ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ –TLS ΠΡΩΤΟΚΟΛΛΟ

ΚΟΛΛΙΑ ΑΝΑΣΤΑΣΙΑ
Α.Μ 5004

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

Πάτρα 2015

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΚΡΩΝΥΜΙΑ

Α.Φ.Μ: Αριθμός Φορολογικού Μητρώου

AD: Associated Data

AEAD: Authenticated Encryption with Associated Data

CA: Certificate Architecture

CBC: Cipher Block Chaining

CPU: Central Process Unit

DCCP: Datagram Congestion Control Protocol

DES: Data Encryption Standard

DSA: Digital Signature Algorithm

DTLS: Datagram Transport Layer Security

ECC: Elliptic Curve Cryptography

FTP: File Transfer Protocol

GMT: Greenwich Mean Time

GOST: σοβιετικός αλγόριθμος, που βασίζεται σε μία συνάρτηση κατακερματισμού γνωστή με το όνομα GOST Hash Function.

HMAC: Hash Message Authentication Code

HTTP: HyperText Transfer Protocol

IANA: Internet Assigned Numbers Authority

IMAP: Internet Message Access Protocol

IP: Internet Protocol

IV: Initializing Vector

KEA: Key Exchange Algorithm

MAC: Media Access Control

MD5: Message Digest

MITM: Man In- The – Middle

POODLE: Padding Oracle On Domgraded Legacy Encryption

PRF: PseudoRandom Function

RC4: Alleged Rc4 Κρυπτογραφικός αλγόριθμος

RSA: Κρυπτογράφηση Δημοσίου Κλειδιού

RTT: Round Trip-Time

SHA: Secure Hash Algorithm

SSL: Secure Sockets Layer

TCP: Transmission Control Protocol

TLS: Transport Layer Security

UDP: User Datagram Protocol

VoIP: Voice over IP

WEP: Wired Equivalent Privacy

ΚΕΦΑΛΑΙΟ 1: SSL ΠΡΩΤΟΚΟΛΛΟ

1.1 Εισαγωγή

Το Διαδίκτυο αποτελεί, στις μέρες μας, αδιαμφισβήτητα ένα καθημερινό και βασικό εργαλείο στη ζωή του σύγχρονου ανθρώπου. Κυριότερες δραστηριότητες, που πραγματοποιούνται δια μέσου αυτού είναι η αναζήτηση πληροφορίας και γνώσης, η επικοινωνία μεταξύ των ατόμων, οι αγορές μέσω διαδικτύου, αλλά και διάφοροι τρόποι ψυχαγωγίας. Γίνεται, συνεπώς, αντιληπτό ότι οι δυνατότητες, που προσφέρει το Διαδίκτυο είναι τεράστιες. Αυτό το καθιστά ένα μέσο αρκετά ελκυστικό, διότι με χαμηλό κόστος είναι δυνατό κανείς να εμπλακεί σε πλήθος δραστηριοτήτων.

Από την άλλη μεριά, όμως, ανακύπτει έντονα το θέμα του αν υπάρχει επαρκής μέριμνα σε ότι αναφέρεται στα ζητήματα της ασφάλειας των χρηστών, οι οποίοι πλοηγούνται στο διαδίκτυο. Ένας υπολογιστής, που είναι συνδεδεμένος στο διαδίκτυο, είναι πιθανό, να εκτίθεται σε αρκετούς κινδύνους, οι οποίοι σχετίζονται άμεσα με θέματα, όπως είναι η δέσμευση των πόρων του συστήματος του, η εγκατάσταση ιομορφικού λογισμικού κλπ. και τελικά μπορεί να αποβούν βλαβεροί για το υπολογιστικό σύστημα.

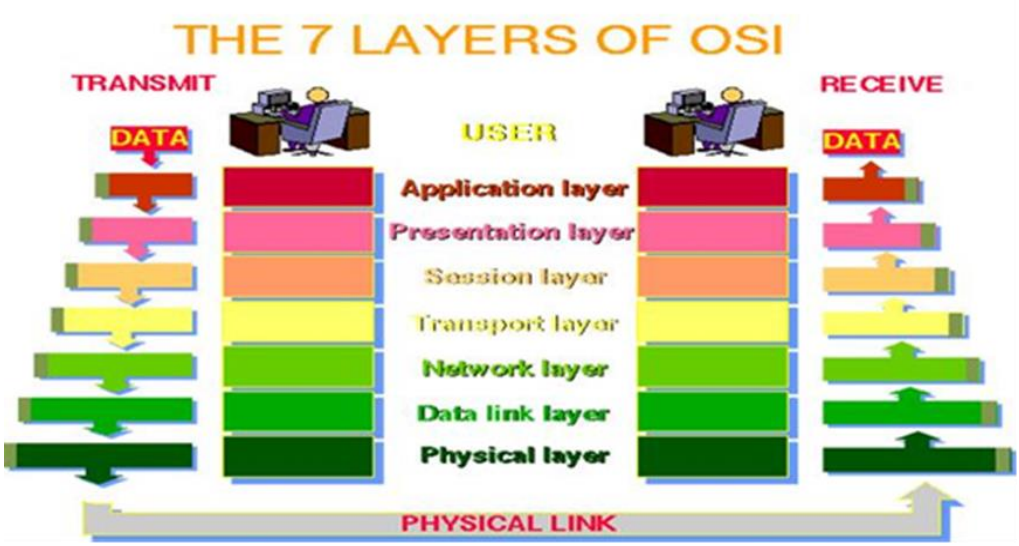
Η πρώτη αναφορά για μελέτη ασφάλειας σε πληροφοριακά συστήματα καταγράφεται στις αρχές τις δεκαετίας του 1970 από την ομάδα εργασίας του συμβουλίου αμυντικής επιστήμης του υπουργείου Άμυνας των ΗΠΑ. Η πρώτη απειλή για τους υπολογιστές εμφανίστηκε το 1970, όταν έκανε την εμφάνιση του ο ιός Creeper στο Arpanet, ενώ το 1998 εμφανίστηκε το πρώτο δικτυακό σκουλήκι. Σήμερα, θα μπορούσε κανείς να καταμετρήσει εκατομμύρια ιούς, αφού ολοένα και αυξάνεται η χρήση δικτυακών συσκευών από τους χρήστες. Το θέμα της ασφαλούς χρήσης του Διαδικτύου απασχολεί εδώ και αρκετά χρόνια όχι μόνο τους απλούς χρήστες, αλλά και την επιστημονική κοινότητα του διαδικτύου, καθώς και την ίδια

την αστυνομία, αφού έχει συσταθεί ειδική ομάδα, που ερευνά ειδικά εγκλήματα μέσω διαδικτύου, αλλά και διάφορες παραβάσεις, που αφορούν στον ψηφιακό κόσμο.

Στην Ελλάδα είναι ευρέως γνωστή η δράση της Δίωξης ηλεκτρονικού εγκλήματος, αλλά και οι επιτυχίες της σε εγκλήματα, που οι δράστες εγκληματούν ψηφιακά, αλλά και ο ιδιαίτερος ζήλος, που επιδεικνύεται για την ενημέρωση ειδικά των πιο ευάλωτων ομάδων του πληθυσμού, -όπως για παράδειγμα οι ανήλικοι χρήστες-, για τους κινδύνους, που παραμονεύουν στη χρήση του διαδικτύου. Συνεπώς, καθίσταται σαφές ότι είναι ζωτικής σημασίας η κατανόηση των τρόπων με τους οποίους ένας χρήστης είναι εκτεθειμένος στο διαδίκτυο, αλλά και τελικά αν και κατά πόσον είναι δυνατό να προστατευθεί κανείς από το πλήθος των δικτυακών κινδύνων.

Οι κύριες προκλήσεις, που αντιμετωπίζει ο επαγγελματίας στον τομέα της ασφάλειας υπολογιστικών συστημάτων σήμερα, είναι η ανάπτυξη ισχυρών κωδικών πρόσβασης και οι έξυπνες κάρτες αυθεντικοποίησης, που εξασφαλίζουν εξουσιοδότηση σε έγκυρους χρήστες, που δεν αποτελούν απειλή για το σύστημα.

Γενικά, είναι σημαντικό να αναλογιστεί κανείς τον τρόπο με τον οποίο πραγματοποιείται η μετάδοση οποιουδήποτε είδους πληροφορίας, είτε πρόκειται για ήχο, δεδομένα, εικόνα κλπ. Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται χρησιμοποιώντας τα πρωτόκολλα TCP (Transfer Control Protocol) και IP (Internet Protocol), τα οποία συνιστούν μαζί ένα πρότυπο και καλύπτουν μέρος του ιδεατού μοντέλου για το δίκτυο και ονομάζεται μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων, ή μοντέλο αναφοράς OSI. Το Ip πρωτόκολλο καλύπτει όλες τις λειτουργίες, τις οποίες το OSI περιγράφει ως τρίτο επίπεδο ή επίπεδο δικτύου, ενώ το TCP περιλαμβάνει όλες τις λειτουργίες, που συνοψίζονται ως τέταρτο επίπεδο ή επίπεδο Μεταφοράς.



Εικόνα 1: Τα επίπεδα του μοντέλου OSI. Παρατηρείται πως η επικοινωνία μεταξύ αποστολέα-παραλήπτη για καθένα από τα επίπεδα του αποστολέα γίνεται στο αντίστοιχο επίπεδο του παραλήπτη και αντίστροφα. Το κάθε επίπεδο βασίζεται στις υπηρεσίες, που παρέχει το επίπεδο, που είναι ακριβώς κάτω από αυτό στην ιεραρχία. Όσο πιο χαμηλό είναι ένα επίπεδο τόσο περισσότερο πλησιάζει στο φυσικό μέσο, ενώ όσο υψηλότερο είναι τόσο περισσότερο πλησιάζει το χρήστη.

Το TLS (Transport Layer Security) πρωτόκολλο, καθώς και ο προκάτοχος αυτού το πρωτόκολλο SSL (Secure Sockets Layer) λειτουργούν πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (HyperText Transfer Protocol) (προβολή ιστοσελίδων), το File Transfer Protocol (FTP) (μεταφορά αρχείων) και το Internet Message Access Protocol (IMAP) (email). Δηλαδή, ανάμεσα στο 4ο ή επίπεδο μεταφοράς και στο 7ο ή επίπεδο εφαρμογών του μοντέλου αναφοράς OSI. Συνεπώς, βασικός ρόλος του SSL πρωτοκόλλου είναι η λήψη πληροφοριών από τις εφαρμογές υψηλότερων επιπέδων, ώστε αυτές να κρυπτογραφηθούν και στη συνέχεια, η μετάδοσή τους στο διαδίκτυο προς τον ηλεκτρονικό υπολογιστή, που έθεσε το αίτημα. Από την άλλη μεριά, το TLS εγγυάται ότι κατά την επικοινωνία εξυπηρέτη - πελάτη (server -client) μέσω του διαδικτύου δεν πρόκειται να μεσολαβήσει κάποιος άλλος χρήστης με σκοπό να υποκλέψει το περιεχόμενο της επικοινωνίας. Στην πραγματικότητα, δηλαδή τα δύο πρωτόκολλα έχουν τον ίδιο βασικό στόχο, απλά το SSL πρωτόκολλο αντικαταστάθηκε από το TLS, διότι οι αυξανόμενες ανάγκες στον τομέα της πληροφορικής οδήγησαν τα συστήματα σε πιο εξελιγμένες μορφής διάτρησης των συστημάτων με αποτέλεσμα να είναι απαραίτητος ο εκσυγχρονισμός του δικτύου για να επιτυγχάνεται ή όσο το

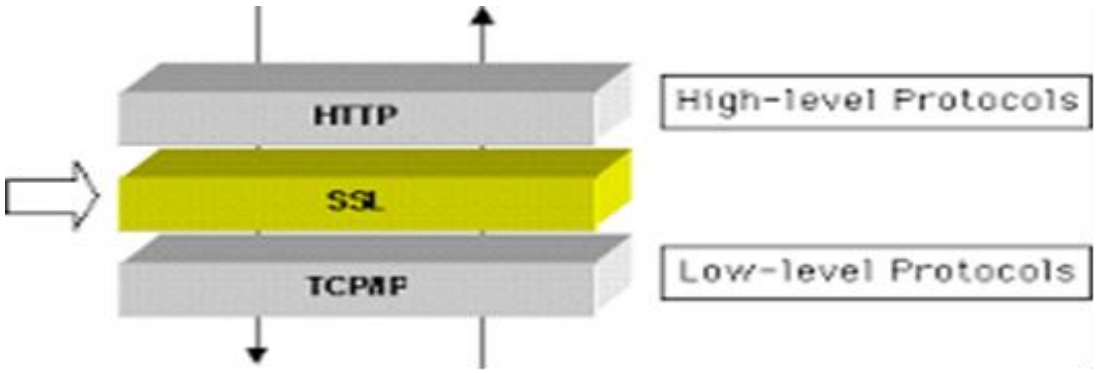
δυνατό μέγιστη ασφάλεια για τον εκάστοτε χρήστη. Έτσι, πριν τη μελέτη του TLS πρωτοκόλλου είναι ύψιστης σημασίας να συνοψιστούν τα κύρια σημεία του πρωτοκόλλου SSL.

