Κεφάλαιο 8

ΑΣΦΑΛΕΙΑ ΣΤΑ ΚΑΤΑΝΕΜΗΜΕΝΑ ΣΥΣΤΗΜΑΤΑ

Σύνοψη

Η ασφάλεια είναι κεντρικής σημασίας θέμα για τα Κατανεμημένα Συστήματα και καλύπτει ευρεία περιοχή εφαρμογής, από τα δίκτυα, τους εξυπηρετητές, τους τερματικούς σταθμούς, τα λειτουργικά συστήματα και τις εφαρμογές λογισμικού. Όλα τα παραπάνω εξετάζονται διεξοδικά προκειμένου να δοθεί στον αναγνώστη μια συνολική εικόνα της ασφάλειας. Θέματα ασφαλείας που θα εξεταστούν είναι τα εξής: απειλές ασφαλείας, ασφάλειες στο μοντέλο αναφοράς, μηχανισμοί ασφάλειας, VPN, κρυπτογραφία, αυθεντικοποίηση, έλεγχος πρόσβασης, εμπιστευτικότητα, ψηφιακές υπογραφές, υποδομές δημοσίου κλειδιού (PKI), ακεραιότητα πληροφορίας, κατανεμημένη άρνηση υπηρεσίας (DDoS), ασφάλεια επιπέδου IP, συστήματα ανίχνευσης παρείσφρησης - Intrusion Detection Systems (IDSs), συστήματα πρόληψης παρείσφρησης (IPSs), firewalls, και άλλα. Οι διάφοροι τύποι απειλών και επιθέσεων, θα πρέπει να ληφθούν σοβαρά υπόψη κατά την σχεδίαση ενός Κ.Σ.

8.1 Εισαγωγή

Ο στόχος των κατανεμημένων συστημάτων είναι η μεγιστοποίηση της απόδοσης συστημάτων συνδέοντας χρήστες και πόρους πληροφορικής με οικονομικό, διαφανή και αξιόπιστο τρόπο. Εξασφαλίζουν επίσης την ανοχή σφαλμάτων και επιτρέπουν την προσβασιμότητα σε εναλλακτικούς πόρους σε περίπτωση που ένας από τους κόμβους αποτύχει. Για την επίτευξη των παραπάνω στόχων, η ασφάλεια ενός κατανεμημένου συστήματος απαιτεί σχολαστικό σχεδιασμό και καλή εφαρμογή. Όλα τα στάδια της ασφάλειας πρέπει να εφαρμόζονται με ιδιαίτερη προσοχή, συμπεριλαμβανομένου του σχεδιασμού, της υλοποίησης, της λειτουργίας και της διαχείρισης των κατανεμημένων συστημάτων. Η ασφάλεια αφορά τα συστήματα, τα προγράμματα και τα δεδομένα που περιλαμβάνονται στα κατανεμημένα συστήματα ενώ επηρέαζεται από διάφορες παράμετρους. Τρείς ιδιαίτερα σημαντικές αρχές ασφαλείας είναι: η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα, γνωστές και ως η τριάδα CIA (Confidentiality, Integrity, Availability).

Εμπιστευτικότητα: Η εμπιστευτικότητα αφορά τη διατήρηση των πόρων και των δεδομένων σε κρυφή ή απρόσιτη κατάσταση για μη εξουσιοδοτημένα άτομα. Αντιμετωπίζεται από μηχανισμούς ελέγχου πρόσβασης σε λειτουργικά συστήματα ή λογισμικό εφαρμογών. Εάν τα δεδομένα είναι προσβάσιμα μέσω του συστήματος αρχείων ή είναι ορατά μέσω δικτύου, η εμπιστευτικότητα αντιμετωπίζεται με κρυπτογράφηση των δεδομένων. Οι αποφάσεις μιας εφαρμογής σχετικά με το εάν τα δεδομένα πρέπει να είναι προσβάσιμα σε έναν χρήστη εξαρτώνται από την αναγνώριση και τον έλεγχο ταυτότητας του χρήστη ή της υπηρεσίας.

Ακεραιότητα: Η ακεραιότητα ασχολείται με την αξιοπιστία των δεδομένων ή των πόρων. Οι μηχανισμοί ακεραιότητας είναι υπεύθυνοι για την αποτροπή μη εξουσιοδοτημένων αλλαγών στα δεδομένα ή την ανίχνευση ότι έχουν γίνει αλλαγές. Οι μηχανισμοί ακεραιότητας χρησιμοποιούνται για την επικύρωση της ταυτότητας χρηστών, συστημάτων και υπηρεσιών μέσω αλγορίθμων ελέγχου ταυτότητας.

