Τεχνολογιες Διαδικτυου

Μαυροπουλος Ανδρεας (217129)

Secure Shell Protocol

Το Secure Shell (ssh) είναι ένα πρωτόκολλο κρυπτογράφησης δικτύου που παρέχει στους χρήστες, την δυνατότητά σύνδεσής ,εκτέλεσης και μεταφοράς αρχείων μέσω ενός ασφαλές και κρυπτογραφημένου δίκτυου. Το πρωτόκολλο SSH αποτελείτε από 3 βασικά στοιχεία: 1.Transport Layer protocol που παρέχει έλεγχο ταυτότητάς διακομιστή , εμπιστευτικότητα και ακεραιότητά με πολύ κάλο forward secrecy. 2.User Authentication Protocol που επικυρώνει τον πέλατη στον διακομιστή. 3. Conecction protocol που πολλαπλασιάζει το encrypted tunnel σε πολλα logical channels. Περαιτέρω το Transport Layer Protocol προσφέρει και συμπίεση, θα εκτελείτε συνήθως πάνω σε μια TCP/IP σύνδεση , αλλα μπορει μπορεί επίσης να χρησιμοποιηθεί πάνω από οποιαδήποτε άλλο αξιόπιστο data stream. Το User Authentication Protocol εκτελείτε πανω απο το Transport Layer Protocol, και το Connection Protocol εκτελείτε πανω απο το Authentication Protocol. Το ssh πρωτόκολλο επιτρέπει την πλήρη διαπραγμάτευση της κρυπτογράφησης, της ακεραιότητας (integrity) , του κλειδιού ανταλλαγής,και του δήμοσιου κλειδιού. Ετσι λοιπόν μπορει η κρυπτογράφηση, η ακεραιότητα, το δημόσιο κλειδί και οι αλγόριθμοι συμπίεσης μπορούν να είναι διαφορετικά για κάθε κατεύθυνση. Για αυτούς τους λόγους πιστεύουν οτι το πρωτόκολλο με την πάροδο του χρόνου θα εξελιχθεί και εταιριες θα χρησιμοποιούν την δικιά τους κρυπτογράφηση. Από την άλλη πλευρά, η απουσία κεντρικής εγγραφής οδηγεί σε συγκρούσεις καθιστώντας δύσκολη τη διαλειτουργικότητα. Ο πρωταρχικός στόχος του πρωτοκόλλου SSH είναι η βελτίωση της ασφάλειας στο Διαδίκτυο. Προσπαθεί να το κάνει αυτο με έναν τρόπο που είναι εύκολο να αναπτυχθεί, ακόμη και με το κόστος της απόλθτης ασφάλειας.

Σε ποιο πρόσφατες εκδόσεις οι κρυπτογραφικοί αλγόριθμοι εχουν αλλάξει. Τα πιο δημοφιλή πρωτόκολλα που χρησιμοποιούνται για την ασφαλή επικοινωνία μέσω του Διαδικτύου τωρα, ειναι τα εξής: Transport Layer Security Protocol (TLS), Signal Protocol,Internet Key Exchange (IKE) Protocol , Secure Shell (ssh) Protocol και Secure Multipurpose Internet Mail Extesnions(S/MIME). Κάθε πρωτόκολλο επικοινωνίας χρησιμοποιεί ορισμένους αλγόριθμους για την επίτευξη ανταλλαγής κλειδιών , confidentiality, authentication , integrity, digital signature. Κάθενα απο αυτα τα πρωτόκολλα κυκλοφορούν με νεές εκδόσεις για να συμβαδίσουν με της υπερσύγχρονες τεχνικές κρυπτογραφίας.

1. Transport Layer Security (TLS 1.3)

Το Transport Layer Security Protocol είναι πρότυπο για την εξασφάλιση επικοινωνίων στον Παγκόσμιο Ιστό. Αρχικά είχε κυκλοφορήσει ως Secure Socket Layer (SSL) από την Netscape Communications το 1995. Με τα χρόνια το πρωτόκολλο εχει βγάλει καινούργιες εκδόσεις καθιστώντας το πιο ασφαλή.

2. Signal Protocol

Το Signal Protocol είναι ενα cryptographic πρωτόκολλο ανταλλαγής μηνυμάτων που παρέχει κρυπτογράφηση από άκρο σε άκρο (E2EE) για άμεση ανταλλαγή μηνυμάτων

3. Internet Key Exchange (IKEv3)

Το Key Exchange Protocol χρησιμοποιείται για τη δημιουργία συσχετίσεων ασφαλείας για τα πρωτόκολλα Ipsec. Χρησιμοποιεί ορισμένα cryptographic primitives για να επιτύχει τους στόχους της δημιουργίας κλειδιών, των έλεγχο ταυτότητας και ασφάλεια.

4. Secure Shell (SSHv2)

Το Secure Shell είναι ενα application layer πρωτόκολλο που επιτρέπει σε έναν υπολογιστή με ασφάλεια να συνδεθεί σε εναν άλλον υπολογιστή μέσω ενός μη ασφαλούς δικτύου,οπως το Διαδίκτυο, έχοντας κανονίσει εναν τρόπο επικοινωνίας. Το SSHv2 παρέχει έλεγχο ταυτότητας δημόσιου κλειδιού και χρησιμοποιεί cryptographically strong Message Authentication Code (MAC) αλγόριθμους για την παροχή ακεραιότητας(integrity) και προέλευση δεδομένων διασφάλισης (data origin assurance).

5. Secure / Multipurpose Internet Mail Extension (S/MIME v4.0)

Το S/MIME είναι ένα ευρέως αποδεκτό πρωτόκολλο για την αποστολή ψηφιακά υπογεγραμμένων και κρυπτογραφημένων μηνυμάτων.Το S/MIME σάς επιτρέπει να κρυπτογραφείτε τα μηνύματα ηλεκτρονικού ταχυδρομείου (email) και να τα υπογράφετε ψηφιακά

6. Authenticated Encryption (AE) Scheme

Το Auntenticated Encryption Scheme προσφέρει ταυτοποίηση.Το block cipher παρέχει εμπιστευτικότητα, αλλά δεν προστατεύει από τυχαία τροποποίηση ή κακόβουλη αλλοίωση.

Συγχρονες Εφαρμογες που χρησημοποιουν SSH

Μια σύγχρονή εφαρμογή που χρησιμοποιεί ssh είναι το Maze το οποίο θα αναλύσουμε σε βάθος. Το Maze είναι μια ασφαλής υπηρεσία αποθήκευσης στο cloud, που χρησιμοποιεί Moving Target Defense και Secure Shell Protocol (SSH) Tunneling.