1.2 Πρωτόκολλο SSL

Το πρωτόκολλο SSL (Secure Sockets Layer) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων ή προσωπικών δεδομένων στο διαδίκτυο. Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων, που ανταλλάσσονται μεταξύ δύο συσκευών εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP πρωτόκολλο για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή, που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου, όπως για παράδειγμα το HTTP, το FTP, το telnet και λοιπά. Γενικά, το SSL προσφέρει συνοπτικά τις εξής διαδικασίες, όπως είναι η πιστοποίηση του server από τον client, η πιστοποίηση του client από τον server και η εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Οι κρυπτογραφικοί αλγόριθμοι, που υποστηρίζονται από το πρωτόκολλο είναι οι εξής: DES - Data Encryption Standard, DSA - Digital Signature Algorithm, KEA - Key Exchange Algorithm, MD5 - Message Digest, RC2/RC4 (Alleged Rc4 Κρυπτογραφικός αλγόριθμος), ΚρυπτογράφησηΔημοσίου Κλειδιού (RSA), Secure Hash Algorithm1 (SHA-1), SKIPJACK, Triple-DES.

Το πρωτόκολλο SSL βασίζεται σε κρυπτογραφικές τεχνικές Δημόσιου Κλειδιού. Σκοπός του είναι η ενθυλάκωση πρωτοκόλλων υψηλότερου επιπέδου. Στην ιεραρχία των πρωτοκόλλων, το πρωτόκολλο SSL βρίσκεται ακριβώς επάνω από το επίπεδο Μεταφοράς (Transport) και κάτω από το επίπεδο Εφαρμογής (Application) στο μοντέλο OSI/ISO. Χρησιμοποιείται ευρέως σε Ενδοδίκτυα (intranets), αλλά και στο Internet, κυρίως σε συναλλαγές ηλεκτρονικού εμπορίου.



Εικόνα 2: Το πρωτόκολλο SSL βρίσκεται ενδιάμεσα από χαμηλού και υψηλού επιπέδου πρωτόκολλα.

Το SSL είναι σχεδιασμένο, ώστε να παρέχει διαφανείς (transparent) υπηρεσίες στο χρήστη. Ένας SSL Web server δέχεται μία αίτηση για «ασφαλή» σύνδεση σε μια θύρα (443) διαφορετική από αυτήν των απλών αιτήσεων HTTP (port 80). Το URL για συνδέσεις στην port 443 είναι της μορφής: "https://www.server.com". Όταν ο client συνδέεται σε αυτήν την θύρα, αρχικοποιεί τη σύνοδο SSL με τη μέθοδο, η οποία καλείται χειραψία (handsake).Το SSL δημιουργεί μια σύνοδο κατά τη διάρκεια της οποίας η χειραψία πραγματοποιείται μόνο μια φορά. Όταν ολοκληρωθεί η χειραψία, η επικοινωνία κρυπτογραφείται και οι έλεγχοι ακεραιότητας εκτελούνται, έως ότου εκπνεύσει η σύνοδος SSL.

Η χειραψία του SSL ομοιάζει με αυτή του TLS πρωτοκόλλου, που περιγράφεται παρακάτω. Η σημαντικότερη διαφορά είναι ότι στο SSL πρωτόκολλο οι δύο πλευρές συμφωνούν σε μία αξιόπιστη επικοινωνία χρησιμοποιώντας την ίδια μέθοδο κρυπτογράφησης και τα ίδια κλειδιά. Στη χειραψία του TLS ο πελάτης και ο εξυπηρετητής διαπραγματεύονται προτού καταλήξουν σε κάποιο είδος κρυπτογράφησης, σε Media Access Control (MAC) και σε κρυπτογραφικά κλειδιά, κι αυτό είναι φανερό στα διάφορα μηνύματα, που ανταλλάσσονται μεταξύ τους, όπως, τα Client Hello, Server Hello, Server Key Exchange, Server Hello Done, Client Key Exchange, Change Cipher Spec, Finished, Change Cipher Spec, και Finished. Στο τέλος της διαδικασίας, υπάρχει κατάλληλο πλαίσιο στον περιηγητή διαδικτύου, που δηλώνει πως έχει εγκατασταθεί μία ασσφαλής σύνδεση.

1.3 Εκδόσεις πρωτοκόλλου SSL

Οι πιο σημαντικές εκδόσεις του πρωτοκόλλου είναι οι ακόλουθες:

SSL 1.0, 2.0 and 3.0: Το SSL πρωτόκολλο αναπτύχθηκε από την Netscape. Στην πραγματικότητα η έκδοση 1.0 δεν εκδόθηκε δημόσια. Η έκδοση 2.0 εκδόθηκε το Φεβρουάριο του 1995, όμως, δεν είχε ιδιαίτερα μεγάλη απήχηση, διότι περιείχε σημαντικά σφάλματα, λάθη και παραλείψεις και δεν το καθιστούσαν ιδιαίτερα ασφαλές. Έτσι, οδηγήθηκαν οι επιστήμονες στη δόμηση του πρωτοκόλλου SSL 3.0. Η νέα αυτή έκδοση εκδόθηκε το 1996 και ήταν ένας επανασχεδιασμός του πρωτοκόλλου, που σχεδιάστηκε από τον Paul Kocher, ο οποίος εργάστηκε με τους μηχανικούς της Netscape Phil Karlton και ο Alan Freier. "Πατέρας του SSL ", θεωρείται ο Dr. Taher Elgamal, διότι ήταν αυτός ο επιστήμονας δημιούργησε το βασικό αλγόριθμο για το πρωτόκολλο. Η 3.0 έκδοση του SSL δε θεωρείται πλέον αρκετά αξιόπιστη και ασφαλής, διότι είναι ευάλωτη, στην επίθεση Padding Oracle On Domgraded Legacy Encryption (POODLE).

Από τα παραπάνω γίνεται εμφανές ότι το SSL λόγω των μειονεκτημάτων από πολύ νωρίς σταμάτησε να ανταποκρίνεται στις απαιτήσεις των χρηστών. Έτσι, έπρεπε να αντικατασταθεί από ένα ισχυρότερο πρωτόκολλο, το οποίο όχι μόνο να δίνει στους χρήστες την αίσθηση της ασφάλειας, αλλά και να παρεμποδίζει όλα τα είδη των παρεμβάσεων και επιθέσεων. Ο απόγονος του SSL , το TSL εξελίχθηκε σημαντικά και ικανοποιεί τις ανάγκες των χρηστών. Είναι, λοιπόν , σημαντικό να αναλυθούν οι διάφορες εκδόσεις, οι οποίες έχουν δημιουργηθεί από την αρχική εμφάνιση του TSL.

TLS 1.0: Το TLS 1.0 ορίστηκε, αρχικά, τον Ιανουάριο του 1999 στο RFC 2246 και αποτελούσε μία αναβάθμιση της SSL έκδοσης 3.0. Οι διαφορές τους δεν ήταν σημαντικές, ήταν, όμως, αρκετές για να αποκλειστεί η λειτουργικότητα μεταξύ μια εφαρμογής TLS και μίας SSL. Είναι δυνατό η TSL να υποβαθμίσει την σύνδεση με SSL 3.0, αποδυναμώνοντας έτσι την ασφάλεια.

TLS 1.1: Το TLS 1.1 ορίζεται στο RFC 4346 τον Απρίλιο του 2006. Οι σημαντικότερες διαφοροποιήσεις, οι οποίες υπάρχουν στην εν λόγω έκδοση σχετίζονται με την επιπρόσθετη προστασία ενάντια σε Cipher Block Chaining (CBC)

επιθέσεις. Το έμμεσο διάνυσμα αρχικοποίησης-Initializing Vector (IV) αντικαθίσταται με ένα άμεσο IV. Επίσης, πραγματοποιείται αλλαγή στο χειρισμό των λαθών, που οφείλονται σε padding. Τέλος, υποστηρίζονται παράμετροι για την εγγραφή Internet Assigned Numbers Authority (IANA) .

TLS 1.2: Το TLS 1.2 περιορίζεται στο RFC 5246 τον Αύγουστο του 2008. Βασίζεται στο πρώιμο εξειδικευμένο TLS 1.1. Οι βασικές διαφορές, που εισάγονται στο πρότυπο αυτό περιλαμβάνουν τα εξής:

- Ο MD5-SHA-1 συνδυασμός στην ψευδοτυχαία συνάρτηση- PseudoRandom Function (PRF) αντικαταστάθηκε με SHA-256, με μία επιλογή της χρήσης της σουίτας κρυπτογραφίας για τα PRFs.
- Ο MD5-SHA-1 συνδυασμός στα τελικά ψηφία του μηνύματος έχει αντικατασταθεί με το SHA-256 με μία επιλογή να χρησιμοποιηθεί συγκεκριμένη σουίτα αλγορίθμων κρυπτογράφησης. Παρόλα αυτά, το μέγεθος των δυαδικών ψηφίων τερματισμού στο μήνυμα είναι ακόμα έως 96 bits. Ο συνδυασμός του MD5-SHA-1 με το ψηφιακά υπογεγραμμένο στοιχείο αντικαθίσταται από ένα μόνο δυαδικό ψηφίο και πραγματοποιείται διαπραγμάτευση κατά τη διάρκεια της χειραψίας, που ορίζεται στο SHA-1. Η βελτίωση έγκειται στο ότι ο πελάτης και ο εξυπηρετητής μπορούν να εξειδικεύσουν με ποιους αλγορίθμους τερματισμού και χειραψίας αποδέχονται τελικά. Η επέκταση της υποστήριξης για την αυθεντικοποίηση της κρυπτογραφημένης πληροφορίας, χρησιμοποιείται κυρίως για GCM και CCM για το μοντέλο της προχωρημένης κρυπτογράφησης. Ο ορισμός της TLS επέκτασης και της προχωρημένης κρυπτογράφησης σουίτας έχει ήδη προστεθεί.

Όλες οι TLS εκδόσεις καθορίστηκαν περαιτέρω στο RFC 6176 το Μάρτιο του 2011, με τη διαφοροποίηση ότι αφαιρείται η συμβατότητα προς τα πίσω με το SSL, όπου οι σύνοδοι του TSL δε θα διαπραγματευτούν ποτέ τη χρήση του SSL 2.0.

TLS 1.3: Ως τα τέλη το 2014, το TLS 1.3 αποτελεί ένα προσχέδιο και οι διάφορες λεπτομέριές του δεν έχουν ακόμα επακριβώς καθοριστεί. Βασίζεται στην εξειδίκευση

των προγόνων του TLS 1.1 και TLS 1.2. Οι βασικές του διαφορές, όμως, από το TLS 1.2 αναμένεται πως θα είναι:

- Η αφαίρεση της Greenwich Mean Time (GMT) ώρας.
- Αφαίρεση του μη απαραίτητου μήκους πεδίου από το Associated Data (AD) πεδίο εισόδου στην κρυπτογράφηση Authenticated Encryption with Associated Data (AEAD).
- Συγχώνευση με υποστήριξη για την Elliptic Curve Cryptography (ECC) από το RFC 4492.
- Μετονομασία στο {Client,Server}KeyExchange σε {Client,Server}KeyShare.
- Προσθήκη μίας συγκεκριμένης HelloRetryRequest για να απορρίπτεται ο πελάτης.
- Επανάληψη χειραψίας για να παρέχεται 1- Round Trip-Time (RTT).
- Αφαίρεση του DHE γκρουπ.
- Αφαίρεση υποστήριξης για συμπίεση
- Αφαίρεση υποστήριξης για σταστική RSA και DH ανταλλαγή.
- Αφαίρεση υποστήριξης για μη AHEAD κρυπτογράφηση.

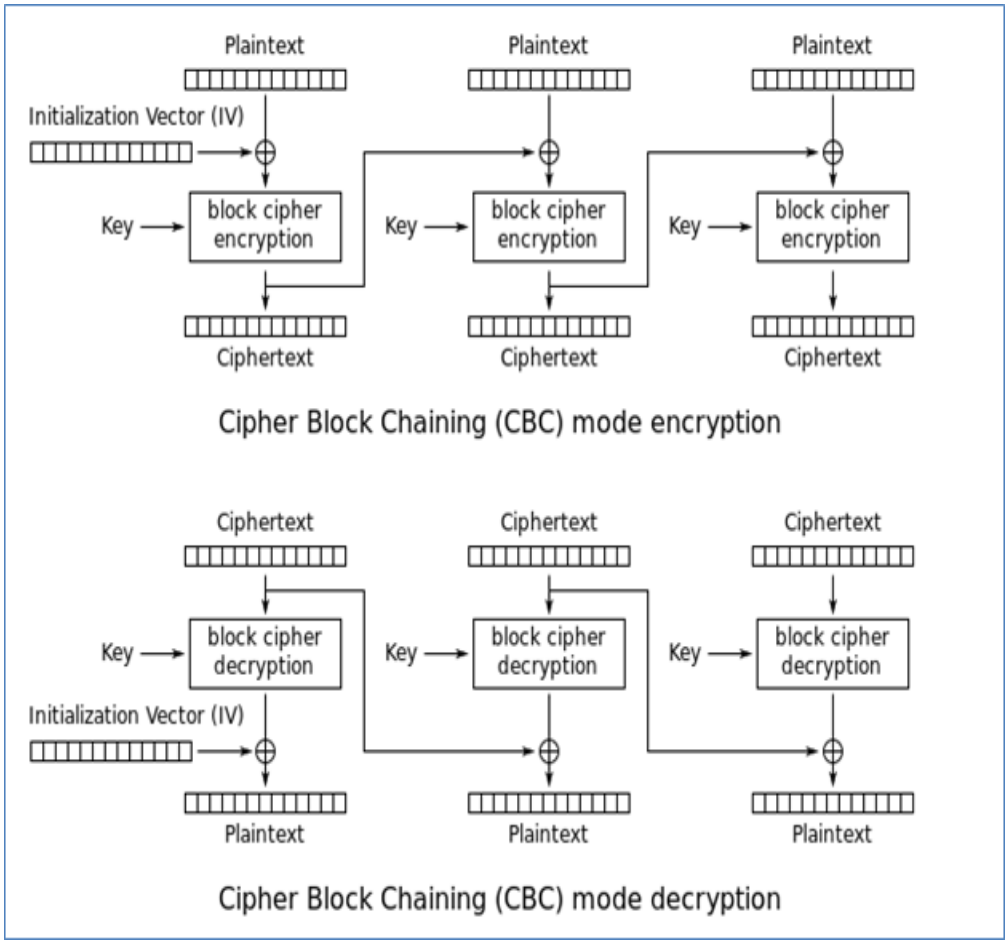
1.4 Επίθεση POODLE

Η επίθεση τύπου POODLE, δηλαδή Padding Oracle On Downgraded Lecacy Encryption είναι μία επίθεση, που σχετίζεται με κάποιον ενδιάμεσο χρήστη, που χρησιμοποιεί το λογισμικό διαδικτύου και ασφάλειας του πελάτη του SSL 3.0 πρωτοκόλλου. Αν οι επιτιθέμενοι χρήστες καταφέρουν να εκμεταλλευτούν το ευάλωτο αυτό πρωτόκολλο, απλά χρειάζεται κατά μέσο όρο να πραγματοποιήσουν 256 SSL 3.0 αιτήσεις για να αποκαλύψουν κρυπτογραφημένα μηνύματα μεγέθους μίας ψηφιολέξης. Κάποιοι επιστήμονες δεν τη θεωρούν αρκετά σημαντική απειλή παρόλα αυτά δεν πρέπει να αγνοείται.

