται η αποκρυπτογράφηση* [54].

για τον αριθμό των ταυτόχρονων SAs που μπορούν να εγκαθιδρυθούν. Τέλος, όσον αφορά τη διαχείριση της κρυπτοσυσκευής, αυτή μπορεί να γίνει είτε με φυσική πρόσβαση στην κρυπτοσυσκευή, είτε με τη χρήση ενός κεντρικού συστήματος διαχείρισης, του VINE Manager, το οποίο χρησιμοποιεί τα πρωτόκολλα SNMP και HTTPS για τη διαχείριση του δικτύου [52]. Αυτό είναι πιθανό να σημαίνει ότι δε χρησιμοποιείται ξεχωριστό κρυπτογραφημένο δίκτυο IPsec από την εφαρμογή διαχείρισης, χωρίς ωστόσο κάτι τέτοιο να αναφέρεται ρητά.

Λογική ασφάλεια

Παρατηρείται ότι η συσκευή είναι πιστοποιημένη από την NSA ως τύπου 1 (Type 1). Γενικά, η NSA κατατάσσει κρυπτογραφικά προϊόντα ή αλγόριθμους ως τύπου 1, 2, 3 ή 4. Οι τύποι προϊόντων ορίζονται στο Εθνικό Γλωσσάρι Διασφάλισης Πληροφοριών, όπου ως τύπου 1 ορίζεται *ο κρυπτογραφικός εξοπλισμός που έχει ταξινομηθεί ή πιστοποιηθεί από την NSA για κρυπτογράφηση και αποκρυπτογράφηση διαβαθμισμένων και ευαίσθητων πληροφοριών εθνικής ασφάλειας (με προϋπόθεση να έχει εξοπλιστεί με τα απαραίτητα κρυπτογραφικά κλειδιά)*, *ο οποίος αναπτύχθηκε χρησιμοποιώντας τις διαδικασίες ανάπτυξης της NSA, χρησιμοποιεί εγκεκριμένους από την NSA αλγόριθμους, και χρησιμοποιείται για την προστασία συστημάτων που απαιτούν τους πιο αυστηρούς μηχανισμούς προστασίας*[87]*.* Επίσης, αναφέρεται από τον κατασκευαστή ότι οι αλγόριθμοι κρυπτογράφησης είναι Τύπου 1 Suite A και Τύπου 1 Suite B. Οι Suites A και B αποτελούν ταξινομημένα από την NSA σύνολα κρυπτογραφικών μεθόδων (αλγορίθμων), η διαφορά των οποίων επίκειται στο ότι οι μέθοδοι της Suite A είναι μυστικοί και μη διαθέσιμοι στο εμπόριο, σε αντίθεση με αυτούς της Suite B, που αποτελεί στην ουσία μία διαλειτουργική κρυπτογραφική βάση τόσο για μη διαβαθμισμένες όσο και για διαβαθμισμένες πληροφορίες. Επομένως, ο αριθμός των συσκευών που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους της Suite A πρέπει να είναι περιορισμένος, γιατί εκτός από τη συσκευή θα πρέπει να έχει

---

87 Committee on National Security Systems (CNSS), 2010. National Information Assurance Glossary. CNSS Instruction No. 4009, p. 78-79.

προβλεφθεί προστασία και για τον αλγόριθμο [57]. Οι αλγόριθμοι Τύπου 1 της Suite A περιλαμβάνουν μεταξύ άλλων τους Accordian, Firefly, Medley, Saville, Walburn [58]. Η Suite B, η οποία έχει πλέον αντικατασταθεί από την NSA με την Commercial National Security Algorithm Suite[88] [61], περιελάμβανε τους εξής αλγορίθμους:

- Advanced Encryption Standard (AES-128 και AES-256)
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Elliptic Curve Diffie-Helman (ECDH)
- Secure Hash-Algorithm 2 (SHA-256 και SHA-384) [59][60].

Από το 2003, ο AES-256 ανήκει στην κατηγορία των αλγορίθμων Τύπου 1.[89] Έτσι, συμπεραίνεται ότι η κρυπτομηχανή μπορεί να υλοποιήσει κρυπτογράφηση με αλγορίθμους AES-256 (Type 1 Suite B) και λοιπούς μυστικούς Type 1 Suite A αλγορίθμους, οι οποίοι δεν είναι διαθέσιμοι στο εμπόριο. Ένας εκ των αλγορίθμων Type 1 της Suite A που υλοποιεί η συσκευή, σύμφωνα με τον κατασκευαστή, είναι ο Firefly, ο οποίος χρησιμοποιείται για δημιουργία κλειδιών [52]. Από τα παραπάνω γίνεται κατανοητή και η διαβάθμιση της συσκευής στον NIAPC από την NCI Agency ως COSMIC TOP SECRET. Η εισαγωγή των κλειδιών στην συσκευή μπορεί να γίνει απομακρυσμένα από οποιαδήποτε κρυπτομηχανή ίδιου τύπου (remote HAIPE-to-HAIPE keying) μέσω του VINE manager ή τοπικά.

---

[88] Η Commercial National Security Algorithm (CNSA) Suite είναι ένα σύνολο κρυπτογραφικών αλγορίθμων που δημοσιεύθηκαν από NSA προς αντικατάσταση των αλγορίθμων της NSA Suite B. Χρησιμεύει ως κρυπτογραφική βάση για την προστασία των πληροφοριών των Εθνικών Συστημάτων Ασφαλείας των ΗΠΑ μέχρι το υψηλότερο επίπεδο μυστικότητας (top secret). Η διαφορά με την Suite B είναι ότι χρησιμοποιούνται συγκεκριμένα μήκη κλειδιών προκειμένου να παρέχεται η ύψιστη ασφάλεια (AES-256, ECDH-P-384, ECDSA-P-384, SHA-384, Diffie-Hellman με 3072-bit modulus, RSA με 3072-bit modulus) [62][63][64]

[89] Committee on National Security Systems (CNSS), 2003. National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information [online] Available at https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/cnss15fs.pdf [Accessed 19 Nov 2020].

Δεν αναφέρονται στοιχεία ως προς τα προφίλ δικαιωμάτων διαχείρισης της συσκευής ή τις δυνατότητές της για καταγραφή ενεργειών (logging) [52].

Φυσική ασφάλεια

Ο κατασκευαστής αναφέρει ότι η αρχιτεκτονική της συσκευής είναι modular και μπορεί να επαναπρογραμματίζεται εύκολα. Επίσης, αναφέρει ότι η κρυπτογράφηση (encryption) είναι επαναπρογραμματίσιμη (programmable). Τα παραπάνω μπορεί να σημαίνουν ότι υπάρχει αφαιρούμενη ειδική μονάδα (module) με τους αλγορίθμους κρυπτογράφησης, όπως και με τη CM-109, χωρίς όμως αυτό να αναφέρεται ρητά. Στις network interfaces, γίνεται αναφορά σε “Red data” και “Black data”. Έτσι, γίνεται αντιληπτό ότι η αρχιτεκτονική της συσκευής είναι τύπου RED/BLACK, με τμήματα ασφαλούς και μη ασφαλούς δικτύου τα οποία διαχωρίζονται και χρησιμοποιούν ξεχωριστές διεπαφές. Σύμφωνα με τον κατασκευαστή, η κρυπτομηχανή διαθέτει δυνατότητα αυτοελέγχου BIT (Built-In Test), όπως και η CM-109. Επίσης, βάσει του κατασκευαστή, η κρυπτομηχανή διαθέτει πιστοποίηση TEMPEST βάσει του προτύπου NSTISSAM 1/92, το οποίο είναι το αντίστοιχο του προτύπου SDIP-27 (Σχήμα 7.2), χωρίς όμως να αναφέρεται το επίπεδο προστασίας TEMPEST που παρέχει. Όσον αφορά την ηλεκτρομαγνητική ακτινοβολία που εκπέμπεται από τη συσκευή, σύμφωνα με τον κατασκευαστή, η συσκευή έχει κατασκευαστεί με συμμόρφωση ως προς το επίπεδο B (Class B) του διεθνούς προτύπου EN 55022 (όπως και η TCE 621) και ως προς το επίπεδο B (Class B) της Ομοσπονδιακής Επιτροπής Επικοινωνιών (Federal Communications Commission – FCC)[90]. Όσον αφορά τα χαρακτηριστικά της επιχειρησιακής ασφάλειας της συσκευής, παρατηρείται ότι για να είναι επιχειρησιακή η κρυπτοσυσκευή, θα πρέπει να έχει εισαχθεί σε αυτή το CIK, όπως και με την TCE 621.

---

[90] Η Ομοσπονδιακή Επιτροπή Επικοινωνιών (FCC) είναι μια ανεξάρτητη υπηρεσία της κυβέρνησης των Ηνωμένων Πολιτειών που ρυθμίζει τις επικοινωνίες μέσω ραδιοφώνου, τηλεόρασης, καλωδίου, δορυφόρου και καλωδίου σε όλες τις Ηνωμένες Πολιτείες. Η FCC διατηρεί τη δικαιοδοσία για τους τομείς της ευρυζωνικής πρόσβασης, της χρήσης ραδιοσυχνοτήτων, της ευθύνης των μέσων μαζικής ενημέρωσης, της δημόσιας ασφάλειας και της εσωτερικής ασφάλειας [66].

Λεπτομέρειες σχετικά με δυνατότητες της συσκευής για προστασία από φυσικές παραβιάσεις ή για τυχόν δυνατότητα επείγουσας διαγραφής δεν αναφέρονται από τον κατασκευαστή. Τέλος, υπάρχει μία διαθέσιμη interface DS-101 στη συσκευή αυτή για εισαγωγή κλειδών από ειδική συσκευή πλήρωσης [52].

Αξιοπιστία

Όσον αφορά τα στοιχεία αξιοπιστίας της συσκευής, ο κατασκευαστής αναφέρει ότι έχει προβλεφθεί για τη συσκευή αυτή MTBF 312,000 ωρών, και το προβλεπόμενο Mean Time To Recover (MTTR) αντιστοιχεί σε 15 λεπτά [52].

Πιστοποιήσεις Common Criteria

Για τη συσκευή αυτή δεν αναφέρεται κάποια CC πιστοποίηση. Παρόλα αυτά, αναφέρεται ότι είναι πιστοποιημένη ως Type 1 από την NSA, που την καθιστά διαβαθμισμένη ως TOP SECRET (αντίστοιχο του COSMIC TOP SECRET για το NATO). Επίσης, αναφέρεται ότι είναι πιστοποιημένη από την Joint Interoperability Test Command (JITC) [67], η οποία αποτελεί τμήμα του Υπουργείου Άμυνας των ΗΠΑ και αποστολή του οποίου είναι η δοκιμή και η πιστοποίηση της διαλειτουργικότητας των προϊόντων τεχνολογίας πληροφοριών του Υπουργείου Άμυνας. Αυτό σημαίνει ότι η συσκευή παρέχει διαλειτουργικότητα με όλους τους κλάδους του Υπουργείου Άμυνας (π.χ Στρατό Ξηράς, Αεροπορία, κ.α) [66].

7.5.5 Οι κρυπτομηχανές Mini-CATAPAN – Αγγλία

Οι Mini-CATAPAN είναι Αγγλικής προέλευσης και κατασκευάζονται από την L3 TRL Technology [68].

Σχήμα 7.12: Η κρυπτομηχανή Mini-CATAPAN [68]

Επίπεδο διαβάθμισης

Υπάρχουν δύο διαθέσιμες εκδόσεις της Mini-CATAPAN, η Suite A και η Suite B. Σύμφωνα με την NCI Agency, η Mini-CATAPAN Suite A είναι διαβαθμισμένη με την μεγαλύτερη δυνατή διαβάθμιση, δηλαδή ως COSMIC TOP SECRET (CTS), ενώ η αντίστοιχη Suite B είναι διαβαθμισμένη ως NATO SECRET (NS) [68]. Έτσι φαίνεται πως η NCI Agency, όπως και στην περίπτωση της TCE 621, θεωρεί την Suite A, με βάση και όσα αναφέρθηκαν στην περίπτωση της KG-250, δυνατότερης διαβάθμισης. Οι αλγόριθμοι που υλοποιούνται από τις κρυπτομηχανές δεν γνωστοποιούνται από τον κατασκευαστή [69][70].

Φυσικά χαρακτηριστικά

Οι κρυπτοσυσκευές Mini-CATAPAN λειτουργούν σε θερμοκρασία 0 °C έως 50 °C. Τροφοδοτούνται με τάση 9 – 28 VDC. Η κατανάλωση ρεύματός τους είναι μικρότερη των 10

W. Έχουν διαστάσεις 155 x 93 x 27 mm (μήκος x πλάτος x ύψος), μέγεθος που τις καθιστά προσαρμόσιμες σε rack 19’’. Το βάρος τους είναι 5,66 kg. [69][70].

Επικοινωνιακές δυνατότητες

Οι κρυπτοσυσκευές Mini-CATAPAN υποστηρίζουν τα πρωτόκολλα επικοινωνίας IP, ATM και SNMPv3, χωρίς να δίνονται όμως λεπτομέρειες για τα υπόλοιπα πρωτόκολλα που τυχόν υποστηρίζει. Διαθέτουν και οι δύο, τόσο στην CT(cipher-text) όσο και στην PT(plaintext) πλευρά, Ethernet interfaces ταχύτητας 10/100 Mbit/s. Η κρυπτοσυσκευή TCE 621/B προσφέρει επομένως throughput της τάξης των 100 Mbit/s. Δεν δίνονται τιμές για το latency στο δίκτυο, όμως σύμφωνα με τον κατασκευαστή, το latency είναι αμελητέο. Δεν δίνονται λεπτομέρειες για τον αριθμό ταυτόχρονων SAs που υποστηρίζει η συσκευή. Τέλος, η συσκευή υποστηρίζει την απομακρυσμένη διαχείριση όλων των κρυπτοσυσκευών στο δίκτυο μέσω ενός κεντρικού συστήματος διαχείρισης, του CATAPAN Device Manager, χωρίς να δίνονται επιμέρους λεπτομέρειες για τον αν η διαχείριση γίνεται μέσω χωριστού κρυπτογραφημένου δικτύου.[69][70]

Λογική ασφάλεια

Οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται από τη συσκευή ανήκουν στην Suite A και στην Suite B αντίστοιχα, χωρίς να αναφέρονται ρητά τα ονόματά τους. Επίσης, δεν γίνεται γνωστό το αν οι αλγόριθμοι κρυπτογράφησης είναι προσαρμόσιμοι (αν δηλαδή μπορεί να αλλαχτεί η παραμετροποίησή τους). Όσον αφορά την εισαγωγή κλειδών στη συσκευή, δεν δίνονται περαιτέρω λεπτομέρειες για το με ποιους τρόπους ακριβώς γίνεται, π.χ με ειδική συσκευή, μέσω απομακρυσμένου συστήματος διαχείρισης κ.α, ωστόσο σύμφωνα με τον κατασκευαστή, οι διαδικασίες εισαγωγής των κλειδιών συμμορφώνονται με τις προδιαγραφές και διαδικασίες βασικής διαχείρισης κλειδών που ορίζει η

CESG[91], η οποία αποτελεί την Εθνική Αρχή Διασφάλισης Πληροφοριών του Ηνωμένου Βασιλείου.[69][70]

Φυσική ασφάλεια

Από το γεγονός ότι υπάρχει συμμόρφωση με πρότυπα TEMPEST (πρότυπο SDIP-27, Level A) και από το γεγονός ότι οι Ethernet interfaces χωρίζονται σε CT και PT (cipher-text και plain-text) βλέπουμε ότι υπάρχει συμμόρφωση με το RED-BLACK πρότυπο. Επίσης, βάσει του κατασκευαστή, η κρυπτομηχανή διαθέτει πιστοποίηση TEMPEST βάσει του προτύπου SDIP-27, σε επίπεδο A. Όσον αφορά την ηλεκτρομαγνητική ακτινοβολία που εκπέμπεται από τη συσκευή, σύμφωνα με τον κατασκευαστή, υπάρχει εναρμόνιση της συσκευής με την Οδηγία 2004/108/ΕΕ του Συμβουλίου της 15ης Δεκεμβρίου 2004 για την προσέγγιση των νομοθεσιών των κρατών μελών σχετικά με την ηλεκτρομαγνητική συμβατότητα, η οποία καταργεί την Οδηγία 89/336/ΕΟΚ που είδαμε στην περίπτωση της TCE-621[92]. Όσον αφορά τα χαρακτηριστικά της επιχειρησιακής ασφάλειας της συσκευής, παρατηρείται ότι για να είναι επιχειρησιακή η κρυπτοσυσκευή, θα πρέπει να βρίσκεται σε αυτή το Crypto Ignition Key. Εάν το CIK απουσιάζει, η συσκευή δεν παρέχει καμία προστασία και άρα η διαβάθμιση που προσφέρει κατακερματίζεται (εμπίπτει σε NPM ACCSEC[93] που είναι στην ουσία UNCLASSIFIED), και υπάρχει επίσης η δυνατότητα για εφεδρικό (backup) CIK, το οποίο χρησιμοποιείται σε περίπτωση που το κύριο (master) CIK χαθεί ή κλαπεί. Επίσης, υπάρχει η δυνατότητα επείγουσας διαγραφής δεδομένων, η οποία

---

91 *Η Εθνική Τεχνική Αρχή για τη Διασφάλιση Πληροφοριών (CESG) της κυβέρνησης του Ηνωμένου Βασιλείου, συμβουλεύει τους οργανισμούς σχετικά με τον τρόπο προστασίας των συστημάτων πληροφοριών και πληροφοριών τους από τις σημερινές απειλές* [71].