Οι υπηρεσίες αποθήκευσης cloud έχουν αναδειχθεί ως δημοφιλής προορισμός για επιχειρήσεις και ιδιώτες για ασφαλή αποθήκευση των εγγράφων, τα οποία ειναι σχεδόν προσβάσιμα απο οπουδήποτε, οποτεδήποτε. Ωστόσο, τα συστήματα αποθήκευσης cloud στατικοί στόχοι επίθεσης που επιτρέπουν στους επιτιθέμενους (hackers) να μελετήσουν το σύστημα χωρίς φόβο ότι τα συμπεράσματά τους σχετικά με το σύστημα θα καταστούν ανακριβή. Ως εκ τούτου, οι ερευνητές ασφάλειας υπολογιστών άρχισαν να διερευνούν τεχνικές, γνωστές ωςMoving Target Defense (MTD), για να μετατρέψουν το σύστημα σε ‘κινούμενο’ στοχο. Ενώ οι παραδοσιακοί τρόποι άμυνας προσπαθουσαν να εντοπίσουν και να καλύψουν τα τρωτά σημεία του συστήματος. Η βασική φιλοσοφία του MTD είναι ότι είναι αδύνατο να κατασκευαστούν απόλυτα ασφαλή συστήματα
Αντ ' αυτού, οι τεχνικές MTD προσπαθούν να αλλάζουν συνεχώς την επιφάνεια επίθεσης προκειμένου να αυξηθεί το κόστος (από άποψη χρόνου και πόρων) και η δυσκολία εκτέλεσης επιτυχημένων επιθέσεων.

Το MAZE παρουσιάζει ενα σφαλές σύστημα αποθήκευσης στο οποίο τα αρχεία που πρεπει να προστατεύονται χωρίζονται σε κομμάτια και ψευδο-τυχαία διασκορπίζονται μέσα σε ένα μεγάλο,

συνεχώς μεταβαλλόμενο λαβύρινθο υπολογιστών.Η μετάβαση από έναν υπολογιστή σε εναν άλλο μέσα στο λαβύρινθο είναι πιθανό μόνο ακολουθώντας τις έγκαιρες δημιουργημένες πόρτες, οι οποίες υλοποιούνται με τη χρήση SSH.Σε κάθε υπολογιστή, μπορεί να υπάρχουν πολλές ανοιχτές πόρτες, και το καθένα να οδηγεί σε διαφορετικό υπολογιστή. Ετσι για να ανακτήσει ένα αρχείο, ο χρήστης πρέπει να ακολουθήσει ένα πρόγραμμα που παρέχεται από την υπηρεσία MAZE μόνο σε εξουσιοδοτημένους χρήστες.Το πρόγραμμα ενημερώνει τον πελάτη για τις πόρτες που πρέπει να διασχίσει για να ανακτήσει όλα τα κομμάτια του αρχείου. Επιπλέον οι υπολογιστές εντός του MAZE έχουν δύο περιόδους ανανέωσης:
- Το πρώτο επανεκκινεί τον υπολογιστή και επαναφορτώνει το λογισμικό του συστήματος από ένα καθαρό αντίγραφο για να ματαιώσει επιθέσεις.
- Το δεύτερο τροποποιεί τα κομμάτια του αρχείου για να γίνει ασύμβατο με τα κομμάτια αρχείου πριν από την τροποποίηση.
Προκειμένου οι attackers να ανακτήσουν με επιτυχία ένα αρχείο, θα πρέπει να ανακτήσουν όλα τα κομμάτια του αρχείου εντός της δεύτερης περιόδου ανανέωσης

Secure Shell (SSH) Protocol Overview

Μπορεί να χρησιμοποιηθεί για απομακρυσμένη πρόσβαση σε γραμμή εντολών, μεταφορά αρχείων και tunneling.Το SSH σχεδιάστηκε ως αντικατάσταση του Telnet το οποίο μετέφερε πακέτα χωρίς κρυπτογράφηση μέσω του Διαδικτύου.Στο πρωτόκολλο Telnet, οποιοσδήποτε με packet sniffer θα μπορούσε να δει τα περιεχόμενα του πακέτου, τα οποία γίνοται προβληματικά όταν αυτά τα πακέτα περιέχουν προσωπικές ή μυστικές πληροφορίες.
Το MAZE χρησιμοποιεί το πρωτόκολλο Secure Shell (SSH) στην εφαρμογή του επειδή επιτρέπει την ασφαλή απομακρυσμένη πρόσβαση γραμμής εντολών και υποστηρίζει tunneling , και τα δυο ειναι θεμελιώδεις για το σχεδιασμό του MAZE.

Το SSH χωρίζει τα δεδομένα σε μια σειρά πακέτων που περιέχουν τα ακόλουθα πεδία:
packet length, padding amount, payload, additional padding και Message Authentication Code (MAC). Ολόκληρα τα πακέτα εκτος του packet length και του MAC είναι κρυπτογραφημένα. Για να εξασφαλίσει τη σύνδεση μεταξύ πελάτη και διακομιστή, το SSH χρησιμοποιεί τρεις τεχνικές χειρισμού δεδομένων:
symmetric encryption, asymmetric encryption και hashing.
Το symmetric encryption χρησιμοποιείται από το SSH για την κρυπτογράφηση ολόκληρης της σύνδεσης.Το μυστικό κλειδί δημιουργείται χρησιμοποιώντας το Diffie Hellman key exchange.Τα δεδομένα που αποστέλλονται μέσω SSH κρυπτογραφούνται και αποκρυπτογραφούνται χρησιμοποιώντας αυτό το μυστικό κλειδί

Asymmetric encryption ssh, χρησιμοποιείται από το διακομιστή για τον έλεγχο ταυτότητας του πελάτη.Αυτή η διαδικασία ονομάζεται συνήθως SSH-key based authentication.Ο πελάτης δημιουργεί ένα ζεύγος κλειδιών και μεταφορτώνει το δημόσιο κλειδί σε κάθε διακομιστή που επιθυμεί να έχει πρόσβαση.Μόλις δημιουργηθεί μια ασφαλής σύνδεση
μεταξύ πελάτη και διακομιστή μέσω symmetric encryption ,ο διακομιστής επικυρώνει τον πελάτη στέλνοντας ένα μήνυμα (challenge) πρόκλησης, κρυπτογραφημένο με το δημόσιο κλειδί του πελάτη, στον πελάτη. Εαν ο πελάτης καταφέρει να αποκρυπτογραφήσει το μήνυμα πρόκλησης τότε έχει αποδείξει ότι έχει το σχετικό (private) ιδιωτικό κλειδί και
επομένως, επικυρώνεται. Hashing χρησιμοποιείται στο SSH για τον υπολογισμό του MAC,
το οποίο εξασφαλίζει ένα received message was not corrupted or altered.Το MAC υπολογίζεται ως το hash του symmetric key, sequence number και του data.Όταν το πακέτο φτάσει στον προορισμό του,ο δέκτης υπολογίζει το ίδιο hash των δεδομένων και το συγκρίνει με το MAC στο ληφθέν πακέτο για να εξασφαλίσει την ακεραιότητά του.