Η POODLE είναι ένα παράδειγμα, απειλής που εκδηλώνει ένα ευάλωτο σύστημα και επιτυγχάνει βάση ενός μηχανισμού να ελαττώνει το επίπεδο ασφαλείας. Τα σφάλματα, που προκαλεί απαιτούν ιδιαίτερη φροντίδα αν σχεδιάζονται για συστήματα τομέων, που τμηματοποιούνται σε μεγάλο βαθμό.

Για να αποφευχθεί αυτή η απειλή είναι δυνατό να απενεργοποιήσει κανείς το SSL 3.0 και στις δύο πλευρές πελάτη και εξυπηρετητή. Όμως, το πρόβλημα της προσέγγισης είναι ότι κάποιοι παλιοί πελάτες και εξυπηρετητές δεν υποστηρίζουν πρωτόκολλα σε εκδόσεις πιο νέες από το TLS 1.0.

Άλλη μέθοδος διαχείρισης θα ήταν η δημιουργία "anti-POODLE record splitting". Αυτό δεν είναι κάτι άλλο παρά ένας μηχανισμός, που διαχωρίζει τις εγγραφές σε πολλά τμήματα και εξασφαλίζει ότι κανένα από αυτά δεν μπορεί να δεχθεί κάποια επίθεση. Όμως, το πρόβλημα του διαχωρισμού αυτού είναι το ότι αν και είναι έγκυρο το να διαμοιράζεται σε μικρότερα τμήματα η πληροφορία, εντούτοις ενδέχεται να δημιουργηθούν προβλήματα συμβατότητας στη μεριά της υλοποίησης του εξυπηρετητή.



Εικόνα 3: Στο σχήμα αναπαρίσταται η επίθεση POODLE τόσο στην πλευρά της κωδικοποίησης (άνω μέρος), όσο και της αποκωδικοποίησης (κάτω μέρος).

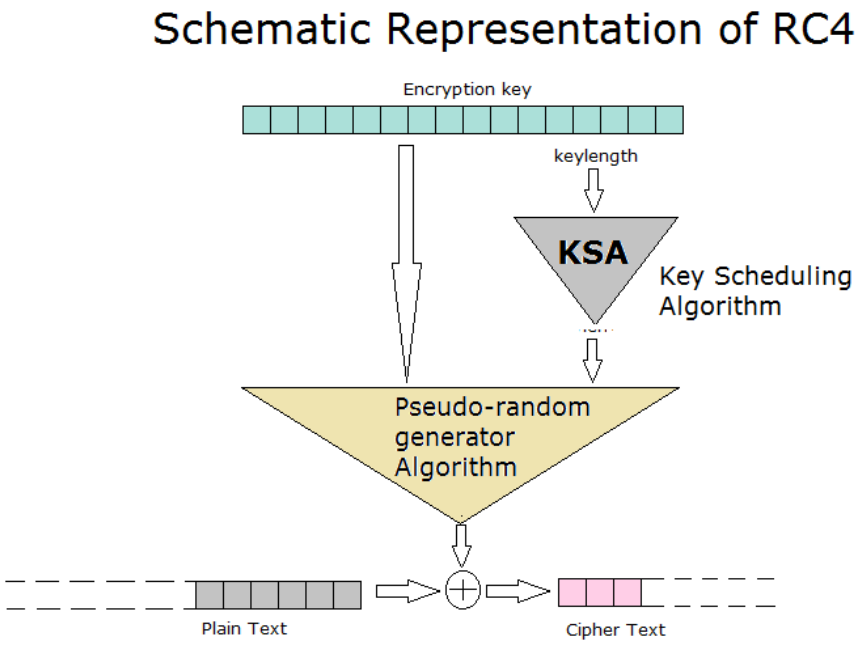
1.5 Μέθοδος RC4

Στην κρυπτογραφία, η RC4 γνωστή και ως ARC4 ή ARCFOUR είναι το πιο ευρέως χρησιμοποιούμενο λογισμικό κρυπτογράφησης stream δεδομένων και χρησιμοποιείται σε δημοφιλή πρωτόκολλα, όπως το TLS για την προστασία της κίνησης στο διαδίκτυο και το Wired Equivalent Privacy (WEP), για την ασφάλεια των ασύρματων δικτύων. Είναι αξιοσημείωτη για την απλότητά της και την ταχύτητά της, παρόλα αυτά, η μέθοδος έχει αδυναμίες, που δεν την καθιστούν τεχνολογία αρκετά χρήσιμη σε νέα συστήματα. Είναι ιδιαίτερα ευάλωτη, όταν η αρχή του stream συνθηματικών εξόδου δεν απορρίπτεται, ή όταν τα κλειδιά, που χρησιμοποιούνται δεν είναι τυχαία ή σχετίζονται με τα κλειδιά, που χρησιμοποιούνται.

Σε αντίθεση με κάθε νέα κρυπτογράφηση streams, η RC4 δε διαχωρίζει ένα nonce παράλληλα με ένα κλειδί. Αυτό σημαίνει ότι ένα εάν ένα μόνο μακροπρόθεσμο κλειδί χρησιμοποιείται για την ασφαλή κωδικοποίηση πολλών streams, τότε το σύστημα κρυπτογράφησης πρέπει να εξειδικεύσει πώς να συνδυάζονται τα nonces με τα μακροπρόθεσμα κλειδιά, ώστε να παράγονται τα κλειδιά για την RC4. Μία προσέγγιση είναι να απευθυνθεί κανείς στην παραγωγή νέων RC4 κλειδιών δημιουργώντας μία συνάρτηση κατακερματισμού μεταξύ του μακροπρόθεσμου κλειδιού και του nonce. Όμως, πολλές εφαρμογές, που χρησιμοποιούν RC4, απλά συνενώνουν το κλειδί με το nonce.

Γενικά, η RC4 αποτελείται από κρυπτογραφημένα streams και συνεπώς, είναι πιο εύπλαστη από τους κοινούς αλγόριθμους κρυπτογράφησης μπλοκ. Εάν δεν χρησιμοποιηθεί μαζί με ένα ισχυρό κωδικό επικύρωσης μηνυμάτων (MAC), τότε η κρυπτογράφηση είναι ευάλωτη σε μια επίθεση χτυπήματος δυαδικού ψηφίου. Η κρυπτογράφηση είναι, επίσης, ευάλωτη σε μια επίθεση κρυπτογράφησης stream, αν δεν εφαρμοστεί σωστά. Είναι σημαντικό ιστορικά να αναφερθεί ότι η RC4 ήταν για πολύ καιρό μία άτρωτη μέθοδος.

Το κλειδί για το stream, που παράγεται από την RC4, καθίσταται ευάλωτο, όταν υπάρχουν πολυποίκιλα επίπεδα προτάσεων και τότε χάνεται η δυνατότητα να διαχωριστεί το είδος της επίθεσης.



Εικόνα 4: Σχηματική αναπαράσταση του RC4.

ΚΕΦΑΛΑΙΟ 2: ΠΡΩΤΟΚΟΛΛΟ TLS

2.1 Πρωτόκολλο TLS –Ορισμός

Το TLS είναι ένα πρωτόκολλο, που εγγυάται ότι κατά την επικοινωνία εξυπηρετητή - πελάτη (server -client) μέσω του Διαδικτύου δεν πρόκειται να μεσολαβήσει κάποιος τρίτος χρήστης, ο οποίος θα υποκλέψει το περιεχόμενο της επικοινωνίας τους. Το TLS έχει διαδεχθεί το SSL πρωτόκολλο και όπως και ο προκάτοχος του, είναι πρωτόκολλο κρυπτογράφησης και χρησιμοποιείται ως ενδιάμεσο πρωτόκολλο μεταξύ του επιπέδου εφαρμογών και του επιπέδου μεταφοράς για να παρέχει ασφάλεια επικοινωνίας στο διαδίκτυο. Το TLS αποτελείται από δύο επί μέρους επίπεδα το TLS Record Protocol και το TLS Handshake Protocol.

Και τα δύο χρησιμοποιούν το X.509 πιστοποιητικό, μέσω ασυμμετρικής κρυπτογράφησης για να αυθεντικοποιήσουν το άλλο μέλος της επικοινωνίας και ανταλλάσσουν ένα συμμετρικό κλειδί. Αυτό το κλειδί της συνόδου χρησιμοποιείται για να κρυπτογραφήσει τη ροή δεδομένων ανάμεσα στις δύο πλευρές. Αυτό επιτρέπει την εμπιστευτικότητα για τα δεδομένα ή για τους κώδικες αυθεντικοποίησης μηνυμάτων. Μερικές εκδόσεις των πρωτοκόλλων είναι ευρέως διαδεδομένες σε εφαρμογές, όπως η δικτυακή πλοήγηση, το ηλεκτρονικό ταχυδρομείο, ο τηλεομοιότυπος μέσω διαδικτύου, τα άμεσα μηνύματα και η τηλεφωνία μέσω διαδικτύου (VoIP). Μία σημαντική ιδιότητα αυτού πέραν της μυστικότητας είναι ότι το κλειδί βραχυπρόθεσμης συνόδου δεν μπορεί να προέλθει από το ασυμμετρικό κλειδί μακροπρόθεσμης συνόδου. Ως αποτέλεσμα, είναι απαραίτητο να επιλεγεί το πιστοποιητικό X.509 για να πιστοποιήσει τις αρχές και μία δομή δημόσιου κλειδιού, έτσι ώστε, τελικά, να επιβεβαιωθεί η σχέση μεταξύ πιστοποιητικού και κατόχου, καθώς επίσης, και για την παραγωγή και διαχείριση της εγκυρότητας του πιστοποιητικού. Ενώ, είναι ιδιαίτερα αποδοτικό σε έμπιστα δίκτυα για την επιβεβαίωση της ταυτότητας, αποτελεί ισχνή τεχνική για δίκτυα αμφιλεγόμενης ασφάλειας, αφού κινδυνεύει από επιθέσεις MITM.

Στη σουίτα πρωτοκόλλων IP, τα πρωτόκολλα TLS και SSL κρυπτογραφούν τα δεδομένα της σύνδεσης του διαδικτύου στο επίπεδο εφαρμογής. Σε ισοδύναμα μοντέλα, αντίστοιχα με τα επίπεδα του OSI, το TLS, καθώς και το SSL, αρχικοποιούνται στο πέμπτο επίπεδο, δηλαδή στο επίπεδο συνόδου και λειτουργούν στο επίπεδο 6, δηλαδή στο επίπεδο παρουσίασης. Στο επίπεδο συνόδου πραγματοποιείται μία χειραψία χρησιμοποιώντας την τεχνική της ασύμμετρης κρυπτογράφησης, σε σχέση με την εγκαθίδρυση ρυθμίσεων κρυπτογράφησης και ένα διαμοιραζόμενο κλειδί για αυτή τη σύνοδο. Έπειτα, στο επίπεδο παρουσίασης κρυπτογραφείται το υπόλοιπο της επικοινωνίας με χρήση συμμετρικής κρυπτογράφησης και το κλειδί συνόδου. Και τα δύο μοντέλα TSL και SSL λειτουργούν για το επίπεδο της μεταφοράς, του οποίου τα τμήματα διατηρούν κρυπτογραφημένα δεδομένα.