92 GOV.UK. Departments, agencies and public bodies. Government Communications Headquarters. CESG [online] Available at https://www.gov.uk/government/organisations/cesg [Accessed 22 Nov 20].

93 Ο βαθμός ασφαλείας NOT PROTECTIVELY MARKED της κυβέρνησης του Ηνωμένου Βασιλείου ισοδυναμεί με τον βαθμό ασφαλείας UNCLASSIFIED του NATO [72]. Ο όρος Accountable σημαίνει ότι πρέπει κατ'ελάχιστο να υπάρχει γνώση του πού βρίσκεται το asset (η συσκευή) και πρέπει να είναι ασφαλές ανά πάσα στιγμή [73].

μπορεί είτε απομακρυσμένα είτε μέσω του κομβίου στον κεντρικό πίνακα (είναι ορατό από την εικόνα της συσκευής), όπως και η εισαγωγή του CIK (γίνεται αντιληπτό από αυτό ότι το CIK μπορεί να είναι και ψηφιακής μορφής). Δεν δίνονται λεπτομέρειες από τον κατασκευαστή σχετικά με τις δυνατότητες φυσικής προστασίας (tamper protection) της συσκευής, ούτε για τυχόν interfaces εισαγωγής κλειδών μέσω ειδικής συσκευής πλήρωσης [69][70].

Αξιοπιστία

Δεν παρέχονται από τον κατασκευαστή στοιχεία αξιοπιστίας της συσκευής (MTTF – MTTR).

Πιστοποιήσεις Common Criteria

Η L3 TRL Technology δεν παρέχει στοιχεία πιστοποιήσεων CC ή άλλων παρόμοιων πιστοποιήσεων.

7.5.6 Η κρυπτομηχανή MISTRAL IP Corporate / Gigabit – Γαλλία

Η MISTRAL IP Corporate / Gigabit αποτελεί την τελευταία κρυπτομηχανή που εξετάζεται στην παρούσα εργασία και είναι Γαλλικής προέλευσης, με κατασκευάστρια εταιρεία την Thales. [74]

Σχήμα 7.13: Η κρυπτοσυσκευή MISTRAL IP Gigabit [74]

Επίπεδο διαβάθμισης

Σύμφωνα με την NCI Agency, η συσκευή αυτή είναι κατάλληλη για την κρυπτογράφηση δεδομένων διαβάθμισης από NATO RESTRICTED και κάτω. Βλέπουμε ότι εδώ δεν ισχύει καμία από τις προηγούμενες διαβαθμίσεις COSMIC TOP SECRET και NATO SECRET, και ότι η κρυπτοσυσκευή αυτή έχει ακόμα μικρότερη διαβάθμιση [75]. Η πιθανότερη αιτία για την οποία ισχύει αυτή η διαβάθμιση είναι ότι, όπως θα δούμε και παρακάτω, η κρυπτοσυσκευή αυτή δεν διαθέτει καθόλου πιστοποίηση TEMPEST, σε αντίθεση με τις άλλες περιπτώσεις που εξετάστηκαν.

Φυσικά χαρακτηριστικά

Η κρυπτοσυσκευή είναι διαστάσεων 443 x 393 x 44 mm (μήκος x πλάτος x ύψος) και μπορεί να προσαρμοστεί σε rack 19'' (1U). Επίσης ζυγίζει περίπου 7 κιλά. Τροφοδοτείται με τάση 115/230 V. Μπορεί να λειτουργήσει σε θερμοκρασίες 5 έως 40 °C και να αποθηκευτεί σε θερμοκρασίες 0 έως 70 °C. Επίσης, τα επίπεδα υγρασίας στα οποία η συσκευή να παραμείνει λειτουργική είναι 5% έως 95% [74].

Επικοινωνιακές δυνατότητες

Η κρυπτοσυσκευή υλοποιεί VPN με τη χρήση του IPsec ESP σε tunnel mode. Παρέχει επίσης τη δυνατότητα για Fast Forward mode, όπου κρυπτογραφείται μόνο το IP payload ή το TCP payload (όχι το IP header), επομένως σε αυτή την περίπτωση δεν είναι εμπιστευτική η πραγματική διεύθυνση IP του πακέτου, καθώς αυτή δεν κρυπτογραφείται. Σύμφωνα με τον κατασκευαστή, η συσκευή μπορεί να παρέχει έως και 6000 ταυτόχρονα VPNs (δηλαδή, SAs). Η ταχύτητα που μπορεί να παρέχει η συσκευή είναι 1 Gbps full duplex (γίνεται αντιληπτό και από το όνομά της ότι η συσκευή παρέχει Gigabit Ethernet Interfaces). Οι interfaces που η συσκευή παρέχει είναι όλες τύπου Ethernet (RJ-45_, και είναι μία console port, δύο Gigabit Ethernet στην plaintext πλευρά και δύο Gigabit Ethernet στην ciphertext πλευρά. Η μία από τις δύο Ethernet ports στην κάθε πλευρά χρησιμοποιείται ως failover, δηλαδή για να πάρει τη θέση της άλλης στον δίκτυο όταν η μία από τις δύο αποτυγχάνει. Τα πρωτόκολλα επικοινωνίας που υποστηρίζει η συσκευή γενικά δεν γίνονται γνωστά. Τέλος, η συσκευή υποστηρίζεται από σύστημα κεντρικής διαχείρισης, το Mistral Management Centre, το οποίο μπορεί να παρακολουθεί την κίνηση στο δίκτυο. Η ρύθμιση της συσκευής μπορεί να γίνει είτε μέσω του Mistral Management Centre, είτε μέσω της console port, είτε μέσω αρχείου ρύθμισης (όπως στους Cisco routers) [74].

Λογική ασφάλεια

Σημαντική λεπτομέρεια αποτελεί το γεγονός ότι δεν υπάρχουν interfaces για την είσοδο ειδικής συσκευής πλήρωσης, παρά μόνο console port, που σημαίνει ότι η συσκευή δεν είναι συμβατή με συσκευές πλήρωσης στρατιωτικού τύπου. Βλέπουμε γενικά ότι η συσκευή χρησιμοποιεί ως αλγόριθμο κρυπτογράφησης τον AES (128-256 bit) της Suite B. Επίσης, η κρυπτοσυσκευή έχει τη δυνατότητα να εμφανίζει ενδείξεις συναγερμού όταν υπάρχει κάποιο security event. Το lifetime των κλειδιών κρυπτογράφησης καθώς και της χρονικής περιόδου όπου θα ισχύει η κρυπτογράφηση μπορεί να επιλεχθεί από το διαχειριστή [74].

Φυσική ασφάλεια

Μπορούμε να διακρίνουμε από τις interfaces την αρχιτεκτονική plaintext – ciphertext (RED-BLACK) όμως απουσιάζει η οποιαδήποτε πιστοποίηση TEMPEST, γεγονός που πιθανότατα είναι και μία από τις αιτίες υποβάθμισης της διαβάθμισής της. Η συσκευή παρέχει γενικά τη δυνατότητα επείγουσας διαγραφής των ευαίσθητων δεδομένων (π.χ κλειδιών), αλλά μόνο τοπικά (όχι απομακρυσμένα). Όσον αφορά την ηλεκτρομαγνητική ακτινοβολία που εκπέμπεται από τη συσκευή, σύμφωνα με τον κατασκευαστή, υπάρχει συμμόρφωση της συσκευής με το διεθνές πρότυπο EN 55022 που έχει αναφερθεί και στις περιπτώσεις της TCE 621 και της KG-250, καθώς και με την Ομοσπονδιακή Επιτροπή Επικοινωνιών, χωρίς να αναφέρεται το επίπεδο συμμόρφωσης. Πολύ σημαντικό στοιχείο επίσης παίζει και η απουσία του CIK, καθώς αυτό δεν αναφέρεται πουθενά από τον κατασκευαστή. Αυτό σημαίνει πως δεν απαιτείται κάποιο CIK για να καταστεί η κρυπτοσυσκευή επιχειρησιακή, και αποτελεί επίσης σημαντική διαφορά από τις υπόλοιπες περιπτώσεις. Δεν αναφέρονται επίσης από τον κατασκευαστή τυχόν δυνατότητες για αυτοέλεγχο BIT της συσκευής. [74]

Αξιοπιστία

Όσον αφορά την αξιοπιστία της συσκευής, ο κατασκευαστής τονίζει ότι το MTBF της συσκευής είναι περίπου 5000 ώρες (δηλαδή η συσκευή λειτουργεί 5000 ώρες έως ότου παρουσιάσει βλάβη, από την πρώτη βλάβη). Δεν παρέχεται κάποια τιμή για το MTTR της συσκευής από τον κατασκευαστή [74].

Πιστοποιήσεις Common Criteria

Η συσκευή, σύμφωνα με τον κατασκευαστή, είναι πιστοποιημένη CC ως EAL3+, η οποία είναι μικρότερη από την ανάλογη πιστοποίηση της EP-430, η οποία είναι EAL4+, που μπορεί επίσης να παίζει σημαντικό ρόλο στην διαβάθμισή της. Επίσης, βλέπουμε ότι

υπάρχει και η πιστοποίηση από την Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ως EU RESTRICTED και DIFFUSION RESTREINTE, που συμβαδίζει με την διαβάθμιση της NCI Agency [74][77].

ΚΕΦΑΛΑΙΟ 8

ΠΡΟΫΠΟΘΕΣΕΙΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΠΛΗΡΟΙ ΜΙΑ ΚΡΥΠΤΟΜΗΧΑΝΗ

Εξετάζοντας τις διαφορετικές κρυπτομηχανές του NIAPC, εξάγονται διάφορα συμπεράσματα για τα χαρακτηριστικά φυσικής σχεδίασης που θα πρέπει να έχουν, τη φυσική και λογική ασφάλεια που θα πρέπει να παρέχουν, τις επικοινωνιακές δυνατότητες που κατ'ελάχιστο θα πρέπει να διαθέτουν και τα λοιπά χαρακτηριστικά τους που προκύπτουν από διάφορες πιστοποιήσεις όσον αφορά την σχεδίαση, ανάπτυξη και αξιοπιστία τους. Τα παραπάνω σε συνδυασμό με το *CC IP Encryptor Protection Profile* της Εθνικής Αρχής Ασφάλειας Επικοινωνιών της Γαλλίας[94] και τον Πίνακα Συμμόρφωσης της Διακήρυξης Διαγωνισμού για το Έργο «*Προμήθεια εξοπλισμού και βελτίωση – επέκταση δικτυακών υποδομών του ΥΠΕΞ και των Αρχών Εξωτερικού*» (στο τμήμα που αφορά την Κρυπτομηχανή IP)[95] βοηθούν στο χτίσιμο ενός προφίλ ελάχιστων προϋποθέσεων που πρέπει να πληροί η κρυπτομηχανή IP, το οποίο αναλύεται στο παρόν κεφάλαιο.

---

94 Direction centrale de la sécurité des systèmes d'information. (2008, July). IP Encryptor Protection Profile - CC3.1. France: Secrétariat général de la défense nationale.

95 Υπουργείο Εξωτερικών. Ειδική Υπηρεσία Συντονισμού και Εφαρμογής Χρηματοδοτικών και Επενδυτικών Προγραμμάτων –ΕΥΣΧΕΠ. Προμήθεια εξοπλισμού και βελτίωση – επέκταση δικτυακών υποδομών του ΥΠΕΞ και των Αρχών Εξωτερικού - Μέρος Γ: Υποδείγματα και Πίνακες Συμμόρφωσης (2014) [online] Available at [online] Available at https://www.mfa.gr/images/docs/dimosioi_diagonismoi/2014_5_21_eysxep_C.pdf [Accessed 23 Nov 2020]

8.1 Προϋποθέσεις φυσικής σχεδίασης συσκευής

- Η συσκευή θα πρέπει να διαθέτει διαφορετικά κυκλώματα Black και Red και τα κυκλώματα της συσκευής να διαθέτουν ξεχωριστές γραμμές τροφοδοσίες για Black και Red, καθώς και φίλτρα γραμμών –τροφοδοτικών ή εναλλακτικά ένα τροφοδοτικό και για τα δύο κυκλώματα, με χρήση ειδικών φίλτρων διαχωρισμού και προστασίας από διαρροή δεδομένων.
- Θα πρέπει η συσκευή να έχει τη δυνατότητα αυτοελέγχου BITE:
    - κατά την εκκίνηση της κρυπτοσυσκευής, (POWER ON-SELF TEST - POST),
    - αυτόματα κατά την διάρκεια λειτουργίας της κρυπτοσυσκευής (ON LINE)
    - μέσω εντολής χειριστού, όποτε απαιτείται, ενώ η συσκευή βρίσκεται σε ουδέτερη κατάσταση αναμονής (idle position).

8.2 Προϋποθέσεις δυνατοτήτων επικοινωνίας συσκευής

- Οι συσκευές θα πρέπει να δημιουργούν εικονικά ιδιωτικά δίκτυα (VPN) κρυπτογραφώντας τα δεδομένα που ανταλλάσσονται από τα προστατευόμενα υποδίκτυα. Τα υποδίκτυα θα πρέπει συνδέονται μεταξύ τους μέσω δικτύων IP. Οι συσκευές θα πρέπει τοποθετούνται στο σημείο πρόσβασης των υποδικτύων προς το γεωγραφικό δίκτυο (το ciphertext δίκτυο).
- Θα πρέπει η συσκευή να υλοποιεί Full Duplex επικοινωνία με ταχύτητα τουλάχιστον 100 Mbps σε Ethernet interface.
- Θα πρέπει να υποστηρίζει τουλάχιστον τα πρωτόκολλα: TCP, IP, DNS, FTP, HTTP, UDP, TFTP, SMTP, SNMP, ICMP στην ciphertext πλευρά, TCP, IP, HTTP, DNS, SNMP, ARP στην plaintext πλευρά.
- Η σύνδεση προς την ανοικτή και την κρυπτογραφημένη πλευρά θα πρέπει να γίνεται με διαφορετικές διεπαφές (red and black interfaces) σύμφωνα με το πρωτόκολλο IEEE802.3, 100Base-TX, (10/100 Mbps) επιλεγόμενες από τον χειριστή μέσω του λογισμικού της συσκευής.

- Θα πρέπει να γίνεται χρήση του πρωτοκόλλου IPsec ESP (Encapsulation Security Payload) σε Tunnel mode.
- Κάθε συσκευή να μπορεί να μπορεί να υλοποιεί ταυτόχρονα τουλάχιστον 1000 συσχετίσεις ασφαλείας (SAs) και να μπορεί να λειτουργεί και να συνεργάζεται σε δίκτυο τουλάχιστον 1000 IPsec συσκευών.
- Οι αναβαθμίσεις του λογισμικού θα πρέπει να γίνονται είτε τοπικά, είτε μέσω Κεντρικού Συστήματος Διαχείρισης.

8.3 Προϋποθέσεις λογικής ασφάλειας συσκευής

- Θα πρέπει να υπάρχει δυνατότητα εισαγωγής κλείδας με τους παρακάτω τρόπους:
    - Με συσκευές τύπου "FILLGUN" ή cartridges/modules τύπου «card».
    - Απομακρυσμένα μέσω του Κεντρικού Συστήματος Διαχείρισης (ΚΣΔ) (REMOTE)
- Θα πρέπει να μπορεί να γίνει ανανέωση της κλείδας από τον χειριστή, εφόσον απαιτηθεί.
- Θα πρέπει να υπάρχει δυνατότητα προγραμματισμού αυτόματης αλλαγής κλειδιών κατά τακτά χρονικά διαστήματα, με κατάλληλο προγραμματισμό.
- Θα πρέπει να διατηρούνται οι κλείδες και οι μεταβλητές λειτουργίας (set-up) σε περιπτώσεις διακοπών της ηλεκτρικής τροφοδοσίας της συσκευής, τουλάχιστον 6 ώρες. Η διατήρηση θα γίνεται μέσω μπαταρίας, το επίπεδο-της οποίας θα ελέγχεται συνεχώς και αυτόματα από το BITE. Να υπάρχει δυνατότητα να μην απολεσθούν οι κλείδες και οι μεταβλητές λειτουργίας (set-up) της συσκευής, όταν απαιτείται αλλαγή της μπαταρίας.
- Θα πρέπει το μέγεθος της ενεργούς κλείδας (master key or primary key) να είναι τουλάχιστον 256 bits (όπως στον AES-256).
- Ο αλγόριθμος κρυπτογράφησης εμπιστευτικότητας θα πρέπει να είναι είτε απόρρητος αλγόριθμος ο οποίος θα είναι προεγκατεστημένος στη συσκευή είτε αλγόριθμος που πληροί τις προϋποθέσεις της Suite B (όπως ο AES-256).
- Στο δίκτυο θα πρέπει να υπάρχουν τρία ξεχωριστά επίπεδα διαχείρισης. Για τον υπεύθυνο ασφαλείας (security officer), που είναι υπεύθυνος για τη διαχείριση Α-

σφαλείας του δικτύου. Για τον διαχειριστή του δικτύου (Network Manager),που είναι υπεύθυνος για τη διαχείριση του δικτύου. Για τον χειριστή (operator), που είναι υπεύθυνος για τη λειτουργία του δικτύου με τη χρήση του user interface (οθόνη και πληκτρολόγιο). Κάθε επίπεδο διαχείρισης θα έχει διαφορετικό κωδικό πρόσβασης.

- Θα πρέπει να υπάρχει δυνατότητα καταγραφής των ενεργειών (logging) για μετέπειτα πιθανό έλεγχο.