SSH Tunneling

Το SSH Tunneling είναι μια μέθοδος για τη μεταφορά αυθαίρετων μη κρυπτογραφημένων δεδομένων σε μια ασφαλής SSH σύνδεση.Το SSH υποστηρίζει διάφορους τύπους tunneling αλλά στο MAZE θα εστιάσουμε κυρίως σε δυο:
direct port forwarding και reverseport forwarding
Στο direct port forwarding το μηχάνημα του πελάτη που εκτελεί ενα client SSH ανοίγει μια σήραγγα(tunnel) και προωθεί οποιαδήποτε δεδομένα αποστέλλονται σε ένα διακομιστή SSH.Ο διακομιστής SSH μπορεί να ζει στο end-point ή να είναι ξεχωριστός από το end-point, οπότε ο διακομιστής SSH συνδέεται με το end-point και του στέλνει τα κρυπτογραφημένα δεδομένα

libssh

Το libssh είναι μια βιβλιοθήκη τηςC που υλοποιεί τα πρωτόκολλα SSHv1 και SSHv2 τόσο για τον πελάτη οσο και για της εφαρμογές διακομιστών.Παρέχει ένα API για τους προγραμματιστές να γράφουν προγράμματα που χρησιμοποιούν το πρωτόκολλο SSH.

SSH Session

Για να δημιουργήσουμε μια σύνδεση SSH με το libssh, διαθέτουμε ένα νέο SSH session object καλώντας τη συνάρτηση ssh_new (), η οποία επιστρέφει ενα ssh session object.Μόλις δημιουργηθεί ενα session μπορούμε να συνδεθούμε σε ένα διακομιστή SSH χρησιμοποιώντας ssh connect(…), περνώντας το ssh session object που δημιουργήσαμε.

Authentication

Μετά τη σύνδεση σε ένα ssh server, πιστοποιούμε τόσο τον διακομιστή όσο και τον χρήστη.
Ο διακομιστής πιστοποιείται για να εξασφαλίστει ότι είναι γνωστό και ασφαλές , για να μπορείς να συνεχίσεις την σύνδεση.Ο έλεγχος ταυτότητας διακομιστή μπορεί να πραγματοποιηθεί χρησιμοποιώντας την εντολή verify_knownhost(…) η οποία λαμβάνει ένα αντικείμενο συνεδρίας ssh ως παράμετρο.Ο χρήστης πιστοποιείται έτσι ώστε ο διακομιστής να μπορεί να αναγνωρίσει τον χρήστη και να επαληθεύσει την ταυτότητα.Η πιο κοινή μέθοδος ελέγχου ταυτότητας χρήστη είναι η χρήση ενός κωδικού πρόσβασης.Ένας κωδικός πρόσβασης αποστέλλεται στο διακομιστή και είτε το αποδέχεται ή όχι.Η δεύτερη πιο κοινή μέθοδος είναι ο έλεγχος ταυτότητας με βάση το κλειδί.
Μόλις πιστοποιηθεί ο χρήστης, ο διακομιστής του παρέχει πρόσβαση σε πολλούς πόρους, όπως το port forwarding.

SSH Tunnels with libssh

το libssh υποστηρίζει δύο τύπους tunneling:
direct port forwarding and reverse port forwarding.

• Direct Port Forwarding:το μηχάνημα πελάτη ανοίγει μια σήραγγα στο διακομιστή σε μια συγκεκριμένη θύρα(port). Όταν μια εφαρμογή στο μηχάνημα πελάτη συνδέεται με το localhost σε αυτή τη θύρα, τα δεδομένα τους προωθούνται στο διακομιστή.Για να εκτελέσουμε port forwarding μεσω libssh δημιουργούμε ένα ξεχωριστό κανάλι που θα χρησιμοποιηθεί για τη σήραγγα δεδομένου ότι τα κανάλια SSH επεξεργάζονται μόνο μία υπηρεσία. Τα κανάλια SSH δημιουργούνται χρησιμοποιώντας το ssh channel new(…) η οποία λαμβάνει ένα ssh session object σαν παράμετρο.

Στη συνέχεια, ανοίγουμε ένα κανάλι προώθησης με την εντολή ssh channel open forward(…). Για να πραγματοποιήσουμε την πραγματική προώθηση χρησιμοποιούμε το ssh channel write(…), για να γράψει τα εισερχόμενα δεδομένα στο διακομιστή.

• Reverse Port Forwarding: Στο Reverse Port Forwarding ο διακομιστής ακούει σε μια θύρα (port). Οποτεδήποτε γίνει μια σύνδεση σε αυτή τη θύρα στο διακομιστή τα εισερχόμενα δεδομένα προωθούνται πίσω στον πελάτη.Για να εκτελέσεουμε reverse port forwarding χρησιμοποιώντας το libssh ζητάμε από τον διακομιστή να ακούει για εισερχόμενες συνδέσεις σε συγκεκριμένη θύρα χρησιμοποιώντας το ssh channel listen forward(…). Για να αποδεχτουμε της εισερχόμενες TCP / IP συνδέσης χρησιμοποιούμε το ssh channel accept forward(…). Μόλις μια TCP / IP σύνδεση γίνει αποδεκτή επιστρέφεται ένα ssh channel object.Στη συνέχεια, διαβάζουμε δεδομένα από το Κανάλι SSH χρησιμοποιώντας το ssh channel read nonblocking(…) και στέλνουμε τα δεδομένα πίσω στον πελάτη χρησιμοποιώντας ssh channel write(…).

MAZE Design

Το σύστημα αποθήκευσης MAZE cloud έχει δύο παραλλαγές, δηλαδή το reactive MAZE και το proactive MAZE, καθένα με τα πλεονεκτήματα και τα μειονεκτήματά του.Και οι δύο προσεγγίσεις χωρίζονται σε δύο μέρη:service-side, και client-side. Το service-side είναι υπεύθυνο για την προετοιμασία των κόμβων που δημιουργούν το χρονοδιάγραμμα , και ακολουθούν το χρονοδιάγραμμα για να δημιουργήσουν της κατάλληλες σήραγγες. Το client-side είναι υπεύθυνο για τη λήψη παραμέτρων από έναν χρήστη , και ακολουθεί το παραγόμενο πρόγραμμα για την αποθήκευση ή την ανάκτηση ενός αρχείου με βάση τις παραμέτρους του χρήστη.