Το TLS πρωτόκολλο επιτρέπει στις εφαρμογές πελάτη-εξυπηρετητή να επικοινωνούν δια μέσου του δικτύου με συγκεκριμένο τρόπο. Εφόσον, τα πρωτόκολλα μπορούν να λειτουργούν με ή χωρίς TLS ή SSL, είναι απαραίτητο ο πελάτης να δείχνει στον εξυπηρετητή την εγκαθίδρυση της σύνδεσης TLS. Υπάρχουν δύο βασικοί τρόποι να επιτευχθεί κάτι τέτοιο. Η πρώτη επιλογή είναι η χρήση διαφορετικού αριθμού θύρας για το TLS, όταν αυτό συνδέεται. Για παράδειγμα είναι δυνατή η χρήση της θύρας 443 για το HTTPS. Η δεύτερη λύση είναι ο πελάτης να ζητήσει από τον εξυπηρετητή να αλλάξει τη σύνδεση με το TLS χρησιμοποιώντας ένα ειδικό μηχανισμό πρωτοκόλλου, για παράδειγμα STARTTLS για ηλεκτρονικό ταχυδρομείο και πρωτόκολλα ειδήσεων.

2.2 Εφαρμογές-Χρήσεις TLS

Στο σχεδιασμό των εφαρμογών, το TLS, συνήθως, υλοποιείται στην κορυφή κάθε πρωτοκόλλου μεταφοράς, ενθυλακώνοντας τα πρωτόκολλα του επιπέδου της εφαρμογής, όπως το HTTP, FTP, SMTP, NNTP and XMPP. Ιστορικά, αρχικά, χρησιμοποιήθηκε με αξιόπιστα πρωτόκολλα μεταφοράς, όπως το TCP. Όμως, έχει επίσης, υλοποιηθεί με πρωτόκολλα μεταφοράς βασισμένα σε δίκτυα μεταγωγής πακέτου, όπως το User Datagram Protocol (UDP) πρωτόκολλο και το Datagram Congestion Control Protocol (DCCP) πρωτόκολλο, με βάση, την προτυποποίηση Datagram Transport Layer Security (DTLS).

Μία βασική χρήση του TLS πρωτοκόλλου, είναι να επιτευχθεί ασφάλεια στο διαδίκτυο, κατά την κίνηση μεταξύ της ιστοσελίδας από HTTP , ώστε να μετατραπεί σε HTTPS. Είναι σημαντικό, επίσης, να τονιστεί ότι χρησιμοποιείται για εφαρμογές ηλεκτρονικού εμπορίου, ηλεκτρονικής τραπεζικής και διαχείρισης.

Σήμερα, όλες οι εκδόσεις των περιηγητών υποστηρίζουν SSL 3.0, TSL 1.0, 1.1 και TSL 1.2 ενεργοποιημένα σαν προεπιλογή, όμως, ακόμα υπάρχουν θεμελιώδη προβλήματα, τα οποία ανακύπτουν και συνίστανται στα κάτωθι:

- Τα TLS 1.1 και 1.2 υποστηρίζονται, αλλά μη ενεργοποιημένα στους περιηγητές Internet Explorer (8-10) για Windows 7 και 8 και το ίδιο ισχύει για τον Opera 12 στο Linux λειτουργικό σύστημα.
- TLS 1.1 and 1.2 δεν υποστηρίζονται από τον Internet Explores (6-8) και από τον Safari 6 για το λειτουργικό σύστημα Mac OS X 10.8.
- Η μείωση των γνωστών επιθέσεων δεν είναι ακόμα ικανοποιητική.

Το τελευταίο, ίσως, αποτελεί το πιο σημαντικό πρόβλημα για την εφαρμογή και ευρεία χρήση αυτών των πρωτοκόλλων, αφού ο σκοπός της εφαρμογής τους είναι να αποφεύγονται τέτοιου είδους επιθέσεις. Για παράδειγμα, όπως αναφέρθηκαν ανωτέρω, δύο γνωστές απειλές όπως οι Poodle κα η Rc4.

Όσον αφορά, στην Poodle επίθεση, όλοι οι σημαντικοί περιηγητές ενεργοποιούν το SSL 3.0 εξ' ορισμού. Κάποιοι περιηγητές ήδη αποτρέπουν την επιστροφή στο 3.0, όμως, η μείωση απαιτεί να υποστηρίζεται τόσο από τον πελάτη, όσο και από τον εξυπηρετητή. Ο περιηγητής Opera έχει δημιουργήσει anti-POODLE

εγγραφές, που είναι αρκετά αποτελεσματικές μόνο στην πλευρά του πελάτη. Ο Safari στο λειτουργικό X10.8 και σε ύστερα λειτουργικά συστήματα απαγορεύει CBC κρυπτογράφηση κατά την επιστροφή του SSL 3.0, αλλά αυτό σημαίνει ότι θα χρησιμοποιηθεί το RC4, το οποίο δεν προτείνεται. Ο Google Chrome και ο Firefox αναμένεται ότι θα απαγορεύουν επιστροφή στο SSL 3.0, αλλά και το ίδιο το SSL 3.0 σε εκδόσεις τους στο κοντινό μέλλον.

Επίσης, κρίνονται απαραίτητες οι μειώσεις των RC4 επιθέσεων. Οι περιηγητές Google Chrome, Mozilla Firefox, Opera, and Internet Explorer για Windows 7 και Windows 8 θέτουν την προτεραιότητα του RC4 στο ελάχιστο.

2.3 Πλεονεκτήματα

Τα σημαντικότερα πλεονεκτήματα, του TLS, συγκριτικά με το SSL σχετίζονται με το πώς αυτά τα δύο πρωτόκολλα έχουν αναπτυχθεί. Είναι σημαντικό, γενικά, να συνοψίσει κανείς τα σημαντικότερα πελονεκτήματα, που συνεπάγονται την ανάπτυξη και χρήση του TLS πρωτοκόλλου μίας και κάτι τέτοιο θα εξηγούσε την ταχύτατη αντικατάσταση του SSL από αυτό. Συνεπώς, τα πιο βασικά θετικά στοιχεία του αναφέρονται παρακάτω:

- Το TLS βασίζεται σε ανοιχτές βάσεις επικοινωνίας, που το καθιστούν πολύ πιο επεκτάσιμο και πιο πιθανό να υποστηρίζει μελλοντική τεχνολογία.
- Το TLS είναι προς τα πίσω συμβατό, το οποίο σημαίνει ότι χρησιμοποιείται για την ασφάλεια της σύνδεσης του πελάτη, όταν αυτός υποστηρίζει το SSL.
- Επιτρέπει ασφαλείς και μη ασφαλείς συνδέσεις πάνω από μία συγκεκριμένη θύρα ενόσω, το SSL προσδιορίζει μία θύρα για ασφαλείς συνδέσεις μόνο. Αυτός ο παράγων δεν προκαλεί περισσότερη ή λιγότερη ασφάλεια.
- Προστατεύει τα δεδομένα, που προέρχονται από το ηλεκτρονικό ταχυδρομείο, τις οθόνες εκκίνησης και τις οικονομικές συναλλαγές.
- Χωρίς την παρουσία του, δεν γίνεται αντιληπτό, κατά πόσο αντί να συνδέεται κανείς με έναν εξυπηρετητή, συνδέεται με ένα ενδιάμεσο χρήστη, που στόχο έχει να επιτεθεί και να υποκλέψει πληροφορία.
- Το TLS είναι εύκολο στη χρήση και η πιο συχνά χρησιμοποιούμενη ασφάλεια στο διαδίκτυο.
- Το TLS δεν απαιτεί συμβολή ή υποστήριξη από κάποιο συγκεκριμένο λειτουργικό σύστημα.
- Με την ανταλλαγή μηνυμάτων στο διαδίκτυο, ελέγχονται τα μηνύματα όσο πραγματοποιείται η μετάδοση από τον έναν υπολογιστή στον άλλον. Αυτό προσδίδει αξιοπιστία στην επικοινωνία μέσω διαδικτύου.
- Το TLS διακόπτει την μη εξουσιοδοτημένη πρόσβαση από χρήστες, που αναμειγνύονται και αποτελούν κάποιον τρίτο, ο οποίος παρεμβάλλεται στη δικτυακή επικοινωνία. Ο τρίτος μπορεί να λαμβάνει μέρος σε επικοινωνία μόνο όταν το επιτρέψουν οι δύο συμβαλλόμενοι χρήστες.

- Το TLS χρησιμοποιείται από τους περισσότερους περιηγητές.

Συνεπώς, καθίσταται σαφές ότι χωρίς τη χρήση του TLS πρωτοκόλλου κυρίως, δε θα είναι δυνατή η διατήρηση της ασφάλειας των δεδομένων για το σύστημα και άρα, θα δυσχεραίνεται η πλοήγηση των χρηστών στο διαδίκτυο, αφού θα είναι εκτεθειμένοι σε επιθέσεις από ενδιάμεσους χρήστες στον κυβερνοχώρο. Κάτι τέτοιο είναι ιδιαίτερα σημαντικό για χρηματοοικονομικές συναλλαγές, αφού τότε ανταλλάσσονται πολλά στοιχεία, τα οποία είναι προσωπικά δεδομένα και σχετίζονται με πιστωτικές κάρτες, κωδικούς ανθρώπων Αριθμός Φορολογικού Μητρώου (Α.Φ.Μ) , στοιχεία ταυτότητας κλπ.

2.4 Μειονεκτήματα

Όπως, κάθε τεχνολογία, έτσι και το TLS πρωτόκολλο πέραν των σημαντικών πλεονεκτημάτων του, που συντελούν στη διατήρηση της ασφάλειας στο διαδίκτυο, έχει και πλήθος αδυναμιών και μειονεκτημάτων. Τα πιο σημαντικά του ελαττώματα αναλύονται παρακάτω:

- Αυξημένος επεξεργαστικός φόρτος. Αυτό είναι το βασικότερο όλων των μειονεκτημάτων της υλοποίησης, τόσο του TLS όσο και του SSL. Ειδικότερα, οι τεχνικές κρυπτογράφησης του δημόσιου κλειδιού απαιτούν έντονη χρήση της Central Process Unit (CPU). Σημαντικό πρόβλημα, συνεπώς, δημιουργείται, όταν χρησιμοποιείται το SSL πρωτόκολλο, τότε δημιουργείται μία καθυστέρηση και οδηγεί σε μείωση της απόδοσης του συστήματος. Η μείωση της απόδοσης είναι άρρηκτα συνδεδεμένη με το ποσοστό του χρόνου, που συνδέονται διάφορες συνδέσεις, αλλά και πόσο χρόνο αναμένεται να διαρκέσουν αυτές.
- Καθυστέρηση λόγω διαχείρισης. Τα περιβάλλοντα τόσο του SSL, όσο και του TLS είναι περίπλοκα και απαιτούν εργασίες συντήρησης. Ο διαχειριστής του συστήματος πρέπει ακόμα, να ρυθμίζει το σύστημα και να ελέγχει τα διάφορα πιστοποιητικά.
- Το TLS μόνο κρυπτογραφεί το μήνυμα, όταν αυτό βρίσκεται σε μεταγωγή και όχι σε ολόκληρη τη διαδικασία από τον αποστολέα στον παραλήπτη.
- Δεν είναι δυνατός ο προσδιορισμός της ταυτότητας του αποστολέα, παρά μόνο το μονοπάτι προς τον αποστολέα.
- Το TLS μπορεί να συγχέει το firewall ως έναν τρίτο χρήστη και να θεωρεί ότι υπόκειται σε επίθεση Man-In –The-Middle (MITM).
- Είναι εξαιρετικά πιθανό να είναι εκτεθειμένο το σύστημα, όταν πραγματοποιείται μία διαδικασία απόφραξης στο TCP.

Αυτοί είναι οι βασικότεροι λόγοι για τους οποίους το TLS δε θεωρείται αψεγάδιαστο πρωτόκολλο, αλλά αναμένεται ότι στο μέλλον θα συντελεστούν σημαντικά βήματα, τα οποία θα οδηγήσουν στη βελτίωσή του. Είναι επίσης, εξαιρετικά πιθανό να απασχολήσει ιδιαίτερα τους επιστήμονες, που ασχολούνται με τον κλάδο της ασφάλειας υπολογιστικών και δικτυακών συστημάτων και να τους ωθήσει να συμπεριλάβουν στο πρωτόκολλο νέες τεχνικές, που να καλύπτουν τα κενά ασφαλείας, τα οποία σημειώνονται ως τώρα σε αυτό.

.

ΚΕΦΑΛΑΙΟ 3: ΛΕΙΤΟΥΡΓΙΑ ΠΡΩΤΟΚΟΛΛΟΥ TLS

3.1 Λειτουργία TLS

Σημαντικό είναι να σκιαγραφηθεί η λειτουργία του πρωτοκόλλου, ούτως ώστε να γίνει φανερό πως αυτό επιτυγχάνει να εξασφαλίζει την ασφάλεια στις δύο πλευρές της επικοινωνίας. Αυτό αναλύεται με τη συμπεριφορά του πελάτη και εξυπηρετητή για την εγκαθίδρυση της σύνδεσης.

Μιάς και ο πελάτης και ο εξυπηρετητής έχουν συμφωνήσει να χρησιμοποιούν TLS, διαπραγματεύονται μία σύνδεση χρησιμοποιώντας μία διαδικασία χειραψίας. Κατά τη διάρκεια της χειραψίας, ο πελάτης και ο εξυπηρετητής συναινούν σε διάφορες παραμέτρους με χρήση της εγκαθίδρυσης της ασφάλειας σύνδεσης. Αυτό περιλαμβάνει πολλά βήματα, που αναλύονται παρακάτω:

1. Ο πελάτης αποστέλλει στον εξυπηρετητή τον αριθμό της έκδοσης του SSL/TLS, που χρησιμοποιεί, τις ρυθμίσεις κρυπτογράφησης, τα συγκεκριμένα δεδομένα συνόδου και άλλη πληροφορία, που χρειάζεται ο εξυπηρετητής για να επικοινωνήσει με τον πελάτη.