8.4 Προϋποθέσεις για το σύστημα παραγωγής κλειδών

- Οι κύριες κλείδες (master keys or primary keys) θα πρέπει να παράγονται εκτός των συσκευών από ειδικό σύστημα παραγωγής και ελέγχου, σύγχρονης τεχνολογίας (αυτό στην ουσία αφαιρεί για λόγους ασφαλείας την δυνατότητα αυτόματης δημιουργίας κλειδών και χρήσης τους από την κρυπτομηχανή).
- Θα πρέπει να υπάρχει και δυνατότητα παραγωγής κλείδων με επιπλέον διαφορετικούς τρόπους συμβατούς όμως με τις δυνατότητες των παρεχομένων κρυπτοσυσκευών (π.χ. εισαγωγή από το πληκτρολόγιο της συσκευής ή με οπτικό δίσκο, κλπ).

8.5 Προϋποθέσεις για το κεντρικό σύστημα διαχείρισης

- Θα πρέπει να υπάρχει ένα Κεντρικό Σύστημα Διαχείρισης για όλες τις συσκευές του δικτύου, το οποίο θα πρέπει να έχει τη δυνατότητα να διαχειρίζεται και να εποπτεύει το έργο της κάθε συσκευής στο δίκτυο.
- Το Κεντρικό Σύστημα Διαχείρισης θα πρέπει να έχει τη δυνατότητα εκτέλεσης όλων των λειτουργιών ασφαλείας και διανομής κλείδων στις μονάδες του δικτύου και να πραγματοποιεί τη διαχείριση ασφαλείας του δικτύου.
- Ο προγραμματισμός αυτόματης αλλαγής και/ή ανανέωσης των κλειδιών να γίνεται και μέσω του Κεντρικού Συστήματος Διαχείρισης.
- Τα δεδομένα της διαχείρισης ασφαλείας του δικτύου θα πρέπει να είναι κρυπτογραφημένα με τον ίδιο αλγόριθμο ασφαλείας που εκτελείται και η επικοινωνία, αλλά με διαφορετικά κλειδιά ή με άλλο αλγόριθμο ίδιου βαθμού ασφαλείας.
- Το Κεντρικό Σύστημα Διαχείρισης θα πρέπει να είναι σχεδιασμένο με τέτοιο τρόπο ώστε να εξασφαλίζεται η διαθεσιμότητα του 100%.

8.6 Προϋποθέσεις φυσικής ασφάλειας συσκευής

- Μία τέτοια συσκευή θα πρέπει να είναι συμβατή κατά το δυνατόν με προδιαγραφές TEMPEST, σύμφωνα με την προδιαγραφή NATO SDIP-27 Level A. Η συμβατότητα αυτή της συσκευής αξιολογείται εφόσον αυτές θα χρησιμοποιούνται κυρίως εντός TEMPEST ζώνης.
- Η συσκευή θα πρέπει να μην είναι ευαίσθητη σε ηλεκτρομαγνητικές παρεμβολές από άλλες ηλεκτρικές/ηλεκτρονικές συσκευές και να μην προκαλεί η ίδια παρεμβολές σε άλλες συσκευές (να είναι κατασκευασμένη δηλαδή σύμφωνα με τα πρότυπα MIL-STD 461 και 462 αντίστοιχες εκδόσεις της Ε.Ε)
- Σε περίπτωση απώλειας ή κλοπής ή καταστροφής μίας συσκευής θα πρέπει να υπάρχει δυνατότητα η εν λόγω συσκευή να εξαιρεθεί από το δίκτυο.
- Θα πρέπει η συσκευή να διαθέτει τεχνική που να καθιστά αδύνατη την ανάγνωση των δεδομένων ασφαλείας της (tamper-proof design), είτε είναι σε τροφοδοσία, είτε είναι εκτός τροφοδοσίας.
- Η συσκευή πρέπει να έχει μηχανισμό διαγραφής δεδομένων ασφαλείας επείγουσας ανάγκης, ο οποίος να μπορεί να εκτελεστεί χειροκίνητα ή να ενεργοποιηθεί αυτόματα όταν ανοίγεται το περίβλημα της συσκευής.
- Θα πρέπει να υπάρχει κλειδί ενεργοποίησης (μηχανικό ή τύπου κάρτας ή software) της συσκευής (crypto ignition key -CIK) για την ενεργοποίηση της συσκευής.
- Η συσκευή θα πρέπει να είναι προδιαγραφών EMI/EMC FCC Class B ή EN 55022 Class B.

8.7 Προϋποθέσεις συνθηκών περιβάλλοντος συσκευής

- Οι συσκευές πρέπει να πληρούν προδιαγραφές, αποδεκτές από το NATO, όπως MILSTD 810E ή αντίστοιχες της Ευρωπαϊκής Ένωσης (Ε.Ε.), ή διεθνείς (ISO).

8.8 Προϋποθέσεις αξιοπιστίας συσκευής

- Ο υπολογισμός της θεωρητικής τιμής MTBF της συσκευής, να γίνει σύμφωνα με το πρότυπο MILHDBK 217F (ή νεώτερη έκδοση) των ΗΠΑ ή άλλη αντίστοιχη έκδοση.

- Η ελάχιστη αποδεκτή Mean Time Between Failures της συσκευής είναι οι 20.000 ώρες.

ΚΕΦΑΛΑΙΟ 9

ΔΥΝΑΤΟΤΗΤΕΣ ΜΕΤΑΒΑΣΗΣ ΑΠΟ ΤΟ ΜΟΝΤΕΛΟ IPSEC ΜΕ ΚΡΥΠΤΟ-ΜΗΧΑΝΗ ΣΤΟ ΜΟΝΤΕΛΟ IPSEC ΧΩΡΙΣ DEDICATED HARDWARE

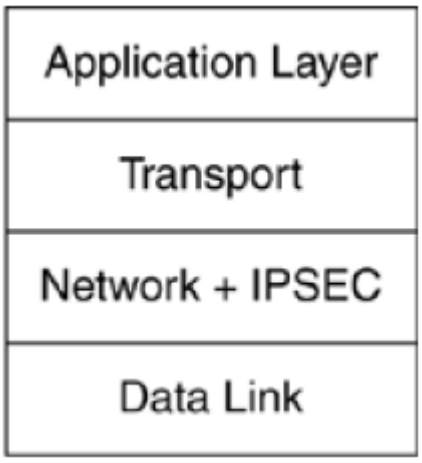
Όπως είδαμε στο κεφάλαιο 6.1, η υλοποίηση του IPSec με τη χρήση κρυπτομηχανών αποτελεί υλοποίηση Bump-In-The-Wire. Για να μπορέσουμε να εξετάσουμε τη δυνατότητα χρήσης του IPSec σε στρατιωτικές δομές χωρίς κρυπτομηχανές, θα πρέπει να δούμε γενικά τους τρόπους με τους οποίους μπορεί να ενσωματωθεί η χρήση του IPSec στα δίκτυα IP. Όπως έχει αναφερθεί και σε προηγούμενο κεφάλαιο, το IPSec μπορεί να ενσωματωθεί τόσο στους δρομολογητές όσο και στους hosts.

9.1 Τρόποι ενσωμάτωσης IPSec στους hosts

Όσον αφορά τους hosts, υπάρχουν δύο τρόποι ενσωμάτωσης του IPSec [80]:

- Ενσωμάτωση στο Λειτουργικό Σύστημα

Όσον αφορά την ενσωμάτωση στους hosts, το IPSec μπορεί να ενσωματωθεί απευθείας στο λειτουργικό σύστημα. Σύμφωνα με τους Doraswarmy και Harkins, εφόσον το IPSec αποτελεί πρωτόκολλο επιπέδου δικτύου, μπορεί να εφαρμοστεί ως μέρος του επιπέδου δικτύου. Εδώ, το IPSec χρησιμοποιεί τις υπηρεσίες του επιπέδου IP για την κατασκευή της κεφαλίδας IP. Αυτό το μοντέλο ενσωμάτωσης είναι πανομοιότυπο με την εφαρμογή άλλων πρωτοκόλλων επιπέδου δικτύου όπως το ICMP [80].

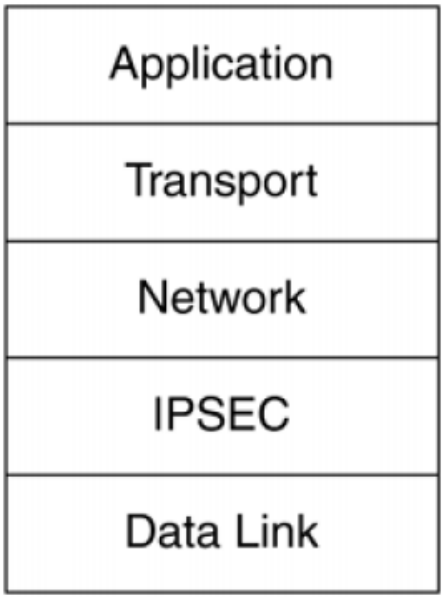


Σχήμα 9.1: Ενσωμάτωση IPSec ως μέρος του επιπέδου δικτύου [81]

Τα κύρια πλεονεκτήματα της πρακτικής αυτής είναι ότι η διαχείριση κλειδών και γενικά οι λειτουργίες της σουίτας πρωτοκόλλων που χρησιμοποιεί το IPSec μπορούν να ενσωματωθούν χωρίς αυτό να φαίνεται στον χρήστη, καθώς και ότι μπορεί να υλοποιήσει όλα τα modes του IPSec. Σημαντικό μειονέκτημα όμως αποτελεί ότι οι δυνατότητες του IPSec σε αυτή την υλοποίηση εξαρτώνται από τις δυνατότητες του εκάστοτε λειτουργικού συστήματος, και μπορεί να μην επιτρέπουν την ανάπτυξη προηγμένων δυνατοτήτων του IPSec [80]. Επίσης, άλλο σημαντικό μειονέκτημα της υλοποίησης αυτής αποτελεί, σύμφωνα με τον Charles M. Kozierok, το ότι ενώ με τη χρήση του IPv6 υποστηρίζεται η ενσωμάτωση του IPSec στο επίπεδο δικτύου, το ίδιο δεν συμβαίνει με το IPv4 με αποτέλεσμα να απαιτούνται αλλαγές στον πηγαίο κώδικα IP σε κάθε host (ή router, όπως θα δούμε παρακάτω), κάτι που δεν αποτελεί σε καμία περίπτωση πρακτική λύση [81].

- Υλοποίηση Bump-In-The-Stack

Σε αυτή την πρακτική, το IPSec εισάγεται και εφαρμόζεται μεταξύ του επιπέδου δικτύου και του επιπέδου σύνδεσης δεδομένων [80].



Σχήμα 9.2: Ενσωμάτωση IPSec ανάμεσα στο επίπεδο δικτύου και στο επίπεδο σύνδεσης δεδομένων [81]

Το κύριο πλεονέκτημα αυτής της πρακτικής είναι η δυνατότητα πλήρους εκμετάλλευσης της σουίτας IPSec και η μη εξάρτηση από το λειτουργικό σύστημα. Το κύριο μειονέκτημά της είναι ότι πολλές λειτουργίες του επιπέδου δικτύου μπορεί να εκτελούνται περισσότερες φορές από ότι χρειάζεται, καθώς το IPSec υλοποιεί πολλές από αυτές, Αυτό το “duplication of effort” ενδεχομένως να οδηγήσει σε ανεπιθύμητες επιπλοκές, όμως με σωστό σχεδιασμό αυτό είναι κάτι που μπορεί να ξεπεραστεί [80]. Αυτή η πρακτική ενδείκνυται για hosts που υλοποιούν IPv4. Εφόσον το IPv4 αποτελεί ακόμη τον κύριο τρόπο υλοποίησης στο επίπεδο δικτύου, μπορούμε να πούμε ότι το Bump-In-The-Stack είναι προς το παρόν η πιο ενδεδειγμένη λύση αν επιλέγαμε να ενσωματώσουμε το IPSec στους hosts στα στρατιωτικά δίκτυα τύπου IP.

9.2 Τρόποι ενσωμάτωσης IPSec στους δρομολογητές

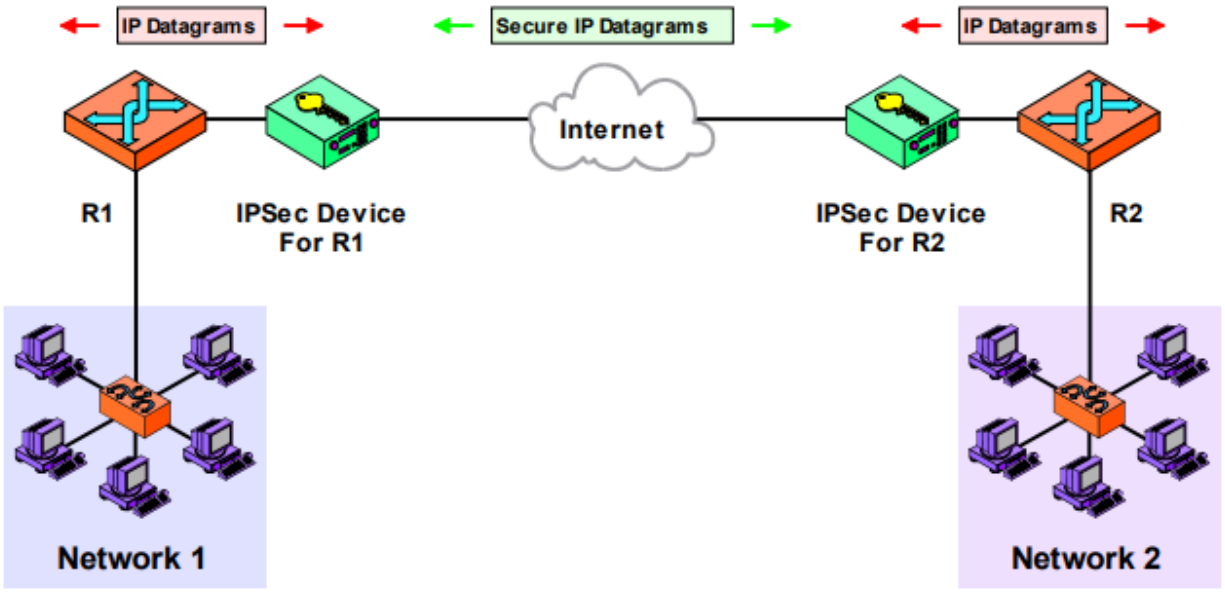
Όσον αφορά τους routers, υπάρχουν δύο τρόποι ενσωμάτωσης του IPSec [80]:

- Ενσωμάτωση στο λογισμικό του router

Αποτελεί πρακτική η οποία είναι σχεδόν όμοια με αυτή της ενσωμάτωσης στο λειτουργικό σύστημα των hosts. Έτσι, και εδώ το IPSec ενσωματώνεται στο επίπεδο δικτύου, με όμοια πλεονεκτήματα και αδυναμίες. Για παράδειγμα, αποτελεί μειονέκτημα το γεγονός ότι η υλοποίηση του custom αλγορίθμου κρυπτογράφησης δεν είναι δυνατή στους περισσότερους (αν όχι σε όλους) routers που υποστηρίζουν IPSec, γιατί έχουν προγραμματιστεί να υποστηρίζουν συγκεκριμένους αλγορίθμους κρυπτογράφησης (π.χ AES-256).

- Υλοποίηση Bump-In-The-Wire

Αποτελεί την υλοποίηση με ξεχωριστή συσκευή (κρυπτομηχανή) η οποία εγκαθίσταται στην εξωτερική πλευρά του router ενός site (π.χ μιας στρατιωτικής Μονάδας), παραλαμβάνει από τον router τα datagrams και προσθέτει τις IPSec ιδιότητες, όπως έχει αναφερθεί στην παρούσα εργασία.



Σχήμα 9.3: Υλοποίηση IPSec Bump-In-The-Wire [82]

Για τις στρατιωτικές δομές που χρησιμοποιούν δίκτυα IP, βάσει των παραπάνω, θα εξεταστούν οι περιπτώσεις μετάβασης από το μοντέλο χρήσης του IPSec Bump-In-The-Wire (BITW) με κρυπτομηχανές στην εξωτερική πλευρά του router είτε στο μοντέλο ενσωμάτωσης του IPSec στον host είτε στο μοντέλο ενσωμάτωσης του IPSec στο λογισμικό

του router, με κριτήρια το κατά πόσο πληρούνται οι προϋποθέσεις ασφάλειας που θέτει το NATO, κατά πόσο επηρεάζεται η ταχύτητα στο δίκτυο και κατά πόσο επηρεάζεται το κόστος ενσωμάτωσης της κάθε τεχνικής στις δικτυακές υποδομές. Θεωρούμε πως τελικός στόχος είναι η σταδιακή μετάβαση από το μοντέλο BITW σε κάποιο από τα άλλα δύο μοντέλα, με την αντικατάσταση των κρυπτομηχανών είτε από κεντρικούς υπολογιστές - hosts στους οποίους θα ενσωματώνεται το IPSec, είτε από δρομολογητές στους οποίους θα ενσωματώνεται το IPSec χωρίς τη χρήση ξεχωριστής συσκευής IPSec. Ο κρίσιμος παράγοντας που θα κρίνει το τελικό συμπέρασμα, κατά την παρούσα εργασία, είναι το κόστος, που αφορά είτε το συγκρινόμενο κόστος προμήθειας των συσκευών σαν σύνολο (αν δηλαδή π.χ χτίζαμε το δίκτυο από την αρχή και διαλέγαμε τον τύπο των συσκευών IPSec) είτε το κόστος μετάβασης (αν δηλαδή θεωρούμε ότι μια στρατιωτική δομή υλοποιεί το μοντέλο Bump-In-The-Wire και μεταβαίνει σταδιακά σε άλλο μοντέλο, με το κόστος που αυτό επιφέρει).