Reactive Approach

Το reactive approach του MAZE περιλαμβάνει τη δημιουργία σηράγγων on-demand.Με άλλα λόγια, οι σήραγγες δημιουργούνται μόνο όταν ένας χρήστης θέλει να αποθηκεύσει ή να ανακτήσει ένα αρχείο. Το πρόγραμμα πελάτη εκτελείται στο μηχάνημα του χρήστη και είναι υπεύθυνο για την αποδοχή παραμέτρων από τον χρήστη και την αποστολή τους στην πύλη. Το πρόγραμμα πελάτη δέχεται μονο τρεις παράμετρους: εάν θέλετε να αποθηκεύσει ή να ανακτήσει ένα αρχείο, τη διαδρομή προς το αρχείο και έναν κωδικό πρόσβασης. Η πύλη τρέχει ένα διακομιστή υποδοχής, ακούγοντας για αιτήματα από client programs. Μόλις ληφθεί ένα αίτημα, η πύλη αναλύει τις παραμέτρους του χρήστη και τις χρησιμοποιεί για να ξεκινήσει τη ρύθμιση της σήραγγας. Η διαδικασία ρύθμισης της σήραγγας περιλαμβάνει τη διάσπαση του αρχείου σε κομμάτια και στη συνέχεια χρησιμοποιώντας τον κωδικό πρόσβασης για να δημιουργεί και κατασκευάζει το πρόγραμμα δηλαδή την δημιουργία των σηράγγων. Ο κωδικός πρόσβασης χρησιμοποιείται για να καθορίσει ποιοι κόμβοι και θύρες θα χρησιμοποιηθούν για την δημιουργία σηράγγων. Σε υψηλό επίπεδο το χρονοδιάγραμμα
παραγωγής λειτουργεί ως εξής: κάνουμε hash τον κωδικό πρόσβασης και χρησιμοποιούμε τα δύο πρώτα bytes της εξόδου hash για να καθορίσουμε τη θύρα του τελικού σημείου της σήραγγας, τα μεσαία δύο bytes για να προσδιορίσουμε την διεύθυνση IP του τελικού σημείου προορισμού(end point), και τα τελευταία δύο bytes για τον προσδιορισμό του
αριθμού θύρας τελικού σημείου προορισμού. Επαναλαμβάνουμε την προαναφερθείσα διαδικασία για τον αριθμό των επιθυμητών σηράγγων.

Service-Side

Τι service-side του MAZE είναι υπεύθυνο για την προετοιμασία των κόμβων, για δημιουργία χρονοδιαγράμματος με βάση τον κωδικό πρόσβασης και να διαβάσει το χρονοδιάγραμμα για να δημιουργήσει κατάλληλες σήραγγες. Στο MAZE τα nodes γίνονται hardened έτσι ώστε το κόστος της διάσχισης ενός κανονικού συνδέσμου δικτύου να γίνει πολύ μεγαλύτερο από το κόστος της διάσχισης μιας σήραγγας. Το hardening του node συνεπάγεται στον περιορισμό της σύνδεσεις με τα τελικά σημεία της σήραγγας έτσι ώστε να μπορούν να δέχονται μόνο συνδέσεις από localhost. Οι σήραγγες είναι μίας-χρήση μόνο, οταν το πρόγραμμα διασχίσει μια σήραγγα, κανένα άλλο πρόγραμμα ή εισβολέας δεν μπορεί να χρησιμοποιήσει αυτή τη σήραγγα. Το κάθε node έχει δυο refresh periods:
1) Τα nodes επανεκκινούνται και το λογισμικό του συστήματος αντιγράφεται πάνω από ένα ασφαλές μέσο μόνο για ανάγνωση
2) Τα κομμάτια αρχείων τροποποιούνται για να γίνουν μη συμβατά με τα κομμάτια του αρχείου πριν από την τροποποίηση
Κατά την πρώτη περίοδο ανανέωσης, οι σήραγγες κατεδαφίζονται και αποκαθίστανται και οποιοσδήποτε attacker εκδιώκεται από τον κόμβο. Στη δεύτερη περίοδο ανανέωσης, τα κομμάτια αρχείων τροποποιούνται χρησιμοποιώντας proactive secret sharing

Schedule Generation

Ο αλγόριθμος δημιουργίας χρονοδιαγράμματος είναι υπεύθυνος για τη δημιουργία μιας σειράς διαδοχικών σηράγγων για να διασχίσει ο πελάτης για να αποθηκεύσει ή να ανακτήσει ένα αρχείο. Διαδοχικές σήραγγες αναφέρονται όταν οι σήραγγες δημιουργούνται από μια πηγή σε έναν προορισμό (source to a destination), και η πηγή της επόμενης σήραγγας είναι ο προορισμός της προηγούμενης σήραγγας. Ο αλγόριθμος δημιουργίας χρονοδιαγράμματος χρησιμοποιεί hashing για τον προσδιορισμό των τελικών σημείων προέλευσης και προορισμού των σηράγγων από τον κωδικό πρόσβασης του χρήστη

Tunnel Setup

Η πραγματική εγκατάσταση και κατασκευή σηράγγων εκτελείται από ένα forwarding program που εκτελείται στον κόμβο πύλης. Το forwarding program είναι υπεύθυνο για τη δημιουργία σηράγγων που καθορίζονται από το χρονοδιάγραμμα. Οι σήραγγες χρησιμοποιούνται από το πρόγραμμα-πελάτη για να ανακτήσουν κομμάτια του αρχείου απο κάθε κόμβο. Για να ολοκληρωθεί η μετάβαση απο κόμβο σε κόμβο ο πρόγραμμα πελάτη συνδέεται στο τρέχον μηχάνημα σε μια συγκεκριμένη θύρα και η σήραγγα ανακατευθύνει τη σύνδεση σε διαφορετικό κόμβο σε διαφορετική θύρα.
Το MAZE χρησιμοποιεί σήραγγες για δύο κύριους λόγους:
(1) μια σήραγγα παρέχει μια ασφαλή σύνδεση πάνω από μια μη αξιόπιστη σύνδεση δικτύου
(2) είναι μιας χρήσης και μονόδρομο
Αφού ένα πρόγραμμα χρησιμοποιείσει μια σήραγγα για να συνδεθεί με έναν διαφορετικό κόμβο, η ίδια σήραγγα δεν μπορεί να χρησιμοποιηθεί ξανά εκτός αν αποκατασταθεί ο κόμβος.