2. Ο εξυπηρετητής στέλνει τον αριθμό της έκδοσης του SSL/TLS, που χρησιμοποιεί, τις ρυθμίσεις κρυπτογράφησης, τα συγκεκριμένα δεδομένα συνόδου και άλλη πληροφορία, που χρειάζεται ο πελάτης για να επικοινωνήσει με τον εξυπηρετητή. Ο εξυπηρετητής, επίσης, στέλνει το δικό του πιστοποιητικό και αν ο πελάτης απαιτήσει την πηγή του εξυπηρετητή, τότε ο εξυπηρετητής απαιτεί το πιστοποιητικό του πελάτη, αν υπάρχει ανάγκη αυθεντικοποίησης.

3. Ο πελάτης χρησιμοποιεί πληροφορία, η οποία έχει αποσταλεί από τον εξυπηρετητή και αυθεντικοποιεί τον εξυπηρετητή, όπως, για παράδειγμα στην περίπτωση του περιηγητή, που συνδέεται με έναν εξυπηρετητή, ο περιηγητής, ελέγχει αν το ληφθέν πιστοποιητικό διαθέτει όνομα υποκειμένου, το οποίο ταιριάζει με το όνομα του εξυπηρετητή με τον οποίον γίνεται η επικοινωνία. Ελέγχεται ακόμα, αν ο εκδότης του πιστοποιητικού είναι μία έμπιστη αρχή έκδοσης πιστοποιητικών ή αν το πιστοποιητικό έχει λήξει και πότε το πιστοποιητικό έχει ανακαλεστεί. Εάν ο εξυπηρετητής δεν μπορεί να αυθεντικοποιηθεί, τότε ο χρήστης προειδοποιείται για το πρόβλημα και πληροφορείται ότι μία κρυπτογραφημένη και αυθεντική σύνδεση δε μπορεί να εγκαθιδρυθεί. Αν ο εξυπηρετητής δεν είναι δυνατό να αυθεντικοποιηθεί επιτυχώς, ο πελάτης προχωρά στο επόμενο βήμα.

4. Χρησιμοποιώντας όλα τα παραγόμενα δεδομένα στη χειραψία, ο πελάτης με τη συνεργασία του εξυπηρετητή και αναλόγως με την διαδικασία κρυπτογράφησης, που χρησιμοποιείται, δημιουργεί μία μυστική προ-σύνοδο, κρυπτογραφεί με το δημόσιο κλειδί του εξυπηρετητή, το οποίο έχει αποκτηθεί από το πιστοποιητικό του εξυπηρετητή κατά τη διάρκεια του 2ου βήματος, κι έπειτα, στέλνει το κρυπτογραφημένο μυστικό στον εξυπηρετητή. Εάν ο εξυπηρετητής ζητήσει αυθεντικοποίηση από τον πελάτη, το οποίο είναι προαιρετικό βήμα για τη χειραψία, ο πελάτης υπογράφει, επίσης, ένα άλλο πλήθος δεδομένων, που είναι μοναδικό στην χειραψία και γνωστό και στον πελάτη και τον εξυπηρετητή. Στην περίπτωση αυτή, ο πελάτης στέλνει και στους δύο τα υπογεγραμμένα δεδομένα και το πιστοποιητικό του πελάτη στον εξυπηρετητή μαζί με τα κρυπτογραφημένα μυστικά.

5. Εάν ο εξυπηρετητής απαιτεί από τον πελάτη αυθεντικοποίηση, ο εξυπηρετητής αναμένει αυθεντικοποίηση από τον πελάτη. Εάν ο πελάτης δε μπορεί να αυθεντικοποιήσει, τότε τελειώνει η σύνοδος. Αν ο πελάτης αυθεντικοποήσει επιτυχώς, ή ο εξυπηρετητής αποφανθεί να παραιτηθεί της αυθεντικοποίησης του πελάτη κατά τη διάρκεια της συνόδου, τότε ο εξυπηρετητής χρησιμοποιεί ένα ιδιωτικό κλειδί για να αποκρυπτογραφήσει τα

μυστικά (secrets) και έπειτα, πραγματοποιεί μία σειρά βημάτων για να παράγει το μυστικό (secret).

6. Εξίσου, ο πελάτης και ο εξυπηρετητής χρησιμοποιούν το μυστικό για να παράγουν τα κλειδιά της συνόδου, τα οποία είναι συμμετρικά κλειδιά, που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση της πληροφορίας, που ανταλλάσσονται κατά τη διάρκεια της συνόδου SSL και επικυρώνουν την ακεραιότητα της.

7. Ο πελάτης στέλνει ένα μήνυμα στον εξυπηρετητή και τον ενημερώνει για τα μελλοντικά μηνύματα του πελάτη, τα οποία κρυπτογραφούνται με το κλειδί της συνόδου. Έπειτα, στέλνει ένα ξεχωριστό μήνυμα, κατά τη διάρκεια του οποίου αναδεικνύεται ότι η χειραψία έχει ολοκληρωθεί.

8. Η χειραψία TLS είναι ολοκληρωμένη και η σύνοδος ξεκινά. Ο πελάτης και ο εξυπηρετητής χρησιμοποιούν τα κλειδιά της συνόδου για να κρυπτογραφήσουν και να αποκρυπτογραφήσουν τα δεδομένα, που αποστέλλονται από τον έναν στον άλλον και για να επικυρώσουν την ακεραιότητά των δεδομένων και των συμβαλλόμενων μερών.

Τα πιο πάνω οριοθετούν τη φυσιολογική λειτουργία του ασφαλούς καναλιού. Σε κάθε χρονική στιγμή, λόγω κάποιου εσωτερικού ή εξωτερικού προβλήματος είναι δυνατό να υπάρξει διακοπή και να πραγματοποιηθεί επαναδιαπραγμάτευση της σύνδεσης, με επανάληψη της διαδικασίας. Αυτό συντελεί στο ότι η χειραψία ολοκληρώνεται και ξεκινά μία ασφαλής σύνδεση, η οποία κρυπτογραφείται και αποκρυπτογραφείτε όταν ολοκληρώνεται η σύνδεση. Αν κάποιο από τα βήματα αποτύχει, τότε αποτυγχάνει η σύνδεση και άρα δε δημιουργείται.

Σημαντικό είναι να τονιστεί ακόμα ότι στο τρίτο βήμα, ο πελάτης πρέπει να ελέγξει την αλυσίδα των υπογραφών από μία έμπιστη ρίζα. Ο πελάτης πρέπει επίσης, να ελέγξει ότι κανένα από αυτά δεν έχουν ανακληθεί. Αν κάθε υπογραφή και υπογράφων είναι έμπιστος τότε η αλυσίδα πίσω από τον εξυπηρετητή είναι πιστοποιημένη και άρα το πιστοποιητικό και συνεπώς, ο εξυπηρετητής είναι έμπιστα.

3.2 TLS Record Protocol

Το TLS Record πρωτόκολλο είναι ένα πρωτόκολλο, που δομείται σε στρώματα. Σε κάθε στρώμα, τα μηνύματα συμπεριλαμβάνουν πεδία για το μήκος , την περιγραφή και το περιεχόμενο. Το πρωτόκολλο δίνει στα μηνύματα τη δυνατότητα να μεταδίδονται, τμηματοποιεί τα δεδομένα σε εύκολα διαχειρίσιμα μπλοκ, συμπιέζει τα δεδομένα, εφαρμόζει το MAC και κρυπτογραφεί και μεταδίδει το αποτέλεσμα. Τα λαμβανόμενα δεδομένα είναι αποκρυπτογραφημένα, επικυρωμένα, και έπειτα, αποστέλλονται σε υψηλού επιπέδου πελάτες.

Η εκτέλεση των βημάτων του πρωτοκόλλου αυτού δε πρέπει να αποστέλλει τύπους εγγραφής, που δεν περιγράφονται στο πρωτόκολλο, εκτός και αν πραγματοποιηθεί διαπραγμάτευση από κάποια επέκταση. Εάν μία TLS εφαρμογή λαμβάνει έναν μη αναμενόμενο τύπο εγγραφής, πρέπει να στείλει ένα μήνυμα προειδοποίησης.

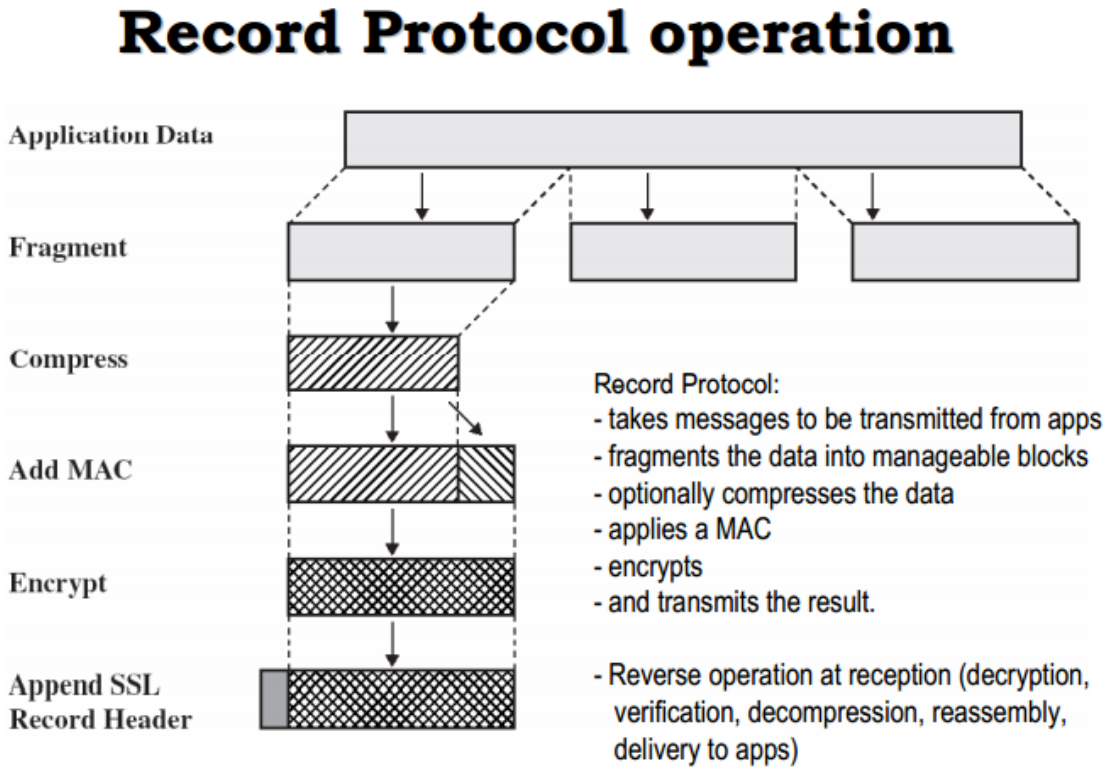
Οποιοδήποτε πρωτόκολλο χρησιμοποιείται για να λειτουργήσει πάνω από το TLS πρέπει να είναι σχεδιασμένο προσεχτικά, ώστε να είναι δυνατό να αντιμετωπίζει κάθε πιθανή επίθεση εναντίον του. Πρακτικά, αυτό σημαίνει ότι ο σχεδιαστής του πρωτοκόλλου πρέπει να είναι βέβαιος για τις ιδιότητες ασφάλειας του TLS, αλλά να μη βασίζεται κατ’ αποκλειστικότητα σε αυτές.

Είναι, επίσης, σημαντικό ότι ο τύπος και το μήκος των δεδομένων μίας εγγραφής δεν προστατεύονται από την κρυπτογράφηση. Εάν η πληροφορία είναι ευαίσθητη, τότε οι σχεδιαστές τις εφαρμογής, ίσως, θελήσουν να λάβουν βήματα, για να ελαχιστοποιήσουν την ροή της πληροφορίας.

Η κατάσταση μίας σύνδεσης TLS είναι το λειτουργικό περιβάλλον για το TLS Record. Παρουσιάζει έναν αλγόριθμο συμπίεσης, έναν αλγόριθμο κρυπτογράφησης και έναν αλγόριθμο MAC. Επιπρόσθετα, οι παράμετροι αυτών των αλγορίθμων είναι γνωστοί, είναι MAC κλειδιά και κλειδιά κρυπτογράφησης για τη σύνδεση και στις δύο κατευθύνσεις ανάγνωσης και εγγραφής.

Υπάρχουν πάντοτε τέσσερις καταστάσεις σύνδεσης, η τρέχουσα ανάγνωση και εγγραφή και η εκκρεμής ανάγνωση και εγγραφή. Όλες οι εγγραφές υπόκεινται σε επεξεργασία στην τρέχουσα ανάγνωση και εγγραφή. Οι παράμετροι ασφάλειας για τις εκκρεμείς καταστάσεις τίθενται από το TLS Handshake πρωτόκολλο και το ChangeCipherSpec. Επιπλέον, το ChangeCipherSpec. έχει τη δυνατότητα επιλεκτικά να δημιουργήσει τις παραμέτρους των εκκρεμών καταστάσεων, στις οποίες η

κατάλληλη τρέχουσα κατάσταση αφαιρείται και αντικαθίσταται από την εκκρεμή. Έπειτα, η εκκρεμής κατάσταση, αρχικοποιείται εκ νέου σε μία κενή κατάσταση. Είναι παράνομο να δημιουργηθεί μία κατάσταση, που δεν αρχικοποιείται με παραμέτρους ασφαλείας ως τρέχουσα κατάσταση. Η αρχική τρέχουσα κατάσταση πάντα καθιστά συγκεκριμένο ότι δε θα χρησιμοποιηθεί ούτε κρυπτογράφηση, ούτε συμπίεση ή MAC.