9.3 Δυνατότητα ενσωμάτωσης του IPSec στον host στα στρατιωτικά δίκτυα IP

Σε αυτή την περίπτωση, το IPSec θα πρέπει να ενσωματωθεί σε κάθε κεντρικό υπολογιστή. Δηλαδή, αντί για τη χρήση των κρυπτομηχανών, κάθε κεντρικός υπολογιστής θα αποτελεί από μόνος του την κρυπτομηχανή για τον εαυτό του, και όλες οι ιδιότητες του IPSec θα δίνονται στα εξερχόμενα datagrams ήδη από τον host (ομοίως θα αφαιρούνται από τα εισερχόμενα datagrams στον host). Επομένως, θα πρέπει να γίνει μια μετάβαση από την αρχιτεκτονική gateway-to-gateway στην αρχιτεκτονική host-to-host. Στα πλαίσια της εργασίας αυτής, θα εξεταστεί το πως είναι δυνατή η εκπλήρωση των προϋποθέσεων του NATO που αναφέρθηκαν στο κεφάλαιο 8 από αυτή την πρακτική και θα αναλυθούν τα πλεονεκτήματα και μειονεκτήματα της πρακτικής αυτής.

Προϋποθέσεις φυσικής σχεδίασης

Όπως και η κρυπτομηχανή, ο κάθε σταθερός/φορητός Η/Υ ο οποίος θα συμμετέχει στο δίκτυο θα πρέπει να διαθέτει διαφορετικά κυκλώματα Black και Red και τα κυκλώματα της συσκευής να διαθέτουν ξεχωριστές γραμμές τροφοδοσίες για Black και Red, καθώς και

φίλτρα γραμμών –τροφοδοτικών ή εναλλακτικά ένα τροφοδοτικό και για τα δύο κυκλώματα, με χρήση ειδικών φίλτρων διαχωρισμού και προστασίας από διαρροή δεδομένων [78]. Ένας τέτοιος υπολογιστής από πλευράς φυσικής σχεδίασης δεν βρίσκεται ελεύθερα στο εμπόριο και θα πρέπει να γίνουν ειδικές παραγγελίες. Αυτό αυτόματα αυξάνει κατακόρυφα το κόστος των υπολογιστών αυτών και το κάνει εφάμιλλο της κρυπτομηχανής, και πιθανώς μεγαλύτερο, καθώς το δημιουργηθέν σύστημα θα λειτουργεί και σαν Η/Υ, δηλαδή θα επαυξάνονται οι λειτουργίες και οι δυνατότητες που θα διαθέτει. Επίσης, ο κάθε υπολογιστής θα πρέπει να διαθέτει δυνατότητα αυτοελέγχου BITE κατά την εκκίνηση του (POST) και αυτόματα κατά την διάρκεια λειτουργίας της κρυπτασφάλισης (ON LINE) και μέσω εντολής χειριστού όποτε απαιτείται ενώ η συσκευή βρίσκεται σε ουδέτερη κατάσταση αναμονής (idle position) [78]. Στην ουσία, αποτελεί έναν έλεγχο της built-in «κρυπτομηχανής», δηλαδή του μηχανισμού κρυπτογράφησης και των δεδομένων (π.χ κλείδες) έτσι ώστε να γνωρίζουμε ότι ο υπολογιστής μπορεί να υλοποιήσει το IPSec και να συμμετέχει στο δίκτυο, και μπορεί να γίνει με τη χρήση λογισμικού στον Η/Υ, χωρίς να επιβαρύνεται ιδιαίτερα το κόστος.

Προϋποθέσεις δυνατοτήτων επικοινωνίας

Οι υπολογιστές που συμμετέχουν στο δίκτυο θα πρέπει να υλοποιούν Full Duplex επικοινωνία με ταχύτητα τουλάχιστον 100 Mbps σε Ethernet interface [78]. Οι περισσότεροι πλέον από τους Η/Υ που κυκλοφορούν στο εμπόριο διαθέτουν κάρτα δικτύου PCI Express που υλοποιούν τουλάχιστον ταχύτητα 100 Mbps σε διεπαφή Ethernet (για την ενσύρματη δικτυακή σύνδεση του Η/Υ). Επειδή οι hosts δεν συνδέουν δίκτυα, δεν απαιτείται δικτυακή σύνδεση προς την ανοικτή πλευρά (plaintext) επομένως δεν απαιτούνται διαφορετικές διεπαφές για τη σύνδεση προς την ανοιχτή και την κρυπτογραφημένη πλευρά, αλλά μόνο προς την κρυπτογραφημένη πλευρά. Στην ουσία όλο το intranet το οποίο θα υλοποιείται από τα δίκτυα των στρατιωτικών δομών θα αποτελεί ένα κρυπτογραφημένο δίκτυο, χωρίς να κυκλοφορούν δεδομένα plaintext (καταργείται έτσι στην ουσία η έννοια της ανοιχτής και κρυπτογραφημένης πλευράς, ωστόσο αυτή ισχύει εντός των hosts).

Κάθε υπολογιστής στο δίκτυο θα πρέπει να μπορεί να υλοποιεί ταυτόχρονα τουλάχιστον 1000 συσχετίσεις ασφαλείας (SAs) και να μπορεί να λειτουργεί και να συνεργάζεται σε δίκτυο τουλάχιστον 1000 IPsec συσκευών [78] (σε αυτή την περίπτωση, κεντρικών υπολογιστών). Αυτό σημαίνει ότι θα πρέπει να υπάρχει ικανός χώρος στη RAM του υπολογιστή που να φιλοξενεί τουλάχιστον 1000 SAs (μαζί με τη μνήμη που απαιτείται για τις λοιπές διεργασίες). Η Security Association Database (SAD) όπως αναφέρθηκε και στο κεφ. 4.2 αποτελείται από ένα πίνακα από σύνολο παραμέτρων (12 για κάθε SA). Για 1000 SAs, μπορούμε να υπολογίσουμε ότι ο πίνακας θα έχει περίπου ένα μέγεθος της τάξης των 0,5 mb (αν κάθε παράμετρος έχει μέγεθος περίπου 32 bytes), επομένως καταλαβαίνουμε ότι τουλάχιστον 1 mb της μνήμης RAM του Η/Υ θα πρέπει να δεσμεύεται για τη λειτουργία της SAD.

Επίσης, τυχόν αναβαθμίσεις του λογισμικού θα πρέπει να μπορούν να γίνουν τοπικά ή μεμακρυσμένα μέσω Κεντρικού Συστήματος Διαχείρισης [78]. Εφόσον πρόκειται για κεντρικό υπολογιστή, αυτό τοπικά μπορεί να γίνει εύκολα μέσω του Administrator, και μεμακρυσμένα μέσω του κρυπτογραφημένου δικτύου, εφόσον η ciphertext πλευρά του δικτύου εκτείνεται έως τους hosts.

Κάθε υπολογιστής στο δίκτυο θα πρέπει να μπορεί να υλοποιεί ταυτόχρονα τουλάχιστον 1000 συσχετίσεις ασφαλείας (SAs) και να μπορεί να λειτουργεί και να συνεργάζεται σε δίκτυο τουλάχιστον 1000 IPsec συσκευών [ ] (σε αυτή την περίπτωση, κεντρικών υπολογιστών). Αυτό σημαίνει ότι θα πρέπει να υπάρχει ικανός χώρος στη RAM του υπολογιστή που να φιλοξενεί τουλάχιστον 1000 SAs (μαζί με τη μνήμη που απαιτείται για τις λοιπές διεργασίες). Η Security Association Database (SAD) όπως αναφέρθηκε και στο κεφ. 4.2 αποτελείται από ένα πίνακα από σύνολο παραμέτρων (12 για κάθε SA). Για 1000 SAs, μπορούμε να υπολογίσουμε ότι ο πίνακας θα έχει περίπου ένα μέγεθος της τάξης των 0,5 mb (αν κάθε παράμετρος έχει μέγεθος περίπου 32 bytes), επομένως καταλαβαίνουμε ότι τουλάχιστον 1 mb της μνήμης RAM του Η/Υ θα πρέπει να δεσμεύεται για τη λειτουργία της SAD.

Επίσης, τυχόν αναβαθμίσεις του λογισμικού θα πρέπει να μπορούν να γίνουν τοπικά ή μεμακρυσμένα μέσω Κεντρικού Συστήματος Διαχείρισης. Εφόσον πρόκειται για κεντρικό

υπολογιστή, αυτό τοπικά μπορεί να γίνει εύκολα μέσω του Administrator, και μεμακρυσμένα μέσω του κρυπτογραφημένου δικτύου, εφόσον η ciphertext πλευρά του δικτύου εκτείνεται έως τους hosts.

Προϋποθέσεις λογικής ασφάλειας

Η εισαγωγή των κλειδών στο Η/Υ θα πρέπει να γίνεται είτε με συσκευή τύπου FILLGUN είτε με module τύπου card [78]. Θα πρέπει δηλαδή ο Η/Υ να έχει ενσωματωμένο έναν smart card reader, και οι smart cards που εμπεριέχουν τις κλείδες να μην μπορούν να διαβαστούν από άλλη συσκευή, η να γίνει εγκατάσταση υποδομής στον Η/Υ για υποδοχή συσκευής FILLGUN (π.χ interface DS-102, για συσκευές KOI-18). Η υλοποίηση της smart card είναι σαφώς πιο εύκολη από την υλοποίηση με fill gun, καθώς οι smart card readers βρίσκονται εύκολα στο εμπόριο. Παρόλα αυτά, η υλοποίηση με χρήση κοινής smart card παρέχει πολύ μικρότερη ασφάλεια, καθώς η κάθε smart card μπορεί να διαβαστεί από οποιαδήποτε συσκευή που διαθέτει smart card reader. Επομένως, θα πρέπει να χρησιμοποιηθεί ένα module το οποίο είναι τροποποιημένο έτσι ώστε η συσκευή ή card που περιέχει τα δεδομένα των κλειδών να μπορεί να διαβαστεί μόνο από τους Η/Υ τους οποίους προγραμματίζει. Η εφαρμογή μιας τέτοιας πρακτικής έχει προφανώς επιπλέον κόστος.

Η εισαγωγή των κλειδών πρέπει επίσης να γίνεται και μεμακρυσμένα μέσω Κεντρικού Συστήματος Διαχείρισης [78]. Επειδή αυτό δεν μπορεί να γίνει μέσω του ήδη υπάρχοντος κρυπτογραφημένου δικτύου (δεν μπορεί το δίκτυο να χρησιμοποιείται και οι κλείδες να αλλάζουν την ίδια στιγμή), θα πρέπει να υλοποιείται ένα δεύτερο κρυπτογραφημένο δίκτυο, με ξεχωριστή κλείδα, μέσω του οποίου θα γίνεται ο παραπάνω προγραμματισμός, όπως συμβαίνει και με τις κρυπτομηχανές.

Ο απαιτούμενος προγραμματισμός αυτόματης αλλαγής κλειδών κατά τακτά χρονικά διαστήματα [79] μπορεί να γίνει εύκολα μέσω λογισμικού, εφόσον στη μνήμη του Η/Υ υπάρχει ικανός αριθμός κλειδών (θα πρέπει να εγκαθίσταται στη μνήμη μαζικά αριθμός κλειδών, π.χ μέσω FILLGUN). Επίσης, η διατήρηση των κλειδών και μεταβλητών λειτουργίας σε περίπτωση διακοπής της ηλεκτρικής τροφοδοσίας θα πρέπει να υφίσταται για

τουλάχιστον 6 ώρες [78]. Αυτό σημαίνει ότι η συσκευή κρυπτογράφησης κανονικά θα πρέπει να διαθέτει μια μπαταρία, η οποία να κρατάει μονίμως την κύρια μνήμη στην οποία αποθηκεύονται τα δεδομένα σε λειτουργία (παρόλο που ο υπολογιστής μπορεί να απενεργοποιηθεί), έτσι ώστε τα δεδομένα να μην χαθούν σε περίπτωση απενεργοποίησης. Προφανώς στην περίπτωση του Η/Υ η μεταφορά των δεδομένων σε δευτερεύουσα μνήμη (σκληρός δίσκος ή NVRAM) κατά την απενεργοποίηση αποτελεί πιο εύκολη και εφαρμόσιμη πρακτική, ωστόσο θα πρέπει να ληφθούν μέτρα για την μη πρόσβαση στα δεδομένα από μη εξουσιοδοτημένο προσωπικό, στοιχείο που θα εξεταστεί στις προϋποθέσεις φυσικής ασφάλειας.

Το μέγεθος της ενεργούς κλείδας θα πρέπει να είναι τουλάχιστον 256 bits και ο αλγόριθμος κρυπτογράφησης εμπιστευτικότητας θα πρέπει να είναι απόρρητος αλγόριθμος του ΝΑΤΟ ή αλγόριθμος που πληροί τις προϋποθέσεις της Suite B [78]. Εδώ, θα πρέπει να γίνει είτε τροποποίηση του πηγαίου κώδικα του IP, όμως αποτελεί όπως είπαμε και παραπάνω για τους hosts εξαιρετικά μη πρακτική επιλογή, καθώς θα έπρεπε όλοι οι hosts στη στρατιωτική δομή να τροποποιηθούν εξίσου. Ένας απόρρητος αλγόριθμος θα μπορούσε να χρησιμοποιείται από το IPSec μέσω ενός προστιθέμενου module (όπως π.χ το CIK στην κρυπτομηχανή) (όπως περιγράφηκε στο κεφάλαιο 6) το οποίο επίσης εξυπηρετεί και μια προϋπόθεση φυσικής ασφάλειας, όπως θα δούμε και παρακάτω. Παρόλα αυτά, η τροποποίηση του Η/Υ ώστε να υπάρχει σε αυτόν η υποδομή για υποδοχή ενός τέτοιου module δεν είναι εύκολη. Θα απαιτούνταν ειδική προμήθεια από εταιρεία του NIAPC, όπως γίνεται και με τις κρυπτομηχανές. Κάθε τέτοια τροποποίηση επιφέρει επιπλέον κόστος, και φέρνει το κόστος προμήθειας ενός τέτοιου Η/Υ ακόμα πιο κοντά σε αυτό της κρυπτομηχανής. Εναλλακτικά, μπορεί να χρησιμοποιηθεί ο AES-256, εφόσον αποδεχθούμε την παραδοχή ότι η κρυπτογράφηση θα είναι διαβάθμισης μόνο έως “ΑΠΟΡΡΗΤΟ”, βάσει των ευρημάτων του κεφαλαίου 7.

Τα τρία ξεχωριστά επίπεδα διαχείρισης του Η/Υ στο δίκτυο (security officer, network manager, operator) μπορούν να υλοποιηθούν εύκολα μέσω του λειτουργικού συστήματος, με τον security officer να έχει πρόσβαση στο κρυπτογραφημένο δίκτυο, στο δίκτυο διαχείρισης καθώς και στη διαχείριση του Η/Υ, τον network manager να έχει πρόσβαση στα δύο αναφερθέντα δίκτυα αλλά όχι στη διαχείριση του Η/Υ και τον operator να είναι

απλά χρήστης του Η/Υ. Κάθε χρήστης θα έχει μοναδικό κωδικό πρόσβασης, και θα υπάρχει κεντρική διαχείριση των κωδικών πρόσβασης από την Αρχή Ασφαλείας της στρατιωτικής δομής.

Προϋποθέσεις συστήματος παραγωγής κλειδών

Και στην υλοποίηση του IPSec μέσω των hosts αλλά και σε αυτή μέσω των routers, οι κύριες κλείδες (master keys or primary keys) θα πρέπει να παράγονται εκτός των συσκευών από ειδικό σύστημα παραγωγής και ελέγχου, σύγχρονης τεχνολογίας [78]. Στην ουσία, η δημιουργία των κλειδών θα πρέπει να γίνεται από ξεχωριστό σύστημα εκτός του κρυπτογραφημένου δικτύου, και μετά να μοιράζεται είτε φυσικά (fillgun, πληκτρολόγιο) είτε μέσω του Κεντρικού Συστήματος Διαχείρισης. Η προμήθεια ενός τέτοιου συστήματος είναι αναπόφευκτη και για τις δύο πρακτικές, επομένως δεν έχει ιδιαίτερη σημασία η εξέταση αποφυγής η μείωσης του κόστους σε αυτή την περίπτωση.

Προϋποθέσεις Κεντρικού Συστήματος Διαχείρισης

Προαπαιτούμενο για τη λειτουργία του IPSec στις στρατιωτικές δομές είναι η ύπαρξη Κεντρικού Συστήματος Διαχείρισης (ΚΣΔ) για όλες τις συσκευές που υλοποιούν το IPSec στο δίκτυο [78]. Επομένως, για όλους τους hosts θα υπάρχει ένας κεντρικός host στον οποίο θα έχει πρόσβαση μόνο προσωπικό με δικαιώματα security officer, οι οποίοι μέσω ενός δεύτερου κρυπτογραφημένου δικτύου θα μπορούν να το εποπτεύουν και να διαχειρίζονται όλους τους υπολογιστές που συμμετέχουν σε αυτό μεμακρυσμένα. Όπως προειπώθηκε, θα πρέπει να μπορεί να κάνει την διανομή των κλειδών στους hosts καθώς και να προγραμματίζει την αυτόματη ανανέωσή τους μέσω χρονοπρογραμματισμού. Σημαντικό στοιχείο αποτελεί ότι πρέπει το ΚΣΔ να είναι διαθέσιμο πάντα 100%, άρα θα πρέπει να έχουν ληφθεί όλα τα απαραίτητα μέτρα προκειμένου να υπάρχει πάντα ένας server ως ΚΣΔ ενεργός στο δίκτυο. Η κυριότερη πρακτική είναι η ύπαρξη εφεδρικών servers, ανάλογα με τα failovers που παρατηρούνται στον server εντός ενός χρονικού διαστήματος, καθώς και η συνεχής υποστήριξή τους με τροφοδοσία ρεύματος (μπαταρία, UPS, ηλεκτροπαραγωγά ζεύγη). Οι παραπάνω ενέργειες για την διαθεσιμότητα του ΚΣΔ είναι

κοινές για κάθε τύπο ενσωμάτωσης του IPSec, επομένως η μείωση του κόστους τους ή η αποφυγή των ενεργειών αυτόν δεν χρήζει εξέτασης.