Αρνητικά στην χρήση σηράγγων

Ένα σημαντικό bottleneck στο MAZE είναι η χρήση των σηράγγων. Όταν ένας πελάτης θέλει να αποθηκεύσει ή να ανακτήσει ένα αρχείο, δημιουργείται ένα σύνολο σηράγγων για να διασχίσουν τα client-programs. Η δημιουργία και η διέλευση μιας σήραγγας απαιτεί περισσότερο χρόνο από την άμεση σύνδεση με έναν κόμβο μέσω SSH. Ως εκ τούτου, έχοντας περισσότερα κομμάτια αρχείων οδηγεί σε περισσότερες σήραγγες για να διασχίσει ο πελατης επομένως οδηγεί και σε πιο αργή

απόδοση. Ωστόσο, με το κόστος της βραδύτερης αποθήκευσης και ανάκτησης , η αύξηση των σηράγγων έχει ως αποτέλεσμα
μεγαλύτερη ασφάλεια. Αυτή η ανταλλαγή μεταξύ απόδοσης και ασφάλειας είναι ανάλογη με εκείνη του onion routing, στο οποίο όσο μεγαλύτερος είναι ο αριθμός των στρωμάτων τόσο πιο αργή είναι η απόδοση. Ωστόσο, αυτή η επιβράδυνση της απόδοσης επιτρέπει
αυξημένη ασφάλεια για ανώνυμη περιήγηση στο Διαδίκτυο.

Συμπερασματα για το MAZE

Τα cloud συστήματα αποθήκευσης αυξάνονται σε δημοτικότητα τόσο για επαγγελματική όσο και για προσωπική χρήση λόγω της αύξησης της διαδικτυακής συνεργασίας και της υπόσχεσης αποθήκευσης σε cloud να είναι προσβάσιμα ανά πάσα στιγμή, οπουδήποτε.
Ωστόσο, η στατική φύση των cloud συστημάτων επιτρέπει στον εισβολέα να μελετήσει διεξοδικά το σύστημα και τα τρωτά σημεία του χωρίς φόβο. Για να αντιμετωπίσουν τα προαναφερθέντα,το MAZE χρησιμοποιεί Moving Target Defense και χρησιμοποιεί ακομα tunneling για να αποτρέψει της επιθέσεις.

Περιορισμοι

Οι νόμιμοι αριθμοί θύρας TCP κυμαίνονται από 1.024 έως 65.535. Λόγω του περιορισμένου αριθμού θυρών, είναι πιθανό να προκύψουν συγκρούσεις. Μια σύγκρουση συμβαίνει όταν το MAZE επιχειρεί να δημιουργήσει μια σήραγγα από το ίδιο τελικό σημείο πηγής σε ένα διαφορετικό τελικό σημείο προορισμού. Με άλλα λόγια, εάν ένας διακομιστής ακούει ήδη σε έναν συγκεκριμένο αριθμό θύρας και προωθεί συνδέσεις σε ένα συγκεκριμένο τελικό σημείο προορισμού δεν μπορεί να του ζητηθεί να ακούσει τον ίδιο αριθμό θύρας αλλά να κάνει forward την σύνδεση σε ένα διαφορετικό τελικό σημείο προορισμού (end-point).Η προσπάθεια να γίνει η προαναφερθείσα θα έχει ως αποτέλεσμα την αποτυχία δημιουργίας της σήραγγας. Η σύγκρουση μπορεί να συμβεί σε δύο περιπτώσεις:
στην παραγωγή προγράμματος για έναν πελάτη ή λόγω ταυτόχρονων πελατών.
Συγκρούσεις συμβαίνουν στην παραγωγή χρονοδιάγραμματων για έναν πελάτη, στο ίδιο χρονοδιάγραμμα δύο σήραγγες εχουν τον ίδιο αριθμό θύρας πηγής, και αυτο γίνεται οταν τα δύο πρώτα bytes της εξόδου του password hashing ισούνται. Συγκρούσεις συμβαίνουν σε ταυτόχρονους πελάτες όταν το πρόγραμμα πολλαπλών πελατών περιέχει τους ίδιους αριθμούς θύρας πηγής αλλά διαφορετικούς προορισμός. Για να αντιμετωπίσουμε αυτό το πρόβλημα μπορούμε να διατηρήσουμε μια λίστα με αριθμούς ανοιχτών θυρών. Μόλις υπάρξει σύγκρουση θα μπορούσαμε να χρησιμοποιήσουμε linear probing. Ωστόσο, εάν χρησιμοποιούνται όλες οι θύρες, μπορούμε να διατηρήσουμε μια ουρά από σήραγγες που θέλουν να εγκατασταθούν σε έναν συγκεκριμένο αριθμό θύρας. Μόλις χρησιμοποιηθεί μια σήραγγα στην ουρά, μπορούμε δημιουργήστε την επόμενη σήραγγα στην ουρά. Το μειονέκτημα αυτής της προσέγγισης, είναι ότι ένας χρήστης μπόρει να αντιμετωπίσει επιβράδυνση επιδόσεων επειδή πρέπει να περιμένουν να χρησιμοποιηθούν προηγούμενες σήραγγες για να δημιουργηθούν νέες.

Wireless Network Security by SSH Tunneling

Η ασύρματη επικοινωνία, όπως το Wi-Fi, είναι ανασφαλής και είναι ευάλωτο σε επιθέσεις όπως το packet sniffing.Τα credentials σύνδεσης στα πακέτα HTTP μπορούν να εξαχθούν από τα πακέτα IEEE 802.11 χρησιμοποιώντας εργαλεία όπως το Wire-shark και μπορούν να χρησιμοποιηθούν από τους επιτιθέμενους. Σε πολλές εταιρείες η απομακρυσμένη πρόσβαση σε επιχειρηματικές εφαρμογές έχει γίνει μια κρίσιμη αποστολή.Σχεδόν όλες οι επιχειρήσεις χρησιμοποιούν το διαδίκτυο για τις καθημερινές τους εργασίες, αλλα το internet-based remote access προσθέτει σημαντικούς κινδύνους. Τα ευαίσθητα δεδομένα μπορούν να συλληφθούν, να τροποποιηθούν ή να επαναχρησιμοποιηθούν οπουδήποτε μεταξύ των απομακρυσμένων εργαζομένων και των corporate

firewalls. Το packet-sniffing και το session-hijacking είναι δύο επικίνδυνες επιθέσεις και βρίσκονται σε συνεχή άνοδο. Λόγω της εύκολης διαθεσιμότητα εξελιγμένων εργαλείων, έχει γίνει ευκολότερη η μεταφορά τέτοιων επιθέσεων. Αν δεν ελεγχθούν, αυτές οι δύο επιθέσεις μπορούν να φέρουν κάτω ολόκληρο το σύστημα. Ο στόχος μας είναι να παρουσιάσουμε το SSH tunneling ως ένας τρόπος για να εξασφαλίσουμε τη σύνδεση μεταξύ του πελάτη και του διακομιστή για να αποφύγουμε το packet sniffing όπως και το session hijacking. Μια δυνατότητα του SSH ονομάζεται port forwarding που επιτρέπει μη ασφαλή TCP/IP δεδομένα να γίνουν tunneled μεσω δημόσιων και ιδιωτικων δίκτυων μέσω μιας σύνδεσης που είναι εξασφαλισμένη και κρυπτογραφημένη.