Εικόνα 5: Συνοψίζεται σχηματικά η λειτουργία του TLS Record πρωτοκόλλου. Παρατηρείται ότι λαμβάνει τα μηνύματα και τα μεταδίδει από τις εφαρμογές, διαιρεί τα δεδομένα σε εύκολα διαχειρίσιμα μπλοκ πληροφορίας, συμπιέζει τα δεδομένα, κρυπτογραφεί, εφαρμόζει MAC και μεταδίδει το αποτέλεσμα. Ενώ, τέλος, στην υποδοχή, υποστηρίζει την ανάστροφη λειτουργία, δηλαδή, αποκρυπτογράφηση, αποσυμπίεση, αποστολή στις εφαρμογές.

3.3 TLS Handshake Protocol

Οι κρυπτογραφικές παράμετροι της κατάστασης της συνόδου παράγονται από το TLS Handshake πρωτόκολλο, το οποίο λειτουργεί πάνω από το TLS record στρώμα. Όταν ένας TLS πελάτης και ο εξυπηρετητής αρχίζουν να επικοινωνούν, συμφωνούν σε μία έκδοση του πρωτοκόλλου, επιλέγουν αλγόριθμο κρυπτογράφησης, σε κάποιες περιπτώσεις αυθεντικοποιούν ο ένας τον άλλον και χρησιμοποιούν τεχνικές δημόσιου κλειδιού κρυπτογράφησης για να παράγουν τα διαμοιραζόμενα μυστικά.

Είναι σημαντικό, συνεπώς, να περιγραφούν τα διάφορα βήματα της χειραψίας στο πρωτόκολλο. Η χειραψία στο TLS Handshake πρωτόκολλο περιλαμβάνει τα ακόλουθα βήματα:

1. Ανταλλαγή μηνυμάτων χαιρετισμού για να συμφωνηθούν οι αλγόριθμοι, οι τιμές των τυχαίων μεταβλητών ανταλλαγής και να ελεγχθεί η ανάληψη της συνόδου.
2. Ανταλλαγή των σημαντικότερων κρυπτογραφικών παραμέτρων για να επιτραπεί στον πελάτη και στον εξυπηρετητή να συμφωνήσουν σε ένα μυστικό.
3. Ανταλλαγή πιστοποιητικών και κρυπτογραφικής πληροφορίας για να επιτραπεί στον πελάτη και στον εξυπηρετητή να αυθεντικοποιήσουν τους εαυτούς τους.
4. Παραγωγή ενός μυστικού από το αρχικό μυστικό και ανταλλαγή των ανταλλασσόμενων μεταβλητών.
5. Παροχή παραμέτρων ασφαλείας στο επίπεδο εγγραφής.
6. Επιτρέπεται στον πελάτη και στον εξυπηρετητή να επικυρώσουν ότι οι όμοιοι τους έχουν υπολογίσει τις ίδιες παραμέτρους ασφαλείας και ότι η χειραψία συνέβη χωρίς να σημειωθεί κάποια εισβολή.

Τα υψηλά στρώματα δεν πρέπει να είναι αναξιόπιστα σε ότι αναφορά στο κατά πόσο το TLS διαπραγματεύεται την ισχυρότερη πιθανή σύνδεση μεταξύ δύο

ομοίων. Υπάρχει πλήθος τρόπων με τους οποίους ένας ενδιάμεσος χρήστης μπορεί να παρασύρει τις οντότητες στις λιγότερο ασφαλείς μεθόδους, που υποστηρίζονται από αυτές. Το πρωτόκολλο έχει σχεδιαστεί για να ελαχιστοποιεί τον κίνδυνο, αλλά υπάρχουν ακόμα πολλές ενεργές και διαθέσιμες επιθέσεις, όπως για παράδειγμα, ότι ένας επιτιθέμενος μπορεί να έχει πρόσβαση στη θύρα μίας ασφαλούς υπηρεσίας και να παρασύρει τη διαπραγμάτευση να πραγματοποείται για μία μη αξιόπιστη σύνδεση.

Ο θεμελιώδης κανόνας είναι ότι τα υψηλότερα επίπεδα πρέπει να «κατανοούν» ποιες είναι οι απαιτήσεις τους σε ασφάλεια και να μην μεταδίδουν ποτέ πληροφορία σε ένα κανάλι λιγότερο ασφαλές από αυτό, το οποίο απαιτούν. Το TLS πρωτόκολλο μπορεί να γίνει ιδιαίτερα ασφαλές αν υποσχεθεί κανείς βαθμό ασφάλειας, δηλαδή αν διαπραγματευτεί κανείς ένα 3DES με ένα RSA κλειδί 1024 δυαδικών ψηφίων ανταλλάσσοντας τα με έναν host, του οποίου το πιστοποιητικό είναι εγγυημένο, και τότε πρέπει να θεωρείται ότι είναι ασφαλές.

Οι πιο πάνω στόχοι επιτυγχάνονται από το πρωτόκολλο χειραψίας, το οποίο συνοψίζεται ακολούθως, ως μία σύνοψη των βασικών του βημάτων:

1. Ο πελάτης στέλνει ένα ClientHello μήνυμα, το οποίο ο εξυπηρετητής πρέπει να απαντήσει με ένα ServerHello μήνυμα, ή αλλιώς, θα συμβεί σφάλμα και η σύνδεση θα αποτύχει. Το ClientHello και το ServerHello χρησιμοποιούνται με σκοπό να εξασφαλιστεί μια βελτίωση των δυνατοτήτων ασφάλειας μεταξύ πελάτη και εξυπηρετητή. Το ClientHello και το ServerHello εγκαθιδρύουν τα εξής χαρακτηριστικά: έκδοση του πρωτοκόλλου, ταυτότητα συνόδου, πρόγραμμα κρυπτογράφησης και μέθοδο συμπίεσης. Επίσης, υπάρχουν δύο επιπλέον τυχαίες μεταβλητές, που παράγονται και ανταλλάσσονται και είναι οι ClientHello.random και ServerHello.random.

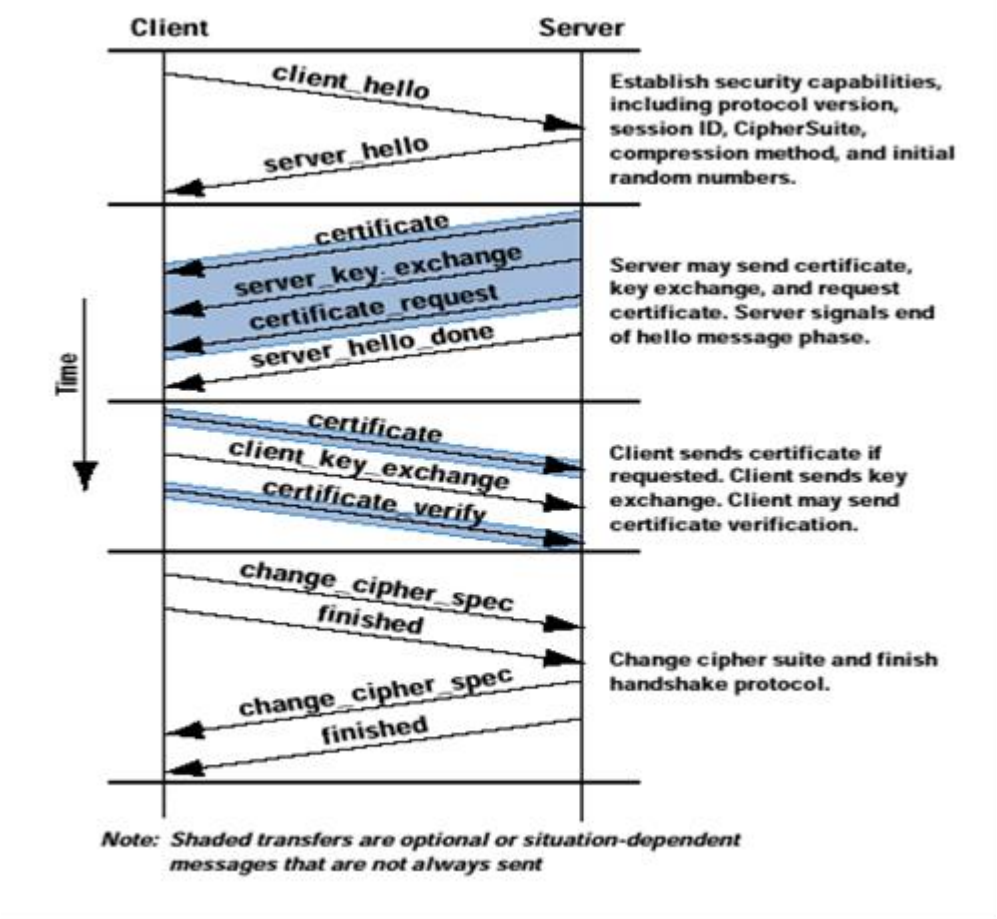
2. Η πραγματική ανταλλαγή κλειδιού χρησιμοποιεί τέσσερα μηνύματα: το πιστοποιητικό εξυπηρετητή, το ServerKeyExchange, το πιστοποιητικό του πελάτη και το ClientKeyExchange. Οι νέες μέθοδοι ανταλλαγής κλειδιού δημιουργούνται από τη συγκεκριμενοποίηση της δομής των μηνυμάτων και από τον καθορισμό της χρήσης των μηνυμάτων, ώστε να επιτρέπουν στον πελάτη και τον εξυπηρετητή να συμφωνούν σε ένα διαμοιραζόμενο μυστικό. Το μυστικό αυτό, πρέπει να είναι αρκετά μεγάλο, περίπου ίσο με 46 ψηφιολέξεις.

3. Ακολουθώντας τα μηνύματα χαιρετισμού, ο εξυπηρετητής θα αποστείλει το πιστοποιητικό σε ένα Message Certificate, ώστε να αυθεντικοποιηθεί. Επιπρόσθετα, ένα μήνυμα ServerKeyExchange, ίσως, αποσταλεί αν είναι απαραίτητο. Εάν ο εξυπηρετητής είναι επιβεβαιωμένος, ίσως, ζητήσει πιστοποιητικό από τον πελάτη, αν αυτό προβλέπεται από το πρόγραμμα κρυπτογράφησης, που έχει επιλεγεί. Έπειτα, ο εξυπηρετητής, θα στείλει το μήνυμα ServerHelloDone, δείχνοντας ότι η φάση του μηνύματος της χειραψίας έχει ήδη ολοκληρωθεί. Ο εξυπηρετητής θα περιμένει μετά μία απάντηση από τον πελάτη.

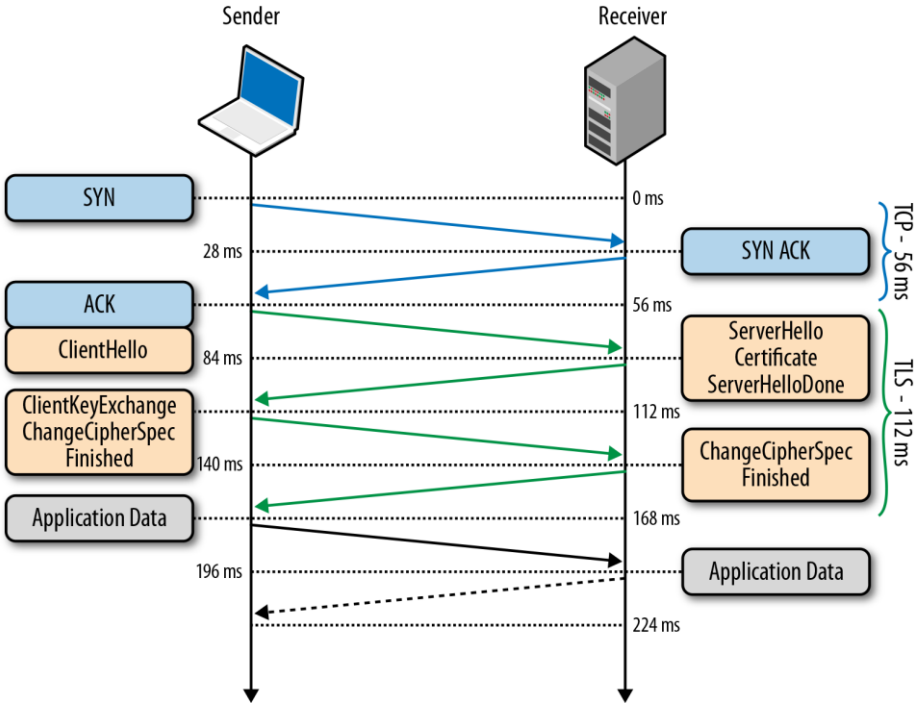
4. Εάν ο εξυπηρετητής έχει στείλει ένα μήνυμα CertificateRequest, τότε ο πελάτης πρέπει να στείλει το μήνυμα του πιστοποιητικού ξανά. Το μήνυμα ClientKeyExchange στέλνεται τώρα και το περιεχόμενο του μηνύματος εξαρτάται από τον αλγόριθμο δημόσιου κλειδιού, που επιλέγεται ανάμεσα στο ClientHello και στο ServerHello. Εάν ο πελάτης έχει στείλει πιστοποιητικό με τη δυνατότητα υπογραφής, ένα ψηφιακά υπογεγραμμένο πιστοποιητικό στέλνεται, ώστε να επικυρώσει την κατοχή του ιδιωτικού κλειδιού του πιστοποιητικού.