Προϋποθέσεις φυσικής ασφάλειας και αξιοπιστίας

Η υποχρεωτική συμβατότητα με την προδιαγραφή NATO SDIP-27 αποτελεί κατασκευαστική απαίτηση έτσι ώστε η συσκευή που υλοποιεί το IPSec (ο Η/Υ - host) να είναι ανθεκτικός στα φαινόμενα TEMPEST [78]. Επίσης, είναι υποχρεωτική η κατασκευή της σύμφωνα με τα πρότυπα MIL-STD 461 και 462 ή αντίστοιχες εκδόσεις της Ε.Ε. Εφόσον τα παραπάνω αποτελούν κατασκευαστικές απαιτήσεις, αυτό σημαίνει ότι το υλικό και η σχεδίαση της συσκευής θα πρέπει να είναι συμβατή με τα παραπάνω πρότυπα. Οι περισσότεροι Η/Υ του εμπορίου είναι συμβατικοί και δεν συνάδουν με τα πρότυπα αυτά, οπότε η ειδική παραγγελία για την κατασκευή μιας τέτοιας συσκευής είναι αναπόφευκτη, και όπως και το επιπλέον κόστος που επιβαρύνει. Μπορούμε μάλιστα να υποθέσουμε ότι, εφόσον ο σχεδιασμός και τα υλικά κατασκευής μιας συσκευής αποτελούν και τις κύριες αιτίες επιβάρυνσης του κόστους της, ότι το κόστος κατασκευής ενός Η/Υ αντί μιας κρυπτομηχανής με τα ίδια υλικά και την ίδια σχεδίαση, θα έχει περίπου το ίδιο κόστος, αν όχι μεγαλύτερο. Ο μόνος τρόπος να αποφευχθεί αυτό το κόστος προμήθειας είναι να διαχωριστούν οι ενδεχόμενες TEMPEST ζώνες έτσι ώστε να λειτουργούν σε αυτές συσκευές με πιθανόν μικρότερες κατασκευαστικές απαιτήσεις, δηλαδή π.χ αν μια συσκευή δεν προβλέπεται ότι θα λειτουργήσει εντός μιας ενδεχόμενης ζώνης TEMPEST, να μην κατασκευάζεται κατ' αυτό το πρότυπο. Δεδομένο όμως είναι ότι μια συσκευή IPSec η οποία ενδέχεται να λειτουργήσει σε πεδίο πολεμικών επιχειρήσεων θα θεωρείται ότι λειτουργεί σε TEMPEST Zone επιπέδου Α, επομένως όσες συσκευές πρόκειται να θεωρηθούν ως τέτοιες θα πρέπει να είναι κατασκευασμένες σύμφωνα με το παραπάνω πρότυπο κατασκευής TEMPEST.

Επίσης, σε περίπτωση απώλειας ή κλοπής ή καταστροφής μίας συσκευής IPSec, θα πρέπει να υπάρχει δυνατότητα η εν λόγω συσκευή να εξαιρεθεί από το δίκτυο [78]. Αυτό μπορεί να γίνει με την άμεση αλλαγή των κλειδών σε όλες τις συσκευές IPSec (Η/Υ -

hosts) και την εξαίρεση της IP του Η/Υ που εκλάπη έτσι ώστε να μην μπορεί να χρησιμοποιηθεί (θεωρούμε ότι κάθε Η/Υ έχει μοναδική IP, την οποία μπορεί να αλλάξει μόνο ο Administrator).

Θα πρέπει επίσης η συσκευή να διαθέτει τεχνική που να καθιστά αδύνατη την ανάγνωση των δεδομένων ασφαλείας της (tamper-proof design), είτε είναι σε τροφοδοσία, είτε είναι εκτός τροφοδοσίας και να διαθέτει μηχανισμό διαγραφής δεδομένων ασφαλείας επείγουσας ανάγκης, ο οποίος να μπορεί να εκτελεστεί χειροκίνητα ή να ενεργοποιηθεί αυτόματα όταν ανοίγεται το περίβλημα της συσκευής [78]. Αυτό σημαίνει ότι θα πρέπει να υπάρχει ειδικός μηχανισμός ο οποίος διαγράφει τα δεδομένα (κλείδες, παράμετροι κλπ) είτε χειροκίνητα μέσω ενός κομβίου είτε σε περίπτωση που ανιχνεύσει κάποιον κακόβουλο χρήστη (π.χ μετά από 3 ανεπιτυχείς προσπάθειες εισόδου ως Administrator ή οποιοσδήποτε χρήστης) είτε σε περίπτωση που προσπαθήσει κάποιος να ανοίξει το case του Η/Υ για να εξάγει από μέσα τα components (π.χ σκληρός δίσκος). Το τελευταίο είναι πολύ δύσκολο να γίνει χωρίς ο Η/Υ να είναι σε λειτουργία, επομένως θα πρέπει κάποια τμήματα του Η/Υ να παραμένουν σε λειτουργία αυτοτελώς (όπως π.χ η μνήμη που συγκρατεί τα δεδομένα) έτσι ώστε να ανιχνεύουν την προσπάθεια “διάρρηξης” του υπολογιστή μέσω αισθητήρων και να διαγράφουν αυτομάτως τα δεδομένα αν επιχειρηθεί κάτι τέτοιο. Αναφέραμε στις προϋποθέσεις λογικής ασφάλειας την απαίτηση για ύπαρξη μπαταρίας η οποία θα διατηρεί τις κλείδες και τις μεταβλητές λειτουργίας (set-up) σε περιπτώσεις διακοπών της ηλεκτρικής τροφοδοσίας της συσκευής, για τουλάχιστον 6 ώρες. Επομένως, φτάνουμε στο συμπέρασμα ότι και για τον Η/Υ - host, η ύπαρξη μιας τέτοιας διάταξης είναι απαραίτητη και για λόγους tamper-proof designing, μαζί με το επιπλέον κόστος εφαρμογής του tamper-proof design και της διάταξης αυτής.

Απαραίτητη προϋπόθεση φυσικής ασφάλειας για τον Η/Υ - host είναι επίσης η ύπαρξη κλειδιού ενεργοποίησης (μηχανικό ή τύπου κάρτας ή software) χωρίς το οποίο να είναι αδύνατη η λειτουργία του. Η εφαρμογή ενός τέτοιου μηχανισμού δεν είναι συνήθης και πρέπει να γίνει και εδώ ειδική κατασκευή, της οποίας το κόστος επιβαρύνεται εάν το κλειδί πρέπει να εμπεριέχει και δεδομένα τα οποία είναι κρίσιμα για τη λειτουργία του IPSec (όπως π.χ ο αλγόριθμος κρυπτογράφησης ο οποίος αναφέρθηκε παραπάνω).

Μία ακόμα κατασκευαστική απαίτηση του NATO για τις συσκευές IPSec αποτελεί ότι η ελάχιστη αποδεκτή Mean Time Between Failures (MTBF) μιας συσκευής IPSec είναι οι 20.000 ώρες. Το πως η συσκευή (H/Y - host) εκπληρώνει αυτό το στόχο θα πρέπει να υπολογιστεί σύμφωνα με το πρότυπο MILHDBK 217F (ή νεώτερη έκδοση) των ΗΠΑ ή με άλλη αντίστοιχη έκδοση [78]. Η μελέτη και ο σχεδιασμός της συσκευής ώστε να εκπληρώνει και αυτό το κριτήριο αποτελεί και αυτό ένα επιπλέον κόστος για την παραγωγή της.

Από τα παραπάνω μπορούμε να δούμε ότι λόγω ειδικών απαιτήσεων του NATO, το κόστος μιας συσκευής IPSec είτε είναι κρυπτομηχανή είτε είναι host είναι σχεδόν το ίδιο, μιας και οι παραπάνω απαιτήσεις είναι κατασκευαστικές και απαιτούν ειδικό σχεδιασμό της συσκευής.

9.3.1 Πλεονεκτήματα και μειονεκτήματα της πρακτικής

Ένα σημαντικό πλεονέκτημα ενσωμάτωσης του IPSec στους hosts σε μια στρατιωτική δομή αποτελεί το γεγονός ότι το κρυπτογραφημένο δίκτυο (ciphertext domain) σε αυτή την περίπτωση εκτείνεται ως τους hosts, και δεν υπάρχει η ανάγκη να διασπαστεί σε κρυπτογραφημένη και μη κρυπτογραφημένη πλευρά. Αυτό επιτρέπει την παροχή end-to-end ασφάλειας μεταξύ δύο οποιωνδήποτε συσκευών στο δίκτυο. Επίσης, προσφέρει επαυξημένη ευελιξία, καθώς στο πεδίο της μάχης δεν θα απαιτείται η χρήση επιπλέον συσκευής όπως η κρυπτομηχανή για την IP συνδεσιμότητα, αλλά μόνο ο H/Y - host μέσω του οποίου θα γίνεται η σύνδεση. Η ενσωμάτωση του IPSec στον host επίσης προσφέρει τη δυνατότητα δημιουργίας προσωποποιημένων προφίλ στο δίκτυο, καθώς για διαφορετικό λογαριασμό χρήστη θα μπορούν να χρησιμοποιούνται διαφορετικές κλείδες - παράμετροι. Έτσι, μπορεί να παρακολουθείται πιο εύκολα η δραστηριότητα του συγκεκριμένου χρήστη στο δίκτυο και να παρέχεται πιο εύκολα η γνώση γύρω από το ποιος επιχείρησε μια κακόβουλη ενέργεια.

Τα μειονεκτήματα της πρακτικής αυτής όμως είναι πολλά και ιδιαίτερα σημαντικά. Ένα σημαντικό μειονέκτημα αποτελεί το γεγονός ότι, για να μην υπάρχει εμπλοκή του χρήστη στη διαδικασία του IPSec (π.χ για να μην χρειάζεται να ενεργοποιεί ένα λογισμικό ή να πληκτρολογεί κάποιο κωδικό, δηλαδή η διαδικασία να γίνεται εν αγνοία του χρήστη) θα

πρέπει, όπως αναφέρθηκε και παραπάνω, να μεταβληθεί ο πηγαίος κώδικας IP σε όλες τις IP συσκευές που συμμετέχουν στο δίκτυο. Αν αναλογιστούμε πόσες IP συσκευές συμμετέχουν σε ένα δίκτυο, μπορούμε να καταλάβουμε ότι κάτι τέτοιο θα απαιτούσε πάρα πολύ χρόνο για την υλοποίησή του και θα προκαλούσε πολλά προβλήματα στην επικοινωνία στη φάση μετάβασης, οπότε θα ήταν μια μη ολοκληρώσιμη πρακτική. Επομένως, η ενσωμάτωση του IPSec στον host μπορεί να γίνει μόνο ως Bump-In-The-Stack, όμως αυτό σημαίνει ότι ο χρήστης θα πρέπει να συμμετέχει ενεργά στη διαδικασία του IPSec, και ως εκ τούτου θα πρέπει να είναι εξουσιοδοτημένος από την Αρχή Ασφαλείας της στρατιωτικής δομής για γνώση - χρήση εγγράφων και υλικού με διαβάθμιση "ΑΠΟΡΡΗΤΟ" [96]. Άρα, οι εξουσιοδοτημένοι χρήστες θα πρέπει να είναι πολύ περισσότεροι, εφόσον οι hosts είναι θεωρητικά πολύ περισσότεροι σε αριθμό από ότι οι gateways (άρα και οι κρυπτομηχανές) σε ένα intranet.

Το σημαντικότερο μειονέκτημα όμως αυτής της πρακτικής είναι το υπέρογκο κόστος της. Αναλύσαμε παραπάνω το πως οι hosts σε μια στρατιωτική δομή μπορούν να ικανοποιήσουν τις απαιτήσεις που θέτει το NATO γύρω από την κατασκευή - λειτουργία μιας IPSec συσκευής. Το κυριότερο συμπέρασμα είναι ότι οι απαιτήσεις φυσικής σχεδίασης (διαφορετικά κυκλώματα red/black), λογικής ασφάλειας (εισαγωγή κλειδών μέσω fillgun, module μυστικού αλγορίθμου), φυσικής ασφάλειας (συμβατότητα με το TEMPEST πρότυπο NATO SDIP-27, tamper-proof design, κλειδί ενεργοποίησης) και αξιοπιστίας (MTBF 20.000 ωρών) αυξάνουν σημαντικά το κόστος προμήθειας ενός τέτοιου συστήματος. Αν θεωρήσουμε πως μια κρυπτομηχανή (με τις λειτουργίες και δυνατότητές της) έχει ένα κόστος x, τότε η σχεδίαση, ανάπτυξη και παραγωγή ενός Η/Υ ο οποίος έχει επιπλέον αυτές τις δυνατότητες και λειτουργίες της κρυπτομηχανής και είναι ομοίως κατασκευασμένος, θα έχει κόστος x + y όπου y οι λειτουργίες και δυνατότητες του συστήματος καθαρά

---

[96] Με τον όρο εξουσιοδότηση προσωπικού, για το χειρισμό διαβαθμισμένων πληροφοριών και υλικού, νοείται το έγγραφο που εκδίδεται από την αρμόδια αρχή, με το οποίο πιστοποιείται η δυνατότητα του συγκεκριμένου προσωπικού αφ'ενός να λαμβάνει γνώση διαβαθμισμένων πληροφοριών και υλικού, αφ'ετέρου δε να τα χειρίζεται με την εχεμύθεια και μυστικότητα που επιβάλλεται από το χαρακτηρισμό τους ως διαβαθμισμένων [84].

ως Η/Υ. Επομένως, καταλαβαίνουμε ότι το κόστος (το οποίο βέβαια εξαρτάται και από άλλους παράγοντες όμως δεν αποτελούν αντικείμενο εξέτασης στην παρούσα εργασία) ενός IPSec host είναι πιθανώς μεγαλύτερο από αυτό της κρυπτομηχανής. Ωστόσο, αυτό που επαυξάνει το κόστος σημαντικά είναι η (θεωρητικά) ύπαρξη πολλών περισσότερων host σε ένα intranet από gateways. Αυτό σημαίνει ότι για το ίδιο intranet μιας στρατιωτικής δομής, αν αυτό χτιζόταν από την αρχή, η προμήθεια των Η/Υ σε αριθμό θα ήταν πολύ μεγαλύτερη από αυτή των routers. Επομένως, καταλαβαίνουμε ότι το κόστος αυτής της πρακτικής είναι σημαντικά πολλαπλάσιο από αυτό της υλοποίησης του IPSec ως Bump-In-The-Wire, και δεν μπορεί επομένως η υλοποίηση αυτή να αφορά το δίκτυο στην ολότητά του. Θεωρητικά, θα μπορούσε μια στρατιωτική δομή να προμηθευτεί μόνο έναν αριθμό Η/Υ οι οποίοι πληρούν τις προϋποθέσεις μιας IPSec συσκευής και είναι συμβατοί με τις υπάρχουσες IPSec συσκευές στο δίκτυο, προκειμένου να εκμεταλλευτεί τα πλεονεκτήματα που αυτή η πρακτική παρέχει, σε περιπτώσεις που απαιτείται επαυξημένη ευελιξία - κινητικότητα ενός τμήματος.

9.4 Δυνατότητα ενσωμάτωσης του IPSec στον router στα στρατιωτικά δίκτυα IP

Στην ενσωμάτωση του IPSec ως Bump-In-The-Wire, όπως έχει αναφερθεί, χρησιμοποιείται μια ειδική IPSec συσκευή (κρυπτομηχανή) στην εξωτερική πλευρά του router, προκειμένου να προστίθενται οι IPSec ιδιότητες στα datagrams. Σε αυτή την ενότητα, θα εξετάσουμε την δυνατότητα ενσωμάτωσης των λειτουργιών της IPSec συσκευής απευθείας στον router. Στην ουσία, θα έχει τροποποιηθεί ο πηγαίος κώδικας των routers έτσι ώστε στο επίπεδο IP να προστίθενται και οι IPSec ιδιότητες. Επομένως, θα εξεταστεί το πως είναι δυνατή η εκπλήρωση των προϋποθέσεων του NATO που αναφέρθηκαν στο κεφάλαιο 8 από αυτή την πρακτική και θα αναλυθούν τα πλεονεκτήματα και μειονεκτήματα της πρακτικής αυτής, όπως και με τους hosts.

Προϋποθέσεις φυσικής σχεδίασης

Κάθε δρομολογητής ο οποίος θα υποστηρίζει το IPSec θα πρέπει να έχει διαφορετικά κυκλώματα για την Red και Black πλευρά, με ξεχωριστές γραμμές τροφοδοσίας και ξεχωριστή πηγή τροφοδότησης, όπως συμβαίνει στην κρυπτομηχανή [78]. Από πλευράς φυσικής σχεδίασης, δεν υπάρχουν τέτοιοι διαθέσιμοι δρομολογητές στο εμπόριο, επομένως θα πρέπει να γίνει ειδική παραγγελία και προμήθεια δρομολογητών ανάλογου σχεδιασμού, με το κόστος του σχεδιασμού και της υλοποίησης των παραπάνω να αυξάνεται, ακριβώς όπως και στην περίπτωση του host.