Διαθεσιμότητα: Η διαθεσιμότητα αφορά την πρόσβαση στα δεδομένα ή τις υπηρεσίες υπολογιστών. Είναι η ιδιότητα ότι ένα σύστημα είναι προσβάσιμο και λειτουργικό. Η προσβασιμότητα περιλαμβάνει την ανοχή σφαλμάτων, την ανάκτηση και την αποκατάσταση.

8.1.1 Υπηρεσίες ασφάλειας στα κατανεμημένα συστήματα.

Οι παραπάνω αρχές έχουν ιδιαίτερη σημασία για όλους τους τύπους των συστημάτων, ενώ έχουν αναπτυχθεί διάφορες υπηρεσίες και τεχνικες για τη διασφάλιση τους. Στα κατανεμημένα συστήματα, για τη διασφάλιση της τριάδας CIA τρεις υπηρεσίες ασφαλείας αποδεικνύονται ιδιαίτερα αποτελεσματικές:

- Ο Έλεγχος πρόσβασης
- Η Αυθεντικοποίηση
- Η Μη Αποποίηση

Έλεγχος Πρόσβασης

Ο έλεγχος πρόσβασης είναι μια τεχνική ασφαλείας που ρυθμίζει ποιος μπορεί να έχει πρόσβαση ή δικαιώματα εκτέλεσης πάνω στους πόρους από ένα υπολογιστικό περιβάλλον. Είναι μια θεμελιώδης έννοια στην ασφάλεια που ελαχιστοποιεί τον κίνδυνο για τις επιχειρήσεις και τους οργανισμούς. Υπάρχουν δύο τύποι ελέγχου πρόσβασης: ο φυσικός και ο λογικός. Ο έλεγχος φυσικής πρόσβασης περιορίζει την πρόσβαση σε χώρους όπως πανεπιστημιουπόλεις, κτίρια, δωμάτια και φυσικά στοιχεία πληροφορικής. Για την ασφάλεια των υποδομών τους οι οργανισμοί χρησιμοποιούν ηλεκτρονικά συστήματα ελέγχου πρόσβασης που βασίζονται σε διαπιστευτήρια χρήστη, σε συσκευές ανάγνωσης καρτών πρόσβασης, στον έλεγχο και τις αναλυτικές αναφορές που προκύπτουν από την κεντρική παρακολούθηση της πρόσβασης των εργαζομένων σε περιορισμένες τοποθεσίες επιχειρήσεων και ιδιόκτητους χώρους, όπως κέντρα δεδομένων. Ορισμένα από αυτά τα συστήματα ενσωματώνουν πίνακες ελέγχου πρόσβασης για περιορισμό της εισόδου σε δωμάτια και κτίρια, καθώς και δυνατότητες συναγερμού και κλειδώματος, για την αποτροπή μη εξουσιοδοτημένης πρόσβασης ή λειτουργίας.

Ο λογικός έλεγχος πρόσβασης περιορίζει τις συνδέσεις σε δίκτυα υπολογιστών, λειτουργικά συστήματα, αρχεία συστήματος, εφαρμογές και δεδομένα. Τα συστήματα ελέγχου λογικής πρόσβασης εκτελούν έλεγχο ταυτότητας και εξουσιοδότηση χρηστών και οντοτήτων αξιολογώντας τα απαιτούμενα διαπιστευτήρια σύνδεσης που μπορεί να περιλαμβάνουν κωδικούς πρόσβασης, προσωπικούς αριθμούς αναγνώρισης, βιομετρικές σαρώσεις, διακριτικά ασφαλείας ή άλλους παράγοντες ελέγχου ταυτότητας. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (Multi Factor Authentication/MFA), ο οποίος απαιτεί δύο ή περισσότερους παράγοντες ελέγχου ταυτότητας, είναι συχνά σημαντικό μέρος μιας πολυεπίπεδης άμυνας για την προστασία των συστημάτων μέσω ελέγχου πρόσβασης.

Σε μια απλή αλληλεπίδραση πελάτη-διακομιστή, ο διακομιστής μπορεί να επιθυμεί να περιορίσει την πρόσβαση σε πόρους. Οι τυπικές τεχνικές για να γίνει αυτό είναι:

• Πίνακας Δικαιωμάτων Πρόσβασης

• Δυνατότητες Χρηστών

• Ετικέτες

Ένας πίνακας ελέγχου πρόσβασης είναι ένα ενιαίο ψηφιακό αρχείο ή γραπτή εγγραφή με «θέματα» και «αντικείμενα» και προσδιορίζει ποιες ενέργειες, εάν υπάρχουν, επιτρέπονται από άτομα. Με απλά λόγια, η μήτρα επιτρέπει μόνο σε ορισμένα άτομα (υποκείμενα) να έχουν πρόσβαση σε ορισμένες πληροφορίες (αντικείμενα).