PACKET SNIFFING

Το packet sniffing ορίζεται ως ανάλυση πακέτων ή πρωτοκόλλου. Περιγράφει τη διαδικασία λήψης και παρακολούθησης ζωντανών δεδομένων καθώς ροές σε ένα δίκτυο για να πάρετε μια περίληψη του τι συμβαίνει στο δίκτυο. Το packet sniffer είναι ένα εργαλείο που χρησιμοποιείται για τη σύλληψη δεδομένον που διέρχονται από το δίκτυο. Το packet analysis μπορεί να μας βοηθήσει να καθορίσουμε τα χαρακτηριστικά του δικτύου,να μάθουμε ποιος έχει χρησιμοποίησή το δίκτυο,να καθορίσουμε το εύρος ζώνης και τη χρήση του. Μπορούμε να αναγνωρίσουμε τους μέγιστους χρόνους χρήσης δικτύων η ακόμα και να ανιχνεύσουμε πιθανές επιθέσεις. Ενα packet sniffer παρακολουθεί και καταγράφει πακέτα σε ένα δίκτυο τα οποία μπορούμε να αποκωδικοποιήσουμε αργότερα σύμφωνα με κάποια προδιαγραφή. Τα wireless packet sniffers χρησιμοποιούνται ευρέως στη διαχείριση δικτύων και απο ερευνητικές κοινότητες λόγω της ικανότητάς τους να παρακολουθούν το δίκτυο κυκλοφορίας στο στρώμα MAC καθώς και στα στρώματα που βρίσκονται παραπάνω. Ιδιαίτερα τα packet sniffers χρησιμοποιούνται ευρέως ως εργαλεία για τη διάγνωση ή την ανακάλυψη προβλήματων δικτύου καθώς και για παρακολούθηση μιας συγκεκριμένης δραστηριότητας. Αλλα μπόρουν επισης να χρησιμοποιηθούν για λάθος η κακόβουλους σκοπούς όπως η παρακολούθηση σημαντικών ή ιδιωτικών πληροφοριών σαν τα όνομα χρήστων και τους κωδικούς πρόσβασης τους.

Υπάρχουν τέσσερις κύριοι τρόποι λειτουργίας του IEEE 802.11 Network Interface Cards (NICs).Ο πρώτος ονομάζεται master mode (Access Point), δεύτερος είναι ο client mode (Station) ,ο τρίτος ειναι ad-hoc mode και το τελευταίο είναι το monitor mode. Εδώ το φιλτράρισμα όλων των πακέτων που λαμβάνονται με βάση τη διεύθυνση MAC είναι απενεργοποιημένα και η λειτουργία επιτρέπει στο NIC να επεξεργάζεται όλα τα που αισθάνεται στο δίκτυο. Μια NIC λειτουργία πρέπει να συνδέεται με ένα σημείο πρόσβασης (AP) ή να συνδέεται σε ένα ad hoc δίκτυο για να κάνει sniff την κυκλοφορία του ασύρματου δικτύου. Από την άλλη το NIC μπορεί να ακούει σε ένα συγκεκριμένο κανάλι στο monitor mode που επιτρέπει το packet sniffing χρησιμοποιώντας ένα packet sniffer όπως Wireshark σε ένα εντελώς παθητικό τρόπο, δηλαδή χωρίς να χρειάζεται να ενταχθεί στο ασύρματο δίκτυο και να είναι σε θέση να μεταδώσει τα πακέτα.

SSH TUNNELING

Η σήραγγα Secure Shell (SSH) είναι μια μέθοδος που δημιουργεί μια εικονική σήραγγα μέσω του ασύρματου δικτύου με τον πελάτη και τον διακομιστή να είναι τα τελικά σημεία (end points) της σήραγγας. Την εικονική σήραγγα μπορούμε να την φανταστούμε ως μια κρυπτογραφημένη διαδρομή που μεταφέρει την κίνηση(traffic) μεταξύ του πελάτη και του διακομιστή. Οποιαδήποτε κίνηση που ρέει μέσω αυτής της σήραγγας κρυπτογραφείται από προεπιλογή. Κάθε φορά που κάποιος πελάτης θέλει να επικοινωνήσει με το διακομιστή, αυτός πρέπει να αρχικοποιεί την εικονική σήραγγα. Η δημιουργία της σήραγγας γίνεται με τη βοήθεια του port forwarding. Υπάρχουν τέσσερις οντότητες στη λειτουργία της σήραγγας SSH, είναι οι εξής:

1)Web browser (Client side)
2)SSH client (Client side)
3)SSH server (Server side)
4)Web server (Server side)

1) Web Browser: Αυτός είναι ο πραγματικός πελάτης που πρέπει να επικοινωνήσει με το διακομιστή. Ο πελάτης χρησιμοποιεί το πρόγραμμα περιήγησης ιστού για να πάρει πρόσβαση στο διακομιστή. Η σήραγγα SSH μπορεί να γίνει χρησιμοποιώντας οποιοδήποτε πρότυπο πρόγραμμα περιήγησης. Στο πρόγραμμα περιήγησης ιστού ο χρήστης πρέπει να αλλάξει τις ρυθμίσεις για να κατευθύνει την κυκλοφορία στο proxy server. Αυτή η έννοια ονομάζεται port forwarding. Η διεύθυνση του proxy server είναι αυτή του πελάτη SSH αυτή η διαμόρφωση είναι σημαντική καθώς τώρα αναγκάζει την κυκλοφορία να ρέει από το πρόγραμμα περιήγησης ιστού στον client-SSH και όχι από το πρόγραμμα περιήγησης ιστού στον διακομιστή ιστού.

2) SSH Client: To ssh-client παίρνει την κίνηση από τον ιστό περιήγησης, χρησιμοποιεί αλγόριθμους κρυπτογράφησης για την κρυπτογράφηση της κυκλοφορίας. Οποιοσδήποτε καλός αλγόριθμος κρυπτογράφησης μπορεί να χρησιμοποιηθεί για το σκοπό αυτό. Αφού τα δεδομένα γίνουν έτοιμα για αποστολή, δημιουργείται η σήραγγα SSH. Ο πελάτης SSH προσδιορίζει με μοναδικό τρόπο έναν συγκεκριμένο διακομιστή SSH. Ως εκ τούτου, η κίνηση που αποστέλλεται από τον ssh-client και μπορεί να ληφθεί μόνο από τον αντίστοιχο διακομιστή SSH που έχει εντοπίσει ο πελάτης SSH. Μετά τη δημιουργία της σήραγγας, η κυκλοφορία αποστέλλεται μέσω του διαδικτύου μέσω της σήραγγας, στον διακομιστή SSH.