Θα πρέπει επίσης ο κάθε router να διαθέτει αυτοέλεγχο BITE κατά την εκκίνηση του (POST), αυτόματα κατά την διάρκεια λειτουργίας του (ON LINE) καθώς και μέσω εντολής χειριστού όποτε απαιτείται ενώ η συσκευή βρίσκεται σε ουδέτερη κατάσταση αναμονής (idle position) [78]. Όπως και με τον host, ο αυτοέλεγχος γίνεται για τη διαπίστωση ότι οι μηχανισμοί - λογισμικό που χρησιμοποιείται για το IPSec βρίσκεται σε λειτουργία και η κρυπτογράφηση είναι “οπλισμένη”. Αυτό μπορεί να υλοποιηθεί με την τροποποίηση του λογισμικού του router ώστε να διενεργεί τον αυτοέλεγχο όπως και η κρυπτομηχανή. Ωστόσο, κάτι τέτοιο δεν αποτελεί στάνταρ διαδικασία για ένα κοινό δρομολογητή, και η εφαρμογή του στον δρομολογητή - κρυπτομηχανή της περίπτωσής μας έχει επιπλέον κόστος.

Προϋποθέσεις δυνατοτήτων επικοινωνίας

Επίσης, σύμφωνα με τις προϋποθέσεις δυνατοτήτων επικοινωνίας που ορίζει το NATO για τις συσκευές IPSec (στην περίπτωση αυτή κάθε δρομολογητής - κρυπτομηχανή) θα πρέπει αυτές να υλοποιούν Full Duplex επικοινωνία με ταχύτητα τουλάχιστον 100 Mbps σε Ethernet interface [79]. Οι περισσότεροι δρομολογητές τελευταίας τεχνολογίας που κυκλοφορούν στο εμπόριο, όπως π.χ οι Cisco 880 Series, διαθέτουν θύρες ethernet τουλάχιστον 10mbps/100mbps.

Επίσης, απαιτείται η ύπαρξη διαφορετικών διεπαφών για την ανοιχτή και κρυπτογραφημένη πλευρά. Δηλαδή, ένας router που υποστηρίζει π.χ μια στρατιωτική μονάδα θα

πρέπει να διαθέτει δύο διεπαφές: μία για το εσωτερικό δίκτυο, δηλαδή τη μη κρυπτογραφημένη πλευρά, και μία για το εξωτερικό δίκτυο, δηλαδή για την κρυπτογραφημένη πλευρά. Οι κεντρικοί routers οι οποίοι ενώνουν τα υποδίκτυα των διάφορων μονάδων δεν απαιτείται να έχουν δύο interfaces για κάθε μονάδα (δρομολογητή) που συνδέεται μαζί τους, αλλά μόνο μία interface για την καθεμία, που θα αντιστοιχεί στην κρυπτογραφημένη πλευρά τους. Μόνο αν κάποιος δρομολογητής υποστηρίζει απευθείας κάποιο plaintext δίκτυο (αν δηλαδή τα δεδομένα πρέπει να αποκρυπτογραφηθούν και να παρουσιαστούν σε υποδίκτυο από hosts) θα πρέπει να διαθέτει και μία interface που θα συνδέεται με το plaintext δίκτυο. Αν υποθέσουμε ότι όλοι οι δρομολογητές υποστηρίζουν μη κρυπτογραφημένη πλευρά, θα πρέπει να διαθέτουν όλοι μία interface για το plaintext δίκτυο και όλες τις υπόλοιπες για τα ciphertext δίκτυα με τα οποία συνδέονται με τους λοιπούς δρομολογητές. Εφόσον μία από τις interfaces του δρομολογητή δεσμευτεί για αυτό το σκοπό, αυτή η προϋπόθεση εκπληρώνεται, ωστόσο συνάδει με την κατασκευαστική προϋπόθεση της συμμόρφωσης με το πρότυπο NATO SDIP-27, που θα δούμε παρακάτω.

Μια ακόμη προυπόθεση αποτελεί το ότι κάθε δρομολογητής - κρυπτομηχανή του δικτύου θα πρέπει να μπορεί να υλοποιεί ταυτόχρονα τουλάχιστον 1000 συσχετίσεις ασφαλείας (SAs) και να μπορεί να λειτουργεί και να συνεργάζεται σε δίκτυο τουλάχιστον 1000 IPsec συσκευών [78]. Όπως εξηγήθηκε και στην περίπτωση των hosts, θα πρέπει να υπάρχει ικανός χώρος στη RAM του υπολογιστή που να φιλοξενεί τουλάχιστον 1000 SAs (μαζί με τη μνήμη που απαιτείται για τις λοιπές διεργασίες), επομένως και σε αυτή την περίπτωση, τουλάχιστον 1 mb της μνήμης RAM του δρομολογητή θα πρέπει να δεσμεύεται για τη λειτουργία της SAD.

Επίσης, τυχόν αναβαθμίσεις του λογισμικού του δρομολογητή θα πρέπει να μπορούν να γίνουν τοπικά ή μεμακρυσμένα μέσω Κεντρικού Συστήματος Διαχείρισης. Όπως θα εξηγήσουμε και παρακάτω, θα πρέπει να υπάρχει και δεύτερο κρυπτογραφημένο δίκτυο σε κάθε δρομολογητή, το οποίο θα χρησιμοποιείται μόνο από το ΚΣΔ για αυτό το σκοπό.

Προϋποθέσεις λογικής ασφάλειας

Όπως και στην κρυπτομηχανή, θα πρέπει και στον δρομολογητή - κρυπτομηχανή που θα σχεδιαστεί και θα αναπτυχθεί να μπορούν να εισαχθούν οι κλείδες με συσκευές fillgun/smart cards καθώς και μεμακρυσμένα μέσω ΚΣΔ, με την αλλαγή - ανανέωση - χρονοπρογραμματισμό αυτόματης αλλαγής κλειδών να μπορεί να γίνει τόσο από το χειριστή του δρομολογητή όσο και από το ΚΣΔ [78]. Οι routers εμπορίου που υποστηρίζουν το IPSec συνήθως δεν υποστηρίζουν την εισαγωγή κλειδών με αυτό τον τρόπο, οπότε αυτό είναι μια κατασκευαστική αλλά και προγραμματιστική απαίτηση η οποία θα πρέπει να συμπληρωθεί από τον κατασκευαστή, με επιπλέον κόστος, όπως και με την περίπτωση των hosts. Η αλλαγή των κλειδών και οι λοιπές ενέργειες που αναφέρθηκαν παραπάνω θα μπορούν να γίνουν από το ΚΣΔ για όλους τους δρομολογητές του δικτύου μέσω της υλοποίησης ενός δεύτερου κρυπτογραφημένου δικτύου, με τη χρήση ξεχωριστής κλείδας κρυπτογράφησης.

Επίσης, όπως εξηγήθηκε και στην περίπτωση των hosts, θα πρέπει ο δρομολογητής να μπορεί να αποθηκεύει τα δεδομένα των κλειδών - μεταβλητών λειτουργίας για τουλάχιστον 6 ώρες σε περίπτωση διακοπής της ηλεκτρικής τροφοδοσίας [78]. Αυτό μπορεί να γίνει εύκολα με την NVRAM του router, ωστόσο η παρακάτω απαίτηση του tamper-proof design του δρομολογητή δεν συνάδει με τη χρήση της NVRAM, καθώς ο δρομολογητής θα πρέπει να παραμένει “ζωντανός” για να μπορεί να διαπιστώσει προσπάθειες παραβίασης, άρα η NVRAM ή οποιαδήποτε μνήμη που συγκρατεί τα δεδομένα χωρίς τροφοδοσία δεν μπορεί να χρησιμοποιηθεί σε αυτή την περίπτωση. Θα πρέπει να χρησιμοποιηθεί για αυτό το σκοπό μνήμη RAM, η οποία τροφοδοτείται με ξεχωριστή μπαταρία, το επίπεδο της οποίας ελέγχεται διαρκώς από το bite και η οποία φορτίζεται από την τροφοδοσία ρεύματος. Επίσης, θα πρέπει να υπάρχει η δυνατότητα αυτόματης προσωρινής αποθήκευσης των δεδομένων σε άλλη μνήμη προκειμένου να αλλαχτεί η μπαταρία που αναφέρθηκε, για λόγους συντήρησης. Αυτό αποτελεί προγραμματιστική απαίτηση και μπορεί να υλοποιηθεί εύκολα από τον κατασκευαστή, χωρίς ιδιαίτερο κόστος.

Και σε αυτή την περίπτωση, το μέγεθος της ενεργούς κλείδας θα πρέπει να είναι τουλάχιστον 256 bits και ο αλγόριθμος κρυπτογράφησης εμπιστευτικότητας θα πρέπει να είναι απόρρητος αλγόριθμος του ΝΑΤΟ ή αλγόριθμος που πληροί τις προϋποθέσεις της

Suite B [78]. Στην περίπτωση του router όμως, επειδή οι routers είναι σημαντικά λιγότεροι από τους hosts σε ένα δίκτυο, και επειδή τα IPSec datagrams κυκλοφορούν μόνο στην κρυπτογραφημένη πλευρά, η τροποποίηση του πηγαίου κώδικα των routers ώστε να μπορούν να υλοποιήσουν συγκεκριμένους αλγορίθμους με συγκεκριμένο μέγεθος κλείδας είναι πιο εύκολη. Ωστόσο, υπάρχει η κατασκευαστική απαίτηση ύπαρξης κλειδιού ενεργοποίησης της συσκευής ως κρυπτοσυσκευή στις προϋποθέσεις φυσικής ασφάλειας. Στην ουσία αυτό σημαίνει πως με την απουσία του κλειδιού η κρυπτογράφηση θα πρέπει να είναι απούσα (null) από το πακέτο που εξέρχεται από το δρομολογητή, η συσκευή όμως θα πρέπει να εξακολουθεί να μπορεί να λειτουργεί ως δρομολογητής. Επομένως, ο αλγόριθμος κρυπτογράφησης θα πρέπει να βρίσκεται μέσα στο κλειδί - module που θα χρησιμοποιείται (π.χ CIK) ως δεδομένο το οποίο θα χρησιμοποιεί ο router για να κρυπτογραφήσει το payload των datagrams. Ως προγραμματιστική απαίτηση, το κόστος υλοποίησης δεν είναι μεγάλο, όμως ως κατασκευαστική απαίτηση (υποδοχή κλειδιού - δημιουργία μοναδικού κλειδιού για κάθε συσκευή) το κόστος εφαρμογής της από τον κατασκευαστή στο δρομολογητή - κρυπτομηχανή που θα παραχθεί είναι υπολογίσιμο, καθώς αυτή η διάταξη δεν είναι συνήθης πρακτική και δεν βρίσκεται εύκολα στο εμπόριο.

Επίσης, τα τρία ξεχωριστά επίπεδα διαχείρισης του δρομολογητή - κρυπτομηχανής στο δίκτυο (security officer, network manager, operator) μπορούν να υλοποιηθούν εύκολα μέσω του λογισμικού του δρομολογητή, για κάθε δρομολογητή, με τη δημιουργία κατηγοριών user. Το logging επίσης των ενεργειών του δρομολογητή υπάρχει σαν δυνατότητα σε κάθε σύγχρονο δρομολογητή, όμως πρέπει να προστεθούν σε αυτό και οι ενέργειες γύρω από το IPSec.

Προϋποθέσεις συστήματος παραγωγής κλειδών - ΚΣΔ

Σε αυτές τις κατηγορίες ισχύει ότι έχει αναλυθεί και στην περίπτωση των hosts, με το κόστος υλοποίησης να μην παρουσιάζει διαφορές σε κάθε περίπτωση.

Προϋποθέσεις φυσικής ασφάλειας και αξιοπιστίας

Και στην περίπτωση ενσωμάτωσης του IPSec στον δρομολογητή, υπάρχουν οι κατασκευαστικές απαιτήσεις συμβατότητας με την προδιαγραφή NATO SDIP-27 (φαινόμενα TEMPEST) και τις προδιαγραφές MIL-STD 461/462. Επομένως, τα υλικά κατασκευής και η σχεδίαση των δρομολογητών - κρυπτομηχανών θα πρέπει να συμβαδίζουν με τα παραπάνω πρότυπα. Εφόσον πρόκειται για κατασκευαστικές απαιτήσεις, είναι δεδομένο πως αυξάνουν το κόστος παραγωγής μιας τέτοιας συσκευής, το οποίο είναι ανάλογο της ζώνης TEMPEST στην οποία προβλέπεται να χρησιμοποιηθεί ο δρομολογητής.

Σε περίπτωση απώλειας ή κλοπής ή καταστροφής ενός δρομολογητή - κρυπτομηχανής, θα πρέπει να υπάρχει δυνατότητα η εν λόγω συσκευή να εξαιρεθεί από το δίκτυο [78]. Για να γίνει αυτό, θα πρέπει άμεσα να αλλαχτούν οι κλείδες - παράμετροι του IPSec σε όλες τις συσκευές IPSec. Επίσης, κάθε συσκευή θα πρέπει να διαθέτει ένα reference ID το οποίο θα στέλνει ως παράμετρο σε κάθε datagram, έτσι ώστε να γίνεται γνωστή η IPSec συσκευή που “εκπέμπει” ένα IP πακέτο. Με βάση αυτό το αναγνωριστικό, θα μπορεί να γίνει και η εξαίρεση της συσκευής από το δίκτυο.

Ο δρομολογητής - κρυπτομηχανή θα πρέπει επίσης να είναι σχεδιασμένος έτσι ώστε να καθιστά αδύνατη την ανάγνωση των δεδομένων ασφαλείας της (tamper-proof design), είτε είναι σε τροφοδοσία, είτε είναι εκτός τροφοδοσίας και να διαθέτει μηχανισμό διαγραφής δεδομένων ασφαλείας επείγουσας ανάγκης, ο οποίος να μπορεί να εκτελεστεί χειροκίνητα ή να ενεργοποιηθεί αυτόματα όταν ανοίγεται το περίβλημα της συσκευής [78]. Επομένως, θα πρέπει και σε αυτή την περίπτωση να υπάρχει ειδικός μηχανισμός ο οποίος διαγράφει τα δεδομένα (κλείδες, παράμετροι κλπ) είτε χειροκίνητα μέσω ενός κομβίου είτε σε περίπτωση που ανιχνεύσει κάποιον κακόβουλο χρήστη (π.χ μετά από 3 ανεπιτυχείς προσπάθειες εισόδου ως Administrator ή οποιοσδήποτε χρήστης) είτε σε περίπτωση που προσπαθήσει κάποιος να ανοίξει το περίβλημα του δρομολογητή για να ανακτήσει τα δεδομένα από τις μνήμες του. Όπως προαναφέρθηκε, θα πρέπει να υπάρχουν ειδικοί αισθητήρες οι οποίοι να συνδέονται με τη μνήμη του δρομολογητή που εμπεριέχει τα κρίσιμα δεδομένα, και σε ανίχνευση ύποπτων κινήσεων αυτά να διαγράφονται αυτομάτως, επομένως η ύπαρξη μπαταρίας τροφοδοσίας των αισθητήρων και της μνήμης αυτής είναι επιβεβλημένη, για να μπορεί να ανιχνεύεται κάθε ύποπτη κίνηση και σε περίπτωση που

ο δρομολογητής είναι εκτός λειτουργίας ή εκτός τροφοδοσίας. Άρα και εδώ όπως και στον host υπάρχει αυτή η κατασκευαστική απαίτηση η οποία εκπληρώνει την προυπόθεση του tamper-proof design αλλά και αυτή της αποθήκευσης των κλειδών για διάστημα 6 ωρών. Η εκπλήρωση αυτής της απαίτησης επιφέρει επιπλέον κόστος για την παραγωγή της συσκευής.

Μία ακόμη απαραίτητη προϋπόθεση φυσικής ασφάλειας για τον δρομολογητή - κρυπτομηχανή όπως αναφέρθηκε και παραπάνω είναι η ύπαρξη κλειδιού ενεργοποίησης (μηχανικό ή τύπου κάρτας ή software) χωρίς το οποίο να είναι αδύνατη η λειτουργία του. Και αυτή η κατασκευαστική απαίτηση επιφέρει για την παραγωγή της συσκευής επιπλέον κόστος

Και σε αυτή την περίπτωση, η ελάχιστη αποδεκτή Mean Time Between Failures (MTBF) μιας συσκευής IPSec είναι οι 20.000 ώρες, υπολογισμένες σύμφωνα με το πρότυπο MILHDBK 217F (ή νεώτερη έκδοση) των ΗΠΑ ή με άλλη αντίστοιχη έκδοση [78]. Όπως και στους hosts, η μελέτη και ο σχεδιασμός της συσκευής ώστε να εκπληρώνει και αυτό το κατασκευαστικό κριτήριο αποτελεί και αυτό ένα επιπλέον κόστος για την παραγωγή της.

Το κύριο συμπέρασμα από τα παραπάνω είναι ότι και στην περίπτωση του δρομολογητή, το κόστος επηρεάζεται από τις ειδικές κατασκευαστικές απαιτήσεις και πιθανώς ξεπερνάει αυτό της κρυπτομηχανής.

9.4.1 Πλεονεκτήματα και μειονεκτήματα της πρακτικής

Η πρακτική αυτή, όπως και αυτή του host, έχει τα δικά της υπέρ και κατά. Το κύριο πλεονέκτημα της πρακτικής αυτής είναι ότι προσεγγίζει αρκετά την ήδη υπάρχουσα πρακτική με τη χρήση των κρυπτομηχανών, καθώς η αρχιτεκτονική IPSec που χρησιμοποιείται είναι πάλι η gateway-to-gateway. Αυτό σημαίνει ότι η υλοποίηση της πρακτικής αυτής μπορεί να γίνει σταδιακά με την αντικατάσταση των routers από IPSec routers οι οποίοι θα είναι συμβατοί με τις ήδη υπάρχουσες κρυπτομηχανές, έτσι ώστε να μην δημιουργούνται προβλήματα στην επικοινωνία κατά την μετάβαση στο νέο μοντέλο.