Όπως φαίνεται στον παρακάτω πίνακα, ο πίνακας αποτελείται από ένα ή περισσότερα θέματα (άτομα) κατά μήκος ενός άξονα και τα συσχετισμένα αντικείμενα (αρχεία) κατά μήκος του άλλου άξονα. Σε ορισμένα άτομα επιτρέπεται η ανάγνωση (R), η εγγραφή (W), η εκτέλεση (E) και η διαγραφή (D) αρχείων. Η περιορισμένη πρόσβαση υποδεικνύεται με μια παύλα.

HR Personnel

HR Records	Gary	Sandy	Tonya	Robyn	Samantha
Salary files	RWED	R-E-D	----	RWED	RWED
Promotion list	---D	R-E-	RWED	RWED	----
Performance Reports	RWED	RW-D	----	----	RWE-

Η βασική ιδέα είναι η εξής: ας υποθέσουμε ότι σχεδιάζουμε ένα σύστημα υπολογιστή έτσι ώστε η πρόσβαση σε ένα αντικείμενο, να προϋποθέτει ότι το πρόγραμμα που επιχειρεί να προσπελάσει το αντικείμενο να έχει ένα διακριτικό που του παραχωρεί τα απαραίτητα δικαιώματα για αυτή την κίνηση. Αυτό το διακριτικό προσδιορίζει ένα αντικείμενο και δίνει στο πρόγραμμα την εξουσία να εκτελέσει ένα συγκεκριμένο σύνολο ενεργειών (όπως ανάγνωση ή γραφή) σε αυτό το αντικείμενο. Ένα τέτοιο διακριτικό είναι γνωστό ως ικανότητα.

Μια ικανότητα (γνωστή σε ορισμένα συστήματα ως κλειδί) είναι ένα μεταδιδόμενο δείγμα εξουσίας που δεν μπορεί να κατασκευαστεί πλαστή μορφή του. Η ικανότητα είναι συνδεδεμένη με ένα χαρακτηριστικό που αναγράφει ένα αντικείμενο μαζί με ένα συσχετισμένο σύνολο δικαιωμάτων πρόσβασης. Ένα πρόγραμμα χρήστη σε ένα λειτουργικό σύστημα που βασίζεται σε δυνατότητες πρέπει να χρησιμοποιεί δυνατότητες πρόσβασης για να μπορεί να προσπελάσει αντικείμενα.

Τα έγγραφα επισημαίνονται με μια ταξινόμηση, όπως "Εμπιστευτικό", "Μυστικό" ή "Άκρως Απόρρητο". Αυτή η ετικέτα ασφαλείας θα είναι καθαρά ορατή στο έγγραφο.

Οι άνθρωποι λαμβάνουν άδεια, χρησιμοποιώντας το ίδιο σχέδιο. Για παράδειγμα, κάποιος μπορεί να διαγραφεί σε επίπεδο "Μυστικό", που σημαίνει ότι μπορεί να διαβάσει έγγραφα "Μυστικό", αλλά όχι ένα έγγραφο με την ένδειξη "Ακρως απόρρητο".

Αυθεντικοποίηση

Η Αυθεντικοποίηση είναι μια διαδικασία που διασφαλίζει και επιβεβαιώνει την ταυτότητα ενός χρήστη. Ο έλεγχος ταυτότητας είναι ένας από τους πέντε πυλώνες της διασφάλισης

πληροφοριών (ΙΑ). Τα άλλα τέσσερα είναι η ακεραιότητα, η διαθεσιμότητα, η εμπιστευτικότητα και η μη άρνηση.

Η αυθεντικοποίηση ξεκινά όταν ένας χρήστης προσπαθεί να αποκτήσει πρόσβαση σε πληροφορίες. Αρχικά, ο χρήστης πρέπει να αποδείξει τα δικαιώματα πρόσβασης και την ταυτότητά του. Όταν συνδέονται σε έναν υπολογιστή, οι χρήστες συνήθως εισάγουν ονόματα χρήστη και κωδικούς πρόσβασης για σκοπούς ελέγχου ταυτότητας. Αυτός ο συνδυασμός χαρακτηριστικών, ο οποίος πρέπει να εκχωρηθεί σε κάθε χρήση, επαληθεύει την πρόσβαση. Ωστόσο, αυτός ο τύπος ελέγχου ταυτότητας μπορεί να παρακαμφθεί από κακόβουλους χρήστες με διάφορους τρόπους.

Μια καλύτερη μορφή αυθεντικοποίησης, τα βιομετρικά στοιχεία, εξαρτάται από την παρουσία και τη βιολογική σύνθεση του χρήστη (δηλαδή αμφιβληστροειδή ή δακτυλικά αποτυπώματα). Αυτή η τεχνολογία καθιστά πιο δύσκολο για τους χάκερ να εισβάλουν σε συστήματα υπολογιστών.