3) SSH Server: Ο διακομιστής SSH, όπως υποδηλώνει το όνομα, κατοικεί στο διακομιστή και βρίσκεται στο άλλο άκρο της εικονικής σήραγγας. Παίρνει την κίνηση που μπήκε μέσα από αυτό την σήραγγα.Ο ssh διακομιστής χρησιμοποιεί αλγόριθμους αποκρυπτογράφησης για να αλλάξει τα δεδομένα πίσω στην αρχική τους μορφή. Οι αλγόριθμοι αποκρυπτογράφησης που χρησιμοποιούνται είναι μετα απο σύμφωνηση ίδιο με τους αλγόριθμους που χρησιμοποιούνται από τον πελάτη SSH.

4) Web Server: Ο διακομιστής web λαμβάνει το αίτημα μέσω του διακομιστή SSH και κάνει την επεξεργασία του. Ο διακομιστής ιστού είναι εντελώς αδιάφορο σε σχέση με τη ροή της κυκλοφορίας προς και από αυτήν. Αφού η απάντηση στο αίτημα γίνει έτοιμη αποστέλλεται πίσω στο διακομιστή SSH, ο οποίος στη συνέχεια το στέλνει στον πελάτη SSH και ούτω καθεξής.
Η επικοινωνία μεταξύ του προγράμματος περιήγησης ιστού στον πελάτη SSH και του διακομιστή SSH στον διακομιστή Web είναι εκτός σήραγγας. Ως εκ τούτου, ουσιαστικά η σήραγγα υπάρχει μόνο μεταξύ του πελάτη SSH και του SSH διακομιστή, καθώς αυτή είναι η μόνη διαδρομή στο διαδίκτυο.
Το καλο της σήραγγας SSH είναι ότι, μόλις δημιουργηθεί μια σήραγγα μεταξύ του πελάτη και του διακομιστή, παραμένει ενεργή καθ ' όλη τη διάρκεια της συνεδρία. Με αποτέλεσμα η σήραγγα μόλις δημιουργηθεί για μια συνεδρία, να μπορεί να χρησιμοποιηθεί για τη μεταφορά οποιουδήποτε όγκου δεδομένων προς και από πίσω χωρίς να ανησυχούν για την πιθανότητα επιθέσεων. Αυτό σημαίνει επίσης ότι η εναέρια εγκατάσταση της σήραγγας πρέπει να γίνει μόνο μία φορά.

Πλεονεκτήματα της SSH

Υπάρχουν πολλά πλεονεκτήματα της σήραγγας SSH και ως εκ τούτου είναι χωρίζεται σε 3 κατηγορίες ως εξής:

1) τέσσερα οφέλη ασφάλειας.

2) πλεονέκτημα όταν χρησιμοποιείται πέρα από τα ”clear text” πρωτόκολλα

3) γενικά πλεονεκτήματα.

1) τέσσερα οφέλη ασφάλειας: Το SSH tunneling παρέχει τα ακόλουθα τέσσερα βασικά οφέλη ασφάλειας:

i) User Authentication
ii) Host Authentication
iii) Data Encryption
iv) Data Integrity

i) Authentication, αναφέρεται επίσης ως ταυτότητα χρήστη, είναι το μέσο με το οποίο ένα σύστημα επαληθεύει ότι η πρόσβαση δίνεται,προορίζετα μόνο σε χρήστες. Η secure shell υλοποιήσεις περιλαμβάνουν έλεγχο ταυτότητας κωδικού πρόσβασης και δημόσιου κλειδιού

ii) Data Encryption,αναφέρεται στην κρυπτογράφηση των δεδομένων για να αποφευχθεί από επιθέσεις, χρησιμοποιώντας αλγόριθμους κρυπτογράφησης. Η σήραγγα SSH μπορεί να χρησιμοποιήσει οποινδήποτε αλγόριθμο κρυπτογράφησης και πρότυπα.

iii) Data integrity, σημαίνει ότι τα δεδομένα που αποστέλλονται από τον πελάτη λαμβάνονται όπως είναι από το διακομιστή. Η σήραγγα φροντίζει έτσι ώστε η ακεραιότητα των δεδομένων να διατηρείται καθώς η κυκλοφορία ρέει μέσω της σήραγγας

Τα ανωτέρω τέσσερα πλεονεκτήματα είναι άμεσα διαθέσιμα όταν χρησιμοποιείται η σήραγγα

2) πλεονέκτημα όταν χρησιμοποιείται πέρα από τα ”clear text” πρωτόκολλα
Όταν χρησιμοποιείτε ένα μη ασφαλές “clear text” protocol όπως το telnet,οποιοσδήποτε στο δίκτυο μπορεί να κλέψει τους κωδικούς πρόσβασής σας και άλλα ευαίσθητες πληροφορίες.

3) γενικά πλεονεκτήματα.

Α) η σήραγγα SSH παρέχει πλήρη προστασία από επιθέσεις.

Β) Το SSH tunneling εξασφαλίζει τα session cookies, με άμεσο αποτέλεσμα να προστατευει απο session hijacking.

γ) η σήραγγα SSH έχει την ικανότητα να συγκρατεί 16 συνδέσεις ταυτόχρονα και έχει ελάχιστες καθυστερήσεις

ΣΥΜΠΈΡΑΣΜΑ

Το SSH tunneling είναι μια απλή & αποτελεσματική λύση για ασφαλή παράδοση περιεχομένου μέσω Διαδικτύου. Το ssh tunneling θα ασφαλίσει αποτελεσματικά την περιήγηση στο διαδίκτυο απο τα packet sniffers. Σε σύγκριση με τα άλλα μέτρα ασφαλείας συνδέσμων, δικτύων και εφαρμογών, όπως WEP, IPsec και PGP , το Secure Shell είναι σχετικά ασφαλές, αξιόπιστο, γρήγορο και εύκολο. Με την ανάπτυξη του secure shell , οι εταιρείες μπορούν να δημιουργούν μια ολοκληρωμένη πλατφόρμα με σήραγγα γενικής χρήσης που μπορεί να χρησιμοποιηθεί σε μια εφαρμογή για να διασφαλίσει διάφορες πολιτικές ασφάλειας, την ιδιωτικότητα, την αυθεντικότητα, και την ακεραιότητα.