Επίσης, σημαντικό πλεονέκτημα της πρακτικής αυτής είναι ότι μειώνει σε σημαντικό ποσοστό των αριθμό των συσκευών που είναι απαραίτητες για τη λειτουργία του δικτύου. Κάθε δρομολογητής στην παρούσα υλοποίηση συνοδεύεται από μία κρυπτομηχανή, ενώ με την νέα υλοποίηση, υπάρχει μόνο ένας δρομολογητής - κρυπτομηχανή που αντικαθιστά το παραπάνω ζευγάρι. Λιγότερες συσκευές στο δίκτυο σημαίνει μικρότερη πιθανότητα εμφάνισης βλαβών και λιγότερες απαιτήσεις συντήρησης, άρα μεγαλύτερη διαθεσιμότητα του δικτύου.

Για την πρακτική αυτή, ένα σημαντικό μειονέκτημα είναι η απόδοση του δικτύου. Στην περίπτωση που χρησιμοποιείται ξεχωριστή συσκευή IPSec, η ταχύτητα της κρυπτογράφησης στο δίκτυο ενισχύεται από την ύπαρξη ξεχωριστού επεξεργαστή για το σκοπό αυτό (ο επεξεργαστής της κρυπτομηχανής) [84, 86]. Δε συμβαίνει το ίδιο αν το IPSec είναι ενσωματωμένο στον router (ή στον host), καθώς ο ίδιος επεξεργαστής χρησιμοποιείται και για τις λειτουργίες της συσκευής ως router. Έτσι, προστίθεται ένα επιπλέον βάρος στον επεξεργαστή του δρομολογητή, και θεωρητικά η διάταξη του router μαζί με κρυπτομηχανή ως ζεύγος είναι ταχύτερη από την χρήση ενός ενιαίου IPSec router. Η επίδραση στην ταχύτητα του δικτύου θα είναι πιο εμφανής σε real-time εφαρμογές (όπως π.χ live streaming από κάμερες παρακολούθησης των κινήσεων του εχθρού) οι οποίες είναι πολλές φορές κρίσιμες για την έκβαση των πολεμικών επιχειρήσεων. Παρόλα αυτά, εάν ενισχυθεί η υπολογιστική δύναμη του IPSec router (που σημαίνει επιπλέον κόστος), το πρόβλημα της ταχύτητας ενδέχεται να ξεπεραστεί.

Το κόστος όμως αποτελεί και εδώ το σημαντικότερο μειονέκτημα. Όπως και στην περίπτωση του host, οι μεγάλες κατασκευαστικές και σχεδιαστικές απαιτήσεις που θέτει το ΝΑΤΟ και αναλύθηκαν παραπάνω επαυξάνουν σημαντικά το κόστος παραγωγής ενός router - δρομολογητή, και το κάνουν πιθανότατα μεγαλύτερο της κρυπτομηχανής, καθώς τόσο τα routing capabilities της συσκευής όσο και η πολυπλοκότητά σχεδίασής της συντελούν σε αυτό. Παρόλα αυτά, όσον αφορά το κόστος, η ενσωμάτωση του IPSec στον router πλεονεκτεί έναντι της ενσωμάτωσης στον host, καθώς ο αριθμός των συσκευών για προμήθεια δεν μπορεί να προσεγγίσει καν τον αριθμό των Η/Υ που θα χρειαζόντουσαν αντικατάσταση στην αντίστοιχη περίπτωση. Επομένως, εφόσον το κόστος είναι πιο βιώσιμο από αυτό της υλοποίησης στους hosts, η μετάβαση μπορεί να γίνει σε αργούς

ρυθμούς και χωρίς να επιβαρύνεται σημαντικά ο προϋπολογισμός του αντίστοιχου κράτους - μέλους του NATO, εφόσον η πρακτική αυτή είναι συμβατή με την Bump-In-The-Wire υλοποίηση.

9.5 Συμπεράσματα

Στο κεφάλαιο αυτό αναλύθηκαν οι τύποι ενσωμάτωσης του IPSec έτσι ώστε να παρουσιαστούν οι εναλλακτικές επιλογές μοντέλων μετάβασης από το μοντέλο Bump-In-The-Wire. Προκειμένου να εξεταστεί το ενδεχόμενο μετάβασης μιας δομής του NATO σε ένα άλλο μοντέλο ενσωμάτωσης IPSec, έπρεπε να ληφθούν υπόψιν οι απαιτήσεις του NATO όσον αφορά τη σχεδίαση, αρχιτεκτονική και λειτουργία των συσκευών IPSec, οι οποίες διαπιστώθηκαν στη μεγαλύτερη έκτασή τους από την εξέταση των συσκευών του NIAPC και τη διεξαγωγή συμπερασμάτων. Με τα ευρήματα αυτά, αναλύθηκε το πως οι συσκευές που αντιστοιχούν στα άλλα μοντέλα υλοποίησης (IPSec host ή IPSec router) μπορούν να ενσωματώσουν στη λειτουργία, σχεδίαση και αρχιτεκτονική τους τις απαιτήσεις του NATO. Βάσει της ανάλυσης αυτής, καταλήγουμε στα παρακάτω συμπεράσματα:

- Το μοντέλο ενσωμάτωσης στους host, παρόλο που παρέχει το πολύ ισχυρό πλεονέκτημα της end-to-end παροχής υπηρεσιών ασφαλούς επικοινωνίας, είναι πολύ δύσκολο να εφαρμοστεί λόγω του ότι το κόστος της προμήθειας των συσκευών που απαιτούνται για την υλοποίηση αυτή υπερβαίνει κατά πολύ το κόστος προμήθειας των κρυπτομηχανών που απαιτούνται για την αρχική υλοποίηση.
- Το μοντέλο ενσωμάτωσης στους routers, συγκριτικά με το μοντέλο Bump-In-The-Wire, φέρει το σημαντικό μειονέκτημα μη ύπαρξης ξεχωριστού επεξεργαστή για τις διεργασίες κρυπτογράφησης. Το γεγονός αυτό συν το ότι η πολυπλοκότητα της συσκευής ενδέχεται να απαιτεί μεγαλύτερη υπολογιστική δύναμη για τις διάφορες διεργασίες της συντελεί στη μείωση της ταχύτητας κρυπτογράφησης, άρα και απόδοσης στο δίκτυο συνολικά [86, 87]. Επομένως, προτού επιχειρηθεί μια μετάβαση από το μοντέλο Bump-In-The-Wire στο μοντέλο ενσωμάτωσης στους routers, θα πρέπει να γίνει περαιτέρω έρευνα γύρω από την επεξεργαστική δύναμη που θα

απαιτείται να έχει ένας IPSec router για να εκτελεί με την ίδια αποδοτικότητα όλες τις λειτουργίες του, και κατά πόσο αυτή επηρεάζει το κόστος σε σύγκριση με την υφιστάμενη Bump-In-The-Wire υλοποίηση.

- Το μοντέλο ενσωμάτωσης στους routers χωρίς ξεχωριστή IPSec συσκευή είναι ευκολότερο να εφαρμοστεί από ότι αυτό των host, καθώς οι συσκευές που απαιτούνται για προμήθεια είναι κατά πολύ λιγότερες. Ωστόσο, όσον αφορά το συνολικό κόστος προμήθειας δρομολογητών σε σύγκριση με αυτό των κρυπτομηχανών δεν υπάρχει σαφής εικόνα γύρω από το ποια υλοποίηση είναι λιγότερο κοστοβόρα. Με δεδομένο όμως ότι δύο συσκευές (δρομολογητής και συσκευή IPSec) αντικαθίστανται από μία σε κάθε περίπτωση (δρομολογητής με ενσωματωμένο IPSec), μπορούμε να υποθέσουμε ότι το κόστος πιθανώς να είναι στα ίδια επίπεδα και στις δύο περιπτώσεις. Επομένως, εφόσον δεν υπάρχει σημαντική διαφορά στο κόστος υλοποίησης (δεν υπάρχει δηλαδή κάποιο ουσιαστικό οικονομικό όφελος από την μετάβαση), δεν υπάρχει ουσιαστικός λόγος για τη μετάβαση στο μοντέλο των IPSec routers από το υφιστάμενο μοντέλο των κρυπτομηχανών, καθώς το τελευταίο αποτελεί ένα ήδη δοκιμασμένο και αποδοτικό μοντέλο.

ΕΠΙΛΟΓΟΣ

Η παρούσα εργασία είχε ως σκοπό την ανάδειξη της λειτουργίας της σουίτας πρωτοκόλλων IPSec στα IP δίκτυα (intranets) των στρατιωτικών δομών της Βορειο-Ατλαντικής Συμμαχίας, με σκοπό την εξέταση υιοθέτησης νέας τεχνικής προσέγγισης στην ενσωμάτωση του IPSec ώστε να χρησιμοποιούνται κατά το δυνατόν λιγότερες συσκευές IPSec (κρυπτομηχανές).

Για το σκοπό αυτό, αρχικά αναλύθηκαν τα πλεονεκτήματα και μειονεκτήματα της hardware-based κρυπτογράφησης, ώστε να αναδειχθεί ο λόγος για τον οποίο η εργασία αυτή εξετάζει τη δυνατότητα μετάβασης σε διαφορετικό μοντέλο ενσωμάτωσης του IPSec, ο οποίος δεν είναι άλλος από την προσπάθεια μείωσης του κόστους που η χρήση αυτών των ειδικοποιημένων συσκευών επιφέρει.

Για την πλήρη κατανόηση του IPSec, αναλύθηκαν πλήρως οι λειτουργίες του και οι τρόποι με τους οποίους υλοποιείται ένα IPSec VPN (μοντέλα αρχιτεκτονικής IPSec VPN), τα πρωτόκολλα που χρησιμοποιεί για τη δημιουργία ασφαλούς επικοινωνίας (AH, ESP), αναλύθηκαν οι φάσεις διαχείρισης και ανταλλαγής κρυπτογραφικών κλειδιών και περιγράφηκε ένα σενάριο ESP σε αρχιτεκτονική gateway-to-gateway, που αποτελεί και τον κύριο τρόπο υλοποίησης του IPSec με τη χρήση των κρυπτομηχανών.

Σημαντικό στοιχείο της παρούσας εργασίας αποτελούν οι συσκευές IPSec (κρυπτομηχανές) που το υλοποιούν στο ΝΑΤΟ. Έτσι, αναλύθηκε πλήρως ο τρόπος με τον οποίο υλοποιεί ένας IP Encryptor το IPSec, η αρχιτεκτονική των IP Encryptors και οι υπηρεσίες που αυτοί προσφέρουν. Υπάρχουν όμως πολλά χαρακτηριστικά που διαχωρίζουν μια κρυπτοσυσκευή που χρησιμοποιείται εντός του ΝΑΤΟ από μια απλή IPSec συσκευή. Έτσι, συγκρίθηκαν παραδείγματα κρυπτομηχανών του Καταλόγου Προϊόντων Διασφάλισης Πληροφοριών του ΝΑΤΟ (NIAPC), οι οποίες εντάσσονται σε αυτόν βάσει κριτηρίων

τα οποία αναλύθηκαν εκτενώς. Από τα χαρακτηριστικά των κρυπτομηχανών αυτών καθώς και από άλλες πηγές, εξάχθηκαν οι απαιτήσεις που θέτει το NATO για τις ελάχιστες προδιαγραφές σχεδίασης, αρχιτεκτονικής, λειτουργίας και δυνατοτήτων των συσκευών αυτών.

Στο τελευταίο μέρος της εργασίας, αναλύθηκαν τα μοντέλα ενσωμάτωσης του IPSec σε ένα IP δίκτυο κορμού (host/OS, host/BITS, router/native, router/BITW). Έγινε μία προσπάθεια αξιολόγησης μιας απόπειρας υλοποίησης των άλλων μοντέλων ενσωμάτωσης του IPSec (host/OS ή BITS, router/native) ώστε να εκπληρώνονται οι απαιτήσεις του NATO και εξάχθηκαν τα συμπεράσματα της εργασίας.

Από την εργασία αυτή εξάγεται ότι οι περισσότερες απαιτήσεις του NATO για τη λειτουργία του IPSec ώστε η επικοινωνία να θεωρείται ασφαλής για δεδομένα με διαβάθμιση “ΑΠΟΡΡΗΤΟ” είναι κατασκευαστικές και αφορούν κατά κύριο λόγο την υιοθέτηση τεχνικών proof designing αλλά και τη δυνατότητα επιπρόσθετων λειτουργιών τις οποίες δεν υποστηρίζουν αντίστοιχοι εξοπλισμοί του εμπορίου. Λόγω της παραπάνω διαπίστωσης, συμπεραίνεται ότι η ενσωμάτωση του IPSec στους hosts σε μια στρατιωτική δομή του NATO είναι ασύμφορη λόγω του πολύ υψηλού κόστους (πολλές συσκευές - ίδιο ή υψηλότερο κόστος προμήθειας μίας συσκευής). Όσον αφορά την αντίστοιχη εγγενή ενσωμάτωση του IPSec στους routers (χρήση ενιαίας συσκευής για routing και IPSec), δεν υπάρχει σαφής διαφοροποίηση ως προς τη διαφορά κόστους, όμως το γεγονός ότι στην περίπτωση αυτή δεν χρησιμοποιείται dedicated επεξεργαστής για την διενέργεια των IPSec διαδικασιών, αλλά αυτές αποτελούν διεργασίες που εκτελούνται από τον ίδιο επεξεργαστή ο οποίος εκτελεί και το routing μπορεί να σημαίνει ότι η απόδοση στο δίκτυο θα μειωθεί σημαντικά. Επομένως, βάσει της εργασίας αυτής, δεν μπορεί να προταθεί η μετάβαση από το μοντέλο BITW στο μοντέλο αυτό, καθώς αυτό θα απαιτούσε σχεδίαση των δρομολογητών με μεγαλύτερη επεξεργαστική δύναμη (άρα και μεγαλύτερο κόστος) χωρίς να εξασφαλίζεται απαραίτητα η ίδια απόδοση στο δίκτυο. Προκειμένου όμως η εικόνα γύρω από τα παραπάνω να είναι πιο σαφής, απαιτείται περαιτέρω μελέτη σχεδίασης και ανάλυσης κόστους και απόδοσης ενός τέτοιου δρομολογητή με IPSec δυνατότητες, ο οποίος ενσωματώνει και τις απαιτήσεις του NATO στην κατασκευή, αρχιτεκτονική και λειτουργία του.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). *Guide to IPsec VPNs*. National Institute of Standards and Technology Special Publication 800-77.

[2] Basu A., Zhang W., Naik N. (2016). *IPsec Anti-Replay Check Failures* [online] Available at: www.cisco.com.

[3] Kent, S. and Seo, K. (2005). *Security Architecture for the Internet Protocol*. RFC 4301.

[4] Kent, S and Atkinson, R. (1998). *IP Encapsulating Security Payload (ESP)*. RFC 2406.

[5] Feilner, M. "*Chapter 1 - VPN—Virtual Private Network*". OpenVPN: Building and Integrating Virtual Private Networks: Learn How to Build Secure VPNs Using this Powerful Open Source Application, Packt Publishing.

[6] Mason, A. G. (2002). *Cisco Secure Virtual Private Network*. Cisco Press, p. 7

[7] National Institute of Standards and Technology (2007). *FIPS PUB 140-2: Security Requirements for Cryptographic Modules.*

[8] Barker, E., Dang, Q., Frankel, S., Scarfone, K., Wouters, Paul (2020). *Guide to Ipsec VPNs*. National Institute of Standards and Technology Special Publication 800-77 (1st Revision)

[9] Committee on National Security Systems. (2007). National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products. *CNSS Policy No. 19*. Committee on National Security Systems .

[10] Deven J . Anthony, J. J. (2018, October 30). *United States Patent Αρ. US 10 , 116 , 446 B2* [online] Available at https://patentimages.storage.goog-leapis.com/79/51/70/e030df50252660/US10116446.pdf [Accessed 19 Oct 2020].

[11] Direction centrale de la sécurité des systèmes d'information. (2008, July). IP Encryptor Protection Profile - CC3.1. France: Secrétariat général de la défense nationale.

[12] Leonardo S.p.a. (χ.χ.). *CM2100IP & KNMS2100IP IP ENCRYPTION SYSTEM.* [online] Available at https://www.leonardocompany.com/documents/20142/3163281/CM2100IP_KNMS2100IP_IP_Encryption_LQ_mm08685_.pdf?t=1542804867793 [Accessed 19 Oct 2020].

[13] NATO NCI Agency. (χ.χ.). *IP Encryption* [online] Available at https://www.ia.nato.int/niapc/Category/IP-Encryption_25 [Accessed 19 Oct 2020].

[14] North Atlantic Council. (2014, May 28). Enclosure "F" to C-M(2002)49 "Communication and Information System Security". .

[15] SEC-34 IP Encryptor (VPN). (χ.χ.). [online] Available at http://privis.net/product/sec-34-ip-encryptor-vpn/ [Accessed 19 Oct 2020].

[16] Selenia Communications S.p.A. (χ.χ.). *CM - 109 IP Crypto Device.* [online] Available at http://www.ia.nato.int/niapc/Product/CM-109-IP_134, *Product Documents, Manufacturer's brochure* [Accessed 19 Oct 2020].

[17] Shirey, R. (2007). *Internet Security Glossary, Version 2 (RFC 4949).* Network Working Group.