5. Στο σημείο αυτό, ένα μήνυμα ChangeCipherSpec στέλνεται από τον πελάτη και ο πελάτης αντιγράφει την εκκρεμή Cipher Spec στην τρέχουσα Cipher Spec. Ο πελάτης, αμέσως, στέλνει το μήνυμα ολοκλήρωσης σε καινούριο αλγόριθμο, κλειδιά και μυστικά. Σε απάντηση, ο εξυπηρετητής στέλνει το δικό του μήνυμα ChangeCipherSpec, μεταδίδοντας την εκκρεμή με την τρέχουσα Cipher Spec και στέλνει το μήνυμα ολοκλήρωσης χρησιμοποιώντας νέο Cipher Spec.

Έτσι, ολοκληρώνεται η χειραψία και ο πελάτης και ο εξυπηρετητής αρχίζουν να ανταλλάσσουν δεδομένα του επιπέδου εφαρμογών. Τέλος, τα δεδομένα των εφαρμογών, δεν πρέπει να στέλνονται πριν ολοκληρωθεί η αρχική χειραψία.



Εικόνα 6: Η επικοινωνία μεταξύ πελάτη (client) και εξυπηρετητή (server), που σχετίζεται με το SSL πρωτόκολλο.



Εικόνα 7: Παρουσιάζονται τα χρονικά διαστήματα, που απαιτούνται για τα διάφορα βήματα της χειραψίας στο πρωτόκολλο ανάμεσα στον παραλήπτη και τον αποστολέα. Παρατηρείται ότι περισσότερο χρόνο καταλαμβάνει η ανταλλαγή δεδομένων εφαρμογών.

ΚΕΦΑΛΑΙΟ 4: ΑΛΓΟΡΙΘΜΟΙ

4.1 Key exchange/agreement

Η ανταλλαγή κλειδιών ή συμφωνία κλειδιών, ή εγκαθίδρυση κλειδιών είναι κάθε μέθοδος στην κρυπτογραφία, με την οποία ανταλλάσσονται κρυπτογραφικά κλειδιά μεταξύ των χρηστών, επιτρέποντας στους χρήστες να χρησιμοποιήσουν έναν αλγόριθμο κρυπτογράφησης. Αν ο αποστολέας και ο παραλήπτης επιδιώκουν να ανταλλάξουν κρυπτογραφημένα μηνύματα, καθένας πρέπει να εξοπλίστει κατάλληλα, ώστε να κρυπτογραφεί μηνύματα, για να είναι δυνατό να συντελέσει, ώστε να αποστέλλονται και να αποκρυπτογραφούνται μηνύματα, τα οποία λαμβάνονται. Η φύση του εξοπλισμού, που απαιτείται εξαρτάται από τις τεχνικές κρυπτογράφησης, που ενδέχεται να χρησιμοποιηθούν. Εάν χρησιμοποιηθεί ένας κώδικας, απαιτείται ένα αντίγραφο του ίδιου κώδικα. Εάν χρησιμοποιούν κρυπτογράφηση, χρειάζονται να χρησιμοποιήσουν κατάλληλα κλειδιά. Αν η κωδικοποίηση είναι συμμετρικού κλειδιού, τότε χρειάζονται και οι δύο μεριές, ένα αντίγραφο του ίδιου κλειδιού. Εάν ένα ασύμμετρο κλειδί χρησιμοποιείται είτε με δημόσιες είτε με ιδιωτικές ιδιότητες, τότε και οι δύο χρειάζονται το άλλο δημόσιο κλειδί.

Το πρόβλημα της ανταλλαγής του κλειδιού είναι πώς να ανταλλάξουν οποιαδήποτε κλειδιά ή άλλη πληροφορία, η οποία απαιτείται, ώστε κανείς άλλος να μην μπορεί να αποκτήσει ένα αντίγραφο. Ιστορικά, αυτές οι απαιτούμενες έμπιστες μεταφορές είναι απαραίτητες και προκαλούνται από διπλωματικά σφάλματα ή κάποιο άλλο πρόβλημα στο κανάλι ασφάλειας. Με την έλευση του δημόσιου ή ιδιωτικού κλειδιού του αλγορίθμου κρυπτογράφησης, το κλειδί της κρυπτογράφησης είναι δυνατό να γίνει δημόσιο, ώστε κανείς χωρίς το κλειδί αποκρυπτογράφησης να μην είναι δυνατό να αποκρυπτογραφήσει το μήνυμα.

Το μόνο πρόβλημα είναι να επιβεβαιωθεί ότι ένα δημόσιο κλειδί ανήκει στον υποτιθέμενο ιδιοκτήτη. Αυτό, είναι δύσκολο, διότι είναι πιθανό κανείς να μιμηθεί άλλη ταυτότητα με κάποιους τρόπους. Αυτό δεν είναι ασήμαντο και ούτε εύκολα

επιλύσιμο πρόβλημα, ιδίως, όταν οι δύο χρήστες απλώς συμμετέχουν, δε συναντώνται και συνεπώς, δεν γνωρίζουν τίποτα ο ένας για τον άλλον.

Η Diffie–Hellman ανταλλαγή κλειδιού σημειώνεται το 1976. Οι Whitfield Diffie και Martin Hellman δημοσίευσαν ένα πρωτόκολλο κρυπτογράφησης, το οποίο καλείται Diffie–Hellman ανταλλαγή κλειδιών (D–H) βάση σεναρίων, που αναπτύχθηκε από τον Ralph Merkle. Το πρωτόκολλο επιτρέπει στους χρήστες να ανταλλάζουν με ασφάλεια τα μυστικά κλειδιά και ακόμα, κι αν ένας αντίπαλος παρακολουθεί το κανάλι επικοινωνίας. Το D–H πρωτόκολλο ανταλλαγής κλειδιών, όμως, δεν αυθεντικοποιεί από μόνο του. Η αυθεντικοποίηση είναι σημαντική διαδικασία, ειδικά, όταν ένας αντίπαλος μπορεί να παρακολουθεί και να τροποποιεί τα μηνύματα στο κανάλι επικοινωνίας.

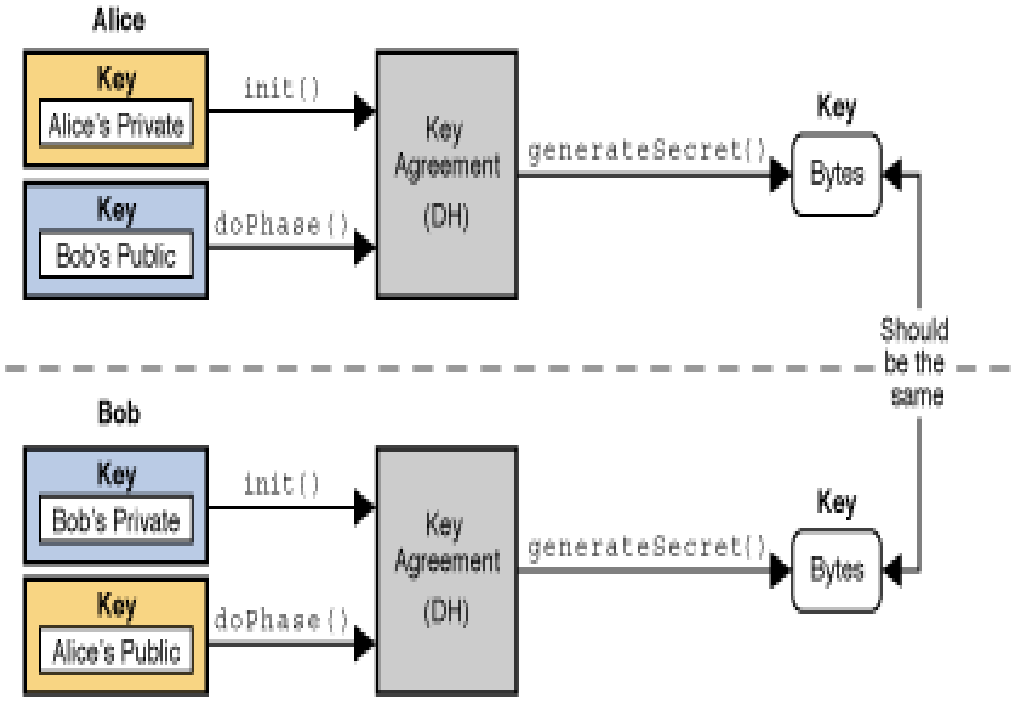
Η υποδομή δημοσίου κλειδιού έχει προταθεί, ως ένας τρόπος γύρω από το πρόβλημα της αυθεντικοποίησης της ταυτότητας. Στην πιο συχνή εφαρμογή, κάθε χρήστης εφαρμόζει ένα πιστοποιητικό αρχής για ένα ψηφιακό πιστοποιητικό, το οποίο εξυπηρετεί άλλους χρήστες ως μία μη έγκυρη αυθεντικοποίηση της ταυτότητας, με τον κίνδυνο συμβιβασμού κάθε χρήστη, στην περίπτωση, που το Certificate Architecture (CA) δε συμβιβάζεται από μόνο του.

Δεν εξασφαλίζεται, βέβαια κάτι, βάση των παραπάνω, για την επίλυση του προβλήματος, εφόσον, η αξιοπιστία του CA από μόνη της δεν είναι ακόμα εγγυημένη από τη μεριά ενός ατόμου. Είναι ένας τρόπος επιχειρημάτων. Η πραγματική αξιοπιστία, η προσωπική επικύρωση και το πιστοποιητικό ανήκουν στο CA και εγκαθιστούν την πίστη του CA, η οποία απαιτείται. Αυτό συνήθως δεν είναι πιθανό. Αυτές οι ρυθμίσεις είναι ψηφιακά υπογεγραμμένα πιστοποιητικά, καταδεικνύοντας ότι το δημόσιο αυτό κλειδί ανήκει στον χρήστη. Βέβαια, μπορεί να συμβούν λάθη και σε αυτή την περίπτωση ή ακόμα να μην είναι έμπιστη η υπογραφή.

Σε ένα έμπιστο δίκτυο, αποφεύγεται η κεντρική αρχή πιστοποίησης. Κάθε χρήστης είναι υπεύθυνος να πάρει ένα πιστοποιητικό από κάποιον άλλον, πριν χρησιμοποιήσει το πιστοποιητικό επικοινωνεί με τις ψηφιακές υπογραφές από το χρήστη, που ισχυρίζεται ότι ήταν ισχυρά συνδεδεμένες με ένα ειδικά δημόσιο κλειδί σε ένα πιστοποιητικό. Το PGP πιστοποιητικό εφαρμόζει ένα δίκτυο έμπιστου μηχανισμού. Μαζί, ο μηχανισμός και το PGP πιστοποιητικό, αποτελούν ένα ευρέως χρησιμοποιούμενο υψηλής ποιότητας κρυπτογραφικό σύστημα.

Η αυθεντικοποίηση συμφωνίας κωδικού αλγορίθμων μπορούν να παράγουν ένα κλειδί ανταλλαγής κρυπτογράφησης χρησιμοποιώντας τη γνώση του

κωδικού χρήστη. Το πρωτόκολλο ανταλλαγής κλειδιού BB84, όπως κάθε ποσότητα κλειδιού αλλαγής πρωτοκόλλου, λαμβάνουν υπόψη ιδιότητες ποσότητας για να εξασφαλίσουν την ασφάλεια τους.



Εικόνα 8: Σχηματική απεικόνιση του αλγορίθμου Key agreement με αποστολέα την Alice και παραλήπτη τον Bob, δύο συνηθισμένα ονόματα για να παρασταθούν τα συμβαλλόμενα μέρη σε μεθόδους κρυπτογράφησης.

4.2 Cipher

Στην κρυπτογραφία, ένας cipher ή cypher είναι ένας αλγόριθμος κρυπτογράφησης και αποκρυπτογράφησης, δηλαδή, μία σειρά από καλά ορισμένα βήματα, τα οποία δεν πρέπει να ακολουθούνται σαν διαδικασία. Αποτελεί μία εναλλακτική λύση, αφού πραγματοποιείται μία λιγότερο συνηθισμένη κρυπτογράφηση. Η κρυπτογράφηση αυτή σχετίζεται με τη μετατροπή της πληροφορίας από το πλήρες κείμενο ή από κάποιον κώδικα. Μία αποκωδικοποίηση είναι κάτι παρόμοιο με έναν κώδικα, όμως, διαφέρει στο ότι τα διάφορα σενάρια είναι διακριτά στην κρυπτογραφία. Στην κλασική κρυπτογραφία, οι κρυπτογραφήσεις είναι διακριτές από τους κώδικες.