Cryptography in the era of quantum computers

Η ιδιωτική επικοινωνία ατόμων και Οργανισμών προστατεύεται ηλεκτρονικά με κρυπτογραφία. Η κρυπτογραφία προστατεύει τις πληροφορίες μας καθώς ταξιδεύει και αποθηκεύεται στο διαδίκτυο. Η υπάρχουσα κρυπτογραφία δημόσιου κλειδιού βασίζεται στη δυσκολία του factoring και στη δυσκολία υπολογισμού των elliptic curve discrete αλογαρίθμων . Επειδή αυτά τα δύο προβλήματα θα επιλυθούν εύκολα και αποτελεσματικά από έναν κβαντικό υπολογιστή αρκετά μεγάλης κλίμακας, εξετάζουμε τώρα προσεγγίσεις κρυπτογραφίας που να είναι ανθεκτικές σε έναν εισβολέα που έχει πρόσβαση σε έναν κβαντικό υπολογιστή. Πρέπει να αναπτύξουμε κρυπτοσυστήματα των οποίων η ασφάλεια βασίζεται σε διαφορετικά, σκληρά μαθηματικά προβλήματα που είναι ανθεκτικά στην επίλυση από έναν κβαντικό υπολογιστή μεγάλης κλίμακας.

Τι εμπλέκεται στην μετα-κβαντική κρυπτογραφία

Οποισδήποτε νέος αλγόριθμος κρυπτογραφίας πρέπει να ενσωματωθεί με υπάρχοντα πρωτόκολλα, όπως το TLS. Ένα νέο κρυπτοσύστημα πρέπει επιπλέον να μετράει:

- το μέγεθος των κλειδιών κρυπτογράφησης και των υπογραφών

-Το χρόνο που απαιτείται για την κρυπτογράφηση και αποκρυπτογράφηση σε κάθε άκρο ενός διαύλου επικοινωνίας ή για την υπογραφή μηνυμάτων και την επαλήθευση υπογραφών

- Το ποσό της κυκλοφορίας που αποστέλλονται μέσω του καλωδίου που απαιτείται για να ολοκληρωθεί η κρυπτογράφηση ή αποκρυπτογράφηση ή να μεταδώσει μια υπογραφή για κάθε προτεινόμενη εναλλακτική λύση.

Τα προτεινόμενα κρυπτοσυστήματα απαιτούν επίσης προσεκτική κρυπτανάλυση, για να διαπιστωθεί εάν υπάρχουν αδυναμίες που θα μπορούσε να εκμεταλλευτεί ένας επιτιθέμενος.

Το έργο της ανάπτυξης νέων κρυπτοσυστημάτων που είναι κβαντικά ανθεκτικά πρέπει να γίνει open sourced, σε πλήρη προβολή των κρυπτογράφων, των οργανισμών, του κοινού και των κυβερνήσεων σε όλο τον κόσμο, για να διασφαλιστεί ότι τα νέα πρότυπα που αναδύονται έχουν ελεγχθεί καλά από την κοινότητα και να διασφαλιστεί ότι υπάρχει διεθνής υποστήριξη.

Τέλος, πρέπει να κάνουμε όλα αυτά γρήγορα επειδή δεν γνωρίζουμε πότε θα σπάσει η κλασική κρυπτογραφία. Είναι δύσκολο και χρονοβόρο να τραβήξουν και να αντικαταστήσουν την υπάρχουσα κρυπτογραφία από το λογισμικό παραγωγής. Προσθέστε σε όλα αυτά το γεγονόντα ότι κάποιος θα μπορούσε να αποθηκεύσει τα υπάρχοντα κρυπτογραφημένα δεδομένα και να τα ξεκλειδώσει στο μέλλον μόλις πάρουν στα χέρια τους έναν κβαντικό υπολογιστή

Post-Quantum Cryptography SSH

Δεδομένης της σημασίας του SSH ο πρώιμος σχεδιασμός για τη μετάβαση στη μετα-κβαντική κρυπτογραφία πρέπει να ξεκινήσει σύντομα. Η ασύμμετρη κρυπτογραφία στο SSH πρέπει να μεταναστεύσει σε δύο μέρη:

Key exchange: κατά τη διάρκεια αυτού του βήματος, ο διακομιστής και ο πελάτης ανταλλάσσουν κρυπτογραφικά μηνύματα χρησιμοποιώντας ασύμμετρους αλγόριθμους ανταλλαγής κλειδιών (όπως RSA και ECDH) που θα χρησιμοποιηθούν για την εξαγωγή ενός συμμετρικού κλειδιού. Αυτό το συμμετρικό κλειδί θα χρησιμοποιηθεί για την κρυπτογράφηση της υπόλοιπης περιόδου σύνδεσης.Αυτοί οι ασύμμετροι αλγόριθμοι ανταλλαγής κλειδιών θα πρέπει να αντικατασταθούν με αλγόριθμους κβαντικής ασφάλειας. Οπως περιγράφηκε παραπάνω, οι συμμετρικοί αλγόριθμοι κλειδιών που χρησιμοποιούνται στην ανταλλαγή κλειδιών (π.χ. AES) δεν είναι τόσο ευάλωτοι στους κβαντικούς υπολογιστές, οπότε απλά πρέπει να αυξήσουμε το μήκος του κλειδιού για να εξασφαλίσουμε τη συμμετρική κρυπτογραφία έναντι ενός κβαντικού αντιπάλου.

Authentication: Κατά τη διάρκεια αυτού του βήματος, ο διακομιστής (και προαιρετικά ο πελάτης) αποδεικνύει την ταυτότητά του χρησιμοποιώντας το δημόσιο κλειδί του. Οι αλγόριθμοι υπογραφής (όπως RSA ή ECDSA) δεν είναι κβαντικοί ασφαλείς και πρέπει να ενημερωθούν.

Μέχρι να αποκτήσουμε πλήρη εμπιστοσύνη στα νέα μετα-κβαντικά κρυπτογραφικά σχήματα, συνιστάται η χρήση τους σε αυτό που ονομάζουμε υβριδική λειτουργία. Για να επιτευχθεί αυτό, τόσο οι ανταλλαγές κλειδιών όσο και οι υπογραφές πρέπει να εκτελούνται παράλληλα, δημιουργώντας τόσο μια κλασική ανταλλαγή/υπογραφή όσο και μετα κβαντική. Τα προκύπτοντα μηνύματα/υπογραφές συνδυάζονται, προσφέροντας την ασφάλεια κατά των κβαντικών επιθέσεων, διατηρώντας παράλληλα την ασφάλεια των σημερινών συστημάτων.

Αναφορές

1.T. Ylonen, C. Lonvick, Ed (2006).The Secure Shell (SSH) Protocol Architecture

2. Kunal Meher, Divya, Midhunchakkaravarthy (2020) The State-of-the-art Cryptographic Algorithms

3. Vasxo Xu, (2020) MAZE: A Secure Cloud Storage Service Using MovingTarget Defense and Secure Shell Protocol (SSH) Tunneling

4.Aniket Burande, Ankita Pise, Sameer Desai, Yohan Martin, Sejal D’mello(2014).Wireless Network Security by SSH Tunneling

5. Post-Quantum Cryptography Microsoft Research team.