[18] Telleen, S. L. (1998, October 19). *The Difference Between Internet, Intranet, and Extranet*. Ανάκτηση από http://www.iorg.com/ [Accessed 19 Oct 2020].

[19] NCI Agency, 2010. *NATO Information Assurance Product Catalogue (NIAPC)* [online] Introduction. Available at https://www.ia.nato.int/niapc/Information/Introduction [Accessed 19 Oct 2020].

[20] 2020, *The NISP Nation* [online] Available at https://nisp.nw3.dk/node/T-35ac841c-00ad-4b74-b116-8e1df21c702c-X.html [Accessed 19 Oct 2020]).

[21] North Atlantic Treaty Organization, 2018. *NATO International Military Staff, NATO Agencies and Bodies.* [online] Available at https://www.nato.int/cps/en/natolive/71172.htm [Accessed 19 Oct 2020]).

[22] Loepker, M., 2005. *NATO Consultation, Command & Control Board INFOSEC Subcommittee "Protection of Information" SC/4 Perspectives*. SPI 2005 Conference. [online] Available at http://spi.unob.cz/old/last/minule.asp [Accessed 19 Oct 2020].

[23] International Organization for Standardization (ISO), 2015. *Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.* International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15408-1, 3rd edition (corrected version).

[24] NCI Agency, 2010. *NATO Information Assurance Product Catalogue (NIAPC).* [online] Vendor Information. Available at https://www.ia.nato.int/niapc/Information/NIAPC-vendor-info [Accessed 20 Oct 2020].

[25] International Organization for Standardization (ISO), 2011. *Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security Functional Components (2011).* International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15408-1, 3rd edition (corrected version).

[26] International Organization for Standardization (ISO), 2011. *Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Evaluation criteria for IT security.* International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15408-1, 3rd edition (corrected version).

[27] National Security Agency (NSA) - National Communications Security Committee (NCSC) - Subcommittee on Compromising Emanations (SCOCE), 2001. *Tempest Glossary*. [online] Available at http://cryptome.org/0001/ncsc-3.htm [Accessed 20 Oct 2020].

[28] Ciampa, M., 2018. *CompTIA Security+ Guide to Network Security Fundamentals.* 6th Edition.

[29] Cryptome.org, 2003. *National Security Agency (NSA). NACSIM 5000 Tempest Fundamentals.* [online] Available at http://cryptome.org/jya/nacsim-5000/nacsim-5000.htm [Accessed 20 Oct 2020].

[30] Internet Archive Wayback Machine, 2009. *National Security Agency (NSA). TEMPEST: A Signal Problem.* [online] Available at https://web.archive.org/web/20130918021523/http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf [Accessed 20 Oct 2020].

[31] Cryptome.org, 2000. National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST 2-95: Red/Black Installation Guidance. [online] Available at http://cryptome.org/jya/tempest-2-95.htm [Accessed 20 Oct 2020].

[32] TEMPEST Equipment Selection Process. Available at https://www.ia.nato.int/niapc/tempest/certification-scheme [Accessed 20 Oct 2020].

[33] Secure Systems and Technologies. *Tempest Introduction*. [online] Available at https://www.apitech.com/globalassets/documents/products/secure-systems--information-assurance/sst/tempest-introduction-iss-3.pdf [Accessed 20 Oct 2020].

[34] Fibersystem AB. *Tempest.* [online] Available at https://www.fibersystem.com/tempest/ [Accessed 21 Oct 2020].

[35] NATO Allied Command Transformation. *NATO Security Indoctrination.* [online] Available at https://www.act.nato.int/images/stories/structure/reserve/hqrescomp/nato-security-brief.pdf [Accessed 13 Nov 2020].

[36] *Thales TCE 621/B and TCE 621/C Cryptel®-IP High Capacity Encryption Devices* [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/e9f5dce5-1e5f-49e2-b291-53557b604289/TCE-621-B-Product%20sheet [Accessed 13 Nov 2020].

[37] NCI Agency, 2010. *NATO Information Assurance Product Catalogue (NIAPC)* [online] Selected Category: IP Encryption. Available at https://www.ia.nato.int/niapc/Category/IP-Encryption 25 [Accessed 13 Nov 2020].

[38] Electronics-Notes.com*. CISPR 22: EN 55022 EMC Standard* [online] Available at https://www.electronics-notes.com/articles/analogue_circuits/emc-emi-electromagnetic-interference-compatibility/cispr22-en55022-standard.php [Accessed 13 Nov 2020].

[39] Valavan, S., Texas Instruments. *Understanding electromagnetic compliance tests in digital isolators* (2014) [online] Available at https://www.tij.co.jp/jp/lit/wp/slyy064/slyy064.pdf [Accessed 13 Nov 2020].

[40] U.S. Department of Defense, 1991. *Military Handbook, Reliability Prediction of Electronic Equipment* (1991) [online] Available at http://www.mwftr.com/CS2/Mil-Hdbk-217F.pdf [Accessed 13 Nov 2020].

[41] Lienig, J., Bruemmer, H., 2017. *Reliability Analysis*. Fundamentals of Electronic Systems Design. Springer International Publishing. pp. 45–73

[42] Selenia Communications*. CM 109 IP Crypto Device* [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/e1d337b8-db92-4662-b95a-1c60041eed2a/CM-109-IP-Manufacturer's%20Brochure [Accessed 16 Nov 2020].

[43] Internet Engineering Task Force (IETF), 2010. *RFC-5798. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6* [online] Available at https://tools.ietf.org/html/rfc5798 [Accessed 16 Nov 2020].

[44] Selex ES. IP Encryption System CM109IP and CM2000IP Families [online] Available at http://usa.selex-comms.com/internet/localization/IPC/media/docs/IP-ENCRYPTION-SYSTEM---CM109IP---CM-2000_selex.pdf [Accessed 16 Nov 2020].

[45] Satav, Sandeep & Sarma, V.V.R., 2008. *MIL-STD-461 F - A study report*. 559-563.

[46] Department Of Defence, 2007. *MIL-STD-461F*. *Requirements for the control of electromagnetic interference characteristics of subsystems and equipment.* pp 1.

[47] Department Of Defence, 1993. *MIL-STD-462D Measurement of electromagnetic interference characteristics.* pp 1.

[48] Evaluation Engineering, 1996. *What Is Built-In Self Test And Why Do We Need It?* [online] Available at https://www.evaluationengineering.com/home/article/13000382/what-is-builtin-self-test-and-why-do-we-need-it [Accessed 16 Nov 2020].

[49] NCI Agency. NIAPC. *EP430GN* [online] Available at https://www.ia.nato.int/niapc/Product/EP430GN_484 [Accessed 16 Nov 20].

[50] DF Epicom. *EP430GN. IP Encryption Unit for NATO networks protection* [online] Available at https://www.zsis.hr/UserDocsImages/Sigurnost/pdfs/EP430GN.pdf [Accessed 16 Nov 2020].

[51] National Institute of Standards and Technology, 2001. *FIPS PUB 140-2: Security Requirements for Cryptographic Modules* [online] Available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf [Accessed 16 Nov 20].

[52] ViaSat, 2012. *Altasec KG-250 HAIPE IP Network Encryptor* [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/9d1ff17e-cc97-4709-95cb-400588bcaf80/AltaSec-KG-250-Product%20Sheet [Accessed 18 Nov 20]

[53] NCI Agency. NIAPC. AltaSec KG-250 [online] Available at https://www.ia.nato.int/niapc/Product/AltaSec-KG-250_304 [Accessed 18 Nov 20].

[54] Department of Defence, 2008. *Unified Capabilities Requirements 2008, Change 3*. Department of Defense, p.1899.

[55] Witzke, E. et al., 2012. *Encryption in Mobile Wireless Mesh Networks*. Sandia Report 5964C, p.2-3.

[56] Committee on National Security Systems (CNSS), 2010. *National Information Assurance Glossary*. CNSS Instruction No. 4009, p. 78-79.

[57] Secrom UC, *What is the NSA's Suite A & B?* [online] Available at https://secrom.com/content/what-nsas-suite-b [Accessed 19 Nov 2020].

[58] Modica et al., 2011. *Multi-Network Cryptographic Device*. US 8,032,763 B2.

[59] Wheeler, B. 2009. *Suite B: Classified Network Security Goes Commercial* [online] Available at https://www.linleygroup.com/uploads/WP_Suite_B_DS4050.pdf [Accessed 19 Nov 2020].

[60] Internet Engineering Task Force (IETF), 2011. *RFC-6379. Suite B Cryptographic Suites for IPsec* [online] Available at https://tools.ietf.org/html/rfc6379#section-3.4 [Accessed 19 Nov 2020].

[61] Internet Engineering Task Force (IETF), 2018. *RFC-6379. Reclassification of Suite B Documents to Historic Status* [online] Available at https://tools.ietf.org/html/rfc8423 [Accessed 19 Nov 2020].

[62] National Security Agency. Central Security Service, 2015. *Commercial National Security Algorithm (CNSA) Suite Factsheet* [online] Available at https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/commercial-national-security-algorithm-suite-factsheet.cfm [Accessed 19 Nov 2020].

[63] National Security Agency, Central Security Service, 2016. *Commercial National Security Algorithm Suite and Quantum Computing FAQ* [online] Available at https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf [Accessed 19 Nov 2020].

[64] Committee on National Security Systems (CNSS), 2016. *Use Of Public Standards For Secure Information Sharing* [online] Available at https://www.cnss.gov/CNSS/openDoc.cfm?62E3+XzEvuaXPrN2uDzjXw== [Accessed 19 Nov 2020].

[65] Committee on National Security Systems (CNSS), 2003. National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information [online] Available at https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/cnss15fs.pdf [Accessed 19 Nov 2020].

[66] Federal Communications Commission, 2008. Fiscal Year 2008 - Performance and Accountability Report [online] Available at https://transition.fcc.gov/Reports/ar2008.pdf [Accessed 19 Nov 2020].

[67] Ribboncommunications.com. *What is JITC?* [online] Available at https://ribboncommunications.com/company/get-help/glossary/jitc [Accessed 19 Nov 2020].

[68] NCI Agency. NIAPC. *Mini-CATAPAN Suite A - BID/2420/*1 [online] Available at https://www.ia.nato.int/niapc/Product/Mini-CATAPAN-Suite-A---BID-2420-1_492 [Accessed 20 Nov 20].

[69] L3 TRL Technology. *MINI-CATAPAN BID/2420 100Mbps UK High Grade S and TS IP Encryption Device* [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/10f88003-6dc2-4722-8361-bed1fbb81ee2/Mini-CATAPAN-Suite-A---BID-2420-1-Product%20Sheet [Accessed 20 Nov 20].

[70] L3 TRL Technology. *MINI-CATAPAN - Suite B BID/2490/1 100Mbps High Grade IP Encryption Device* [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/66d6594a-00fe-4aea-9603-049cb4008b67/Mini-CATAPAN-Suite-B---BID-2490-1-Product%20Sheet [Accessed 20 Nov 20].

[71] GOV.UK. Departments, agencies and public bodies. Government Communications Headquarters. *CESG* [online] Available at https://www.gov.uk/government/organisations/cesg [Accessed 22 Nov 20].

[72] *HMG Security Policy Framework* (2010) [online] Available at https://image.guardian.co.uk/sys-files/Guardian/documents/2011/07/21/hmg-security-policy_0_0.pdf [Accessed 22 Nov 20].

[73] Scottish Police Services Authority. *Information Management Strategy SPSA 0062* (2011) [online] Available at https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element3-SPSAStrategy.pdf [Accessed 22 Nov 20].

[74] *Thales Mistral Gigabit* (2009) [online] Available at https://www.ia.nato.int/DocumentGenerator/repository/version/8ec58cb7-ac01-4c1a-b06d-b86761f3efc9/MISTRAL-IP-Corporate---Gigabit-Manufacturer's%20Brochure [Accessed 22 Nov 20].

[75] NCI Agency. NIAPC. *MISTRAL IP Corporate/Gigabit* [online] Available at https://www.ia.nato.int/niapc/Product/MISTRAL-IP-Corporate---Gigabit_429 [Accessed 22 Nov 20].

[76] Department Of Defence, 2000. MIL-STD-810F. *Test Method Standard For Environmental Engineering Considerations and Laboratory Tests*.

[77] European Council. Council of the European Union. Information Assurance. *Mistral System* [online] Available at https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/eu-restricted/vpn-encryptor/mistral-system/ [Accessed 22 Nov 20].

[78] Υπουργείο Εξωτερικών. Ειδική Υπηρεσία Συντονισμού και Εφαρμογής Χρηματοδοτικών και Επενδυτικών Προγραμμάτων –ΕΥΣΧΕΠ. *Προμήθεια εξοπλισμού και βελτίωση – επέκταση δικτυακών υποδομών του ΥΠΕΞ και των Αρχών Εξωτερικού - Μέρος Γ: Υποδείγματα και Πίνακες Συμμόρφωσης* (2014) [online] Available at https://www.mfa.gr/images/docs/dimosioi_diagonismoi/2014_5_21_eysxep_C.pdf [Accessed 23 Nov 2020]

[79] Loisel, Y. *Cryptography in software or hardware: It depends on the need* [online] Available at https://www.embedded.com/cryptography-in-software-or-hardware-it-depends-on-the-need/ [Accessed 28 Feb 2021]

[80] *User manual | RedEagle ID/IQ Contract Price List – L* [online] Available at https://manualzz.com/doc/7331723/redeagle-id-iq-contract-price-list---l [Accessed 28 Feb 2021]

[81] Doraswamy, N., et al. (2003)*., IPSec. The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, 2nd Edition, Prentice-Hall, Inc., Chapter 4, “IPSec Architecture, pp. 89-94.

[82] Kozierok, Charles M. (2005) *The TCP/IP guide: a comprehensive, illustrated Internet protocols reference.* No Starch Press.

[83] Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (2005), *ΦΕΚ 336/2005*, Τεύχος Δεύτερο

[84] Sam Wiltshire (2020) *Hardware Encryption vs. Software Encryption: The Simple Guide.* The Ontrack Data Recovery Blog [online] Available at: https://www.ontrack.com/en-us/blog/hardware-encryption-software-encryption [Accessed 26 Mar 2020]

[85] *AES 256 Hardware Encryption*. Zybersafe [online] Available at https://zybersafe.com/aes256hardwareencryption/ [Accessed 26 Mar 2020]

[86] Ferrante, A., Piuri, V., and Owen, J. (2005). *IPSec Hardware Resource Requirements Evaluation*. In NGI 2005, Rome, Italy. EuroNGI.

[87] www.pixabay.com (2019) [online] Available at https://pixabay.com/el/illustrations/vpn-για-την-εγχώρια-ασφάλεια-4079772/ [Accessed 16 June 2021].

[88] libreswan.org [online] Available at https://libreswan.org/wiki/images/9/90/Host2host.png [Accessed 16 June 2021].

[89] sc1.checkpoint.com. *Layer Two Tunneling Protocol (L2TP) Clients.* [online] Available at https://sc1.checkpoint.com/documents/R76/CP R76 VPN AdminGuide/14529.htm [Accessed 16 June 2021].

[90] www.firewall.cx. *Configuring Site to Site IPSec VPN Tunnel Between Cisco Routers* [online] Available at http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/867-cisco-router-site-to-site-ipsec-vpn.html [Accessed 16 June 2021].

[91] www.idc-online.com. *Authentication Header* [online] Available at http://www.idc-online.com/technical_references/pdfs/data_communications/Authentication_Header.pdf

[92] diecarvi.files.wordpress.com [online] Available at https://diecarvi.files.wordpress.com/2013/07/ipsec-tunnel-and-transport-mode-frame-structure1.png?w=1100 [Accessed 16 June 2021].

[93] Migault, Daniel & Guggemos, Tobias & Killian, Sylvain & Laurent, Maryline & Pujolle, Guy & Wary, jean-philippe. (2017). Diet-ESP: IP layer security for IoT. Journal of Computer Security. 25. 1-31. 10.3233/JCS-16857

[94] support.huawei.com. *S600-E V200R011C10 Configuration Guide - VPN* [online] Available at https://support.huawei.com/enterprise/en/doc/EDOC1000178025/c8a93c0/ipsec-fundamentals [Accessed 16 June 2021].

[95] www.viasat.com. *KG-255X HAIPE and EDE-CIS Encryptor* [online] Available at https://www.viasat.com/products/cybersecurity/kg-255x/ [Accessed 16 June 2021].

[96] www.rohde-schwarz.com. *R&S®SITLine IP* [online] Available at https://www.rohde-schwarz.com/cz/products/cybersecurity/network-encryption/rs-sitline-ip_63493-617133.html [Accessed 16 June 2021].

[97] www.cryptomuseum.com. *KIV-7* [online] Available at https://www.cryptomuseum.com/crypto/usa/kiv7/ [Accessed 16 June 2021].

[98] www.cryptomuseum.com . *DS-101* [online] Available at https://www.cryptomuseum.com/intel/nsa/ds101/index.htm [Accessed 16 June 2021].

[99] A&G Power CO., LTD. Products. *DS-101-S* [online] Available at https://www.ag-power.com.tw/product/ds-101-s/ [Accessed 16 June 2021].

[100] www.cryptomuseum.com. *KOI-18* [online] Available at https://www.cryptomuseum.com/crypto/usa/koi18/index.htm [Accessed 16 June 2021].

[101] NCI Agency, 2010. NATO Information Assurance Product Catalogue (NIAPC). *ID-One PIV Dual interface (contact + 13.56 MHz contactless) plus PROX (125 Hz) chip for PACS* [online] Available at https://www.ia.nato.int/niapc/Product/ID-One-PIV-Dual-interface--contact---13.56-MHz-contactless--plus-PROX--125-Hz--chip-for-PACS_542 [Accessed 16 June 2021].