Οι κώδικες γενικά, συνίστανται από διαφορετικά μήκη λέξεων χαρακτήρων στην έξοδο, ενώ η κρυπτογράφηση γενικά, υποκαθιστά τον ίδιο αριθμό χαρακτήρων στην είσοδο. Υπάρχουν και συστήματα κρυπτογράφησης, που ενδέχεται να χρησιμοποιούν μεγαλύτερο πλήθος χαρακτήρων στην έξοδο από το πλήθος των χαρακτήρων, που δέχτηκαν ως είσοδο. Οι κώδικες λειτουργούν υποκαθιστώντας σύμφωνα με ένα μεγάλο βιβλίο κωδικών, το οποίο συνδέεται με κάποια τυχαία ακολουθία χαρακτήρων ή αριθμών, ή είναι κάποια λέξη ή φράση. Όταν χρησιμοποιείται κρυπτογράφηση της αρχικής πληροφορίας, τότε είναι γνωστή η πληροφορία και η κρυπτογραφημένη πληροφορία είναι ένα κρυπτογραφημένο κείμενο. Το μήνυμα περιλαμβάνει το σύνολο της πληροφορίας του μηνύματος πλήρους κειμένου, αλλά δεν είναι μία μορφή, εύκολα αναγνώσιμη από ανθρώπινο παράγοντα ή υπολογιστή, χωρίς κάποιον κατάλληλο μηχανισμό αποκρυπτογράφησης του.

Η λειτουργία ενός cypher κρυπτογράφησης εξαρτάται από το τμήμα της βοηθητικής πληροφορίας, που καλείται κλειδί ή κρυπτομεταβλητή. Η διαδικασία κρυπτογράφησης ποικίλει και εξαρτάται από το κλειδί, το οποίο αλλάζει τη λεπτομερή λειτουργία του αλγορίθμου. Ένα κλειδί πρέπει να επιλέγεται πριν τη χρήση του αλγορίθμου για την κωδικοποίηση του μηνύματος. Χωρίς τη γνώση του κλειδιού, ενδεχομένως να καθίσταται ιδιαίτερα δύσκολο, αν όχι ακατόρθωτο να αποκρυπτογραφηθεί το πλήρες κείμενο σε μορφή, που είναι κανείς δυνατό να διαβάσει.

Οι περισσότεροι ciphers εντάσσονται σε διάφορες κατηγορίες, όπως για παράδειγμα:

- Αν λειτουργούν βάση ενός μπλοκ συμβόλων σταθερού μεγέθους (block ciphers), ή αν λειτουργούν βάση ενός συνεχούς stream συμβόλων. (Stream ciphers).
- Αν το ίδιο κλειδί χρησιμοποιείται και για τις δύο διαδικασίες κωδικοποίηση και αποκωδικοποίηση (συμμετρικοί αλγόριθμοι) , ή αν απαιτείται διαφορετικό κλειδί για κάθε διαδικασία (Ασυμμετρικοί αλγόριθμοι). Αν ο αλγόριθμος είναι συμμετρικός, τότε το κλειδί πρέπει να είναι γνωστό στον αποστολέα και στον παραλήπτη, αλλά σε κανέναν άλλο χρήστη. Εάν ο αλγόριθμος είναι ασυμμετρικός, ενώ τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι διαφορετικά είναι τελικά άρρηκτα συνδεδεμένα και πρέπει από το ένα να εξάγεται το άλλο. Αν αυτό δε συμβαίνει, υπάρχει η ιδιότητα για το δημόσιο ή ιδιωτικό κλειδί και κάποιο από τα κλειδιά γίνεται δημόσιο χωρίς να χάνεται η αξιοπιστία του συστήματος.

Σε περίπτωση, που το σύστημα υφίσταται μία μαθηματική επίθεση, παράδειγμα η έλλειψη πληροφορίας, ούτως ώστε να αντιστραφεί η κρυπτογράφηση, δύο παράγοντες κατέχουν σημαντικό ρόλο:

- Η διαθέσιμη υπολογιστική ισχύς, η οποία αναπαριστά την ισχύ, που μπορεί να δαπανηθεί για να επιλυθεί το πρόβλημα.
- Το μέγεθος του κλειδιού, που αναπαριστά το μέγεθος του κλειδιού, που απαιτείται για την κρυπτογράφηση του μηνύματος. Όσο αυξάνει το μέγεθος του κλειδιού, τόσο αυξάνει και η πολυπλοκότητα της εξαντλητικής αναζήτησης σε σημείο, όπου γίνεται μη πρακτική.

Εφόσον, αυτό, που θέλει κανείς να πετύχει είναι η μεγάλη υπολογιστική δυσκολία και η πολυπλοκότητα, θεωρητικά, θα μπορούσε κανείς να επιλέξει έναν αλγόριθμο και το επίπεδο δυσκολίας, που επιθυμεί και άρα, να αποφασίσει αντίστοιχα το μέγεθος του κλειδιού.

Στο TLS πρωτόκολλο περιγράφεται η συνολική δομή του κώδικα, που περιγράφει το cipher. Αυτό περιλαμβάνει την εξής δομή γραμμένη σε γλώσσα προγραμματισμού C:

```
block-ciphered struct {
    opaque content[TLSCompressed.length];
    opaque MAC[CipherSpec.hash_size];
    uint8 padding[GenericBlockCipher.padding_length];
    uint8 padding_length;
} GenericBlockCipher;
```

Αρχικοποιώντας κατάλληλα τα μέλη της ανωτέρω δομής είναι δυνατός ο σχηματισμός των απαραίτητων κωδίκων και των κλειδιών, καθώς και η κλήση του αντίστοιχου cipher αλγορίθμου για την προστασία των δεδομένων μέσω της κρυπτογράφησης κατά την εφαρμογή του TLS πρωτοκόλλου.

4.3 Data Integrity

Η ακεραιότητα των δεδομένων αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μία γνωστή κατάσταση, χωρίς ανεπιθύμητες τροποποιήσεις από μη εξουσιοδοτημένα άτομα, καθώς και στην παρεμπόδιση της πρόσβασης ή χρήσης των υπολογιστών και του δικτύου του συστήματος από άτομα χωρίς δικαιοδοσία.

Η ακεραιότητα των δεδομένων είναι η αντίθετη έννοια από την έννοια του data corruption, που είναι μία μορφή απώλειας δεδομένων. Ο γενικότερος σκοπός κάθε τεχνικής ακεραιότητας των δεδομένων είναι να εξασφαλιστεί ότι τα δεδομένα εγγράφονται, με επιθυμητό τρόπο και επίσης, σε ενδεχόμενη ανάκτησή τους ότι τα δεδομένα είναι τα ίδια, όπως όταν εγγράφηκαν αρχικά. Συνεπώς, η ακεραιότητα στόχο έχει να αποτρέπει την ακούσια αλλαγή της πληροφορίας. Η ακεραιότητα δεν πρέπει να συγχέεται με την ασφάλεια, που απεικονίζει την τάση να προστατεύονται δεδομένα από μη έγκριτες αρχές.

Κάθε ανεπιθύμητη αλλαγή στα δεδομένα είναι αποτέλεσμα μίας αποθήκευσης, ανάκτησης, ή διαδικασίας επεξεργασίας, συμπεριλαμβανομένου της κακής πρόθεσης, της βλάβης στο υλικό και του ανθρώπινου λάθους αποτελεί ένα πρόβλημα ακεραιότητας δεδομένων. Αν, επίσης, οι αλλαγές συνέβησαν λόγω μη εξουσιοδοτημένης πρόσβασης, το πρόβλημα ενδέχεται να εμπίπτει και σε πρόβλημα ασφάλειας των δεδομένων. Ανάλογα, λοιπόν, από τη φύση των δεδομένων, που εμπλέκονται στο πρόβλημα, το ζήτημα ενδέχεται να εμφανίζεται οπουδήποτε από ένα pixel σε μία εικόνα έως μία επιχειρησιακή βάση δεδομένων. Η ακεραιότητα δεδομένων διακρίνεται συνήθως, σε δύο είδη:

- Φυσική ακεραιότητα, η οποία σχετίζεται με τις προκλήσεις, που συνδέονται με τη σωστή αποθήκευση και προσκόμιση των δεδομένων. Αυτά είναι προβλήματα, που συμπεριλαμβάνονται σε ηλεκτρονικά, μηχανικά λάθη, αδυναμίες σχεδίασης συστημάτων, καταστροφή υλικών, φυσικές καταστροφές, πολεμικές και τρομοκρατικές συνθήκες και από άλλους κινδύνους του περιβάλλοντος, όπως τα επίπεδα της υπεριώδους ακτινοβολίας, υπερβολικά υψηλές ή χαμηλές θερμοκρασίες ή υψηλή ή χαμηλή πίεση.

- Λογική ακεραιότητα, η οποία σχετίζεται με την ορθότητα και τη λογική, του τμήματος των δεδομένων, που δίνονται σε ένα συγκεκριμένο περιεχόμενο. Αυτό συμπεριλαμβάνει θέματα, όπως, η αναφορική και η συνολική ακεραιότητα σε μία σχετιστική βάση δεδομένων ή άγνοια δεδομένων αισθητήρων σε ρομποτικά συστήματα. Συνεπώς, σχετίζονται με το νόημα των δεδομένων. Τέτοια προβλήματα εντοπίζονται σε σφάλματα λογισμικού, σχεδιαστικές αδυναμίες, ανθρώπινα λάθη. Οι συνηθέστερες μέθοδοι για τον έλεγχο της λογικής ακεραιότητας σχετίζονται με τον περιορισμό ελέγχου, την επιβεβαίωση προγραμμάτων και άλλους ελέγχους δοκιμών.

Εξίσου, η φυσική και η λογική ακεραιότητα, συχνά διαμοιράζονται πολλές συχνές προκλήσεις, όπως το ανθρώπινο σφάλμα και τα σχεδιαστικά λάθη, συνεπώς, πρέπει και οι δύο να ασχοληθούν κατάλληλα με τρέχουσες απαιτήσεις εγγραφής και ανάκτησης δεδομένων.

Εικόνα 9: Στο σχήμα παρατίθενται οι βασικές αρχές της ακεραιότητας δεδομένων, που συνίστανται στην αλήθεια, την πληρότητα, την ακρίβεια, την επικύρωση και στη δυνατότητα ανάκτησής τους.

Στο TLS πρωτόκολλο χρησιμοποιούνται διάφοροι σημαντικοί αλγόριθμοι για να εξασφαλιστεί η ακεραιότητα των δεδομένων. Ανάλογα με την έκδοση του TLS πρωτοκόλλου, υποστηρίζονται και διαφορετικοί αλγόριθμοι για το σκοπό αυτό. Στις εκδόσεις TLS 1.0 και 1.1 χρησιμοποιούνται οι αλγόριθμοι Hash Message Authentication Code (HMAC)-MD5, HMAC-SHA1, GOST 28147-89 IMIT, GOST R 34.11-94. Ο GOST αλγόριθμος είναι ένας σοβιετικός αλγόριθμος, που βασίζεται σε μία συνάρτηση κατακερματισμού γνωστή με το όνομα GOST Hash Function. Στην έκδοση του TLS 1.2 εκτός από τους ανωτέρω αλγορίθμους χρησιμοποιούνται οι αλγόριθμοι HMAC-SHA 256/384 και AEAD.

Data integrity

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	status
HMAC-MD5	Yes	Yes	Yes	Yes	Yes	Defined for TLS 1.2 in RFCs
HMAC-SHA1	No	Yes	Yes	Yes	Yes	
HMAC-SHA256/384	No	No	No	No	Yes	
AEAD	No	No	No	No	Yes	
GOST 28147-89 IMIT[21]	No	No	Yes	Yes	Yes	Proposed in RFC drafts
GOST R 34.11-94[21]	No	No	Yes	Yes	Yes	

Εικόνα 10: Στον πίνακα παρατίθενται οι αλγόριθμοι ακεραιότητας δεδομένων, που χρησιμοποιούνται σε κάθε έκδοση των πρωτοκόλλων SSL και TLS.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία:

- http://www.saylor.org/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf
- http://bkarak.wizhut.com/www/lectures/networks-07/NetworkProtocolsHandbook.pdf

Δημοσιεύσεις:

- https://tools.ietf.org/html/rfc5246
- http://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029

URLs:

- http://en.wikipedia.org/wiki/Transport_Layer_Security
- http://computer.howstuffworks.com/encryption4.htm
- http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS
- http://validationcertificateinfo.blogspot.gr/2012/12/the-advantages-and-disadvantages-of.html
- https://www.sslshopper.com/why-ssl-the-purpose-of-using-ssl-certificates.html
- https://eclass.upatras.gr/modules/document/file.php/CEID1064/%CE%94%CE%B9%CE%B1%CE%BB%CE%AD%CE%BE%CE%B5%CE%B9%CF%82%202014-15/11_Security.pdf

- http://www.slideshare.net/Jamez_Lee_S_Hunter/an-introduction-to-data-integrity (Εικόνα Data integrity)
- http://www.infocellar.com/networks/osi-model.htm (Εικόνα OSI)
- https://sysmincomputing.wordpress.com/2010/12/14/ipv6/ (Εικόνα για την επίθεση POODLE)
- https://securityblog.redhat.com/tag/symmetric-encryption/ (Εικόνα RC4)
- http://tech.yanatm.com/?p=338 (Εικόνα TLS record)
- http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html (Εικόνα handshake)
- http://chimera.labs.oreilly.com/books/1230000000545/ch04.html (Εικόνα handshake)
- http://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html (Εικόνα Key agreement)
- http://en.wikipedia.org/wiki/Transport_Layer_Security (Εικόνα εκδόσεων TLS)

Αναφορές:

- http://www.webopedia.com/TERM/S/SSL.html
- http://www.webstart.com/jed/papers/HRM/references/ssl.html

Πρότυπα:

- http://www.tsl.co.uk/download%5CTSL%20UMD%20Protocol.pdf