Ένας σχετικός όρος είναι η ακεραιότητα του μηνύματος, που συχνά ονομάζεται έλεγχος ταυτότητας μηνύματος. Είναι συχνά σημαντικό να βεβαιωθείτε ότι ένα ληφθέν μήνυμα δεν έχει παραβιαστεί κατά τη μεταφορά.Μερικές φορές δεν υπάρχει απαίτηση για απόρρητο του μηνύματος κατά τη μεταφορά. μερικές φορές υπάρχει. Μια μορφή ισχυρού αθροίσματος που βασίζεται σε κρυπτογραφικές τεχνικές προσαρτάται στα μηνύματα για τέτοιους σκοπούς. Αυτό μερικές φορές ονομάζεται ψηφιακή υπογραφή ή κωδικός ελέγχου ταυτότητας μηνύματος (MAC).

Μη Αποποίηση

Όσον αφορά την ψηφιακή ασφάλεια, η μη αποποίηση σημαίνει να διασφαλιστεί ότι ένα μεταφερόμενο μήνυμα έχει σταλεί και ληφθεί από τα μέρη που ισχυρίζονται ότι έστειλαν και έλαβαν το μήνυμα. Η μη άρνηση είναι ένας τρόπος για να διασφαλιστεί ότι ο αποστολέας ενός μηνύματος δεν μπορεί αργότερα να αρνηθεί ότι έστειλε το μήνυμα και ότι ο παραλήπτης δεν μπορεί να αρνηθεί ότι έλαβε το μήνυμα.

Η μη αποποίηση μπορεί να επιτευχθεί με τη χρήση των:

- ψηφιακών υπογραφών: λειτουργούν ως ένα μοναδικό αναγνωριστικό για ένα άτομο, όπως μια γραπτή υπογραφή.
- Χρονικές σημάνσεις (timestamps): οι χρονικές σημάνσεις περιέχουν την ημερομηνία και την ώρα που συντάχθηκε ένα έγγραφο και αποδεικνύει ότι ένα έγγραφο υπήρχε σε μια συγκεκριμένη στιγμή.

8.2 Απειλές και επιθέσεις ασφαλείας

Σκεφτείτε έναν κόμβο και έναν διακομιστή που συνδέονται μέσω μιας σύνδεσης δικτύου. Δεδομένου ότι τα στοχοποιημένα συστήματα μπορεί να πάσχουν από κάποιες ευπάθειες ή αδυναμίες λογισμικού υπάρχουν διάφορες επιθέσεις που μπορούν να πραγματοποιηθούν σε τέτοιες διασυνδέσεις όπως:

- Η Παθητική Εγγραφή καναλιού
- Η Ενεργητική Εγγραφή καναλιού
- Η Άρνηση παροχής υπηρεσιών
- Η Παραποίηση δεδομένων και αρχείων
- Η Επανάληψη σήματος

- Η Ανάλυση Κυκλοφορίας

Με βάση την ποικιλομορφία των παραπάνω επιθέσεων είναι προφανές ότι οι απειλές ασφάλειας και οι επιθέσεις μπορούν να αφορούν οποιοδήποτε επίπεδο των κατανεμημένων συστημάτων, από το φυσικό έως και το επίπεδο εφαρμογής. Παρουσιάζεται λοιπόν ιδιαίτερη προκληση στην ασφάλεια των κατανεμημένων συστημάτων καθώς είναι δυνατό μια επιτυχής επίθεση σε ένα στρώμα να καταστήσει άχρηστα τα μέτρα ασφάλειας που λαμβάνονται από τα άλλα στρώματα. Παρακάτω αναλύονται οι βασικές κατηγορίες ευπαθειών και απειλών που αποτελούν κυρίαρχα ρίσκα για τα κατανεμημένα συστήματα

8.2.1 Ευπάθειες και Απειλές Ασφαλείας Κατανεμημένων Συστημάτων

Οι ευπάθειες αναφέρονται σε σχεδιαστικές ή λειτουργικές αδυναμίες που που ενδέχεται να θέσουν ένα σύστημα σε κίνδυνο απέναντι σε επιτιθέμενους. Αντίστοιχα, μια απειλή αντικατοπτρίζει τη δυνατότητα ή την πιθανότητα ένας εισβολέας να προκαλέσει ζημιά ή να υπονομεύσει το σύστημα. Επιπλέον, η ασφάλεια είναι μια ιδιότητα συστημάτων από άκρο σε άκρο. Κατά συνέπεια, τα τρωτά σημεία ενός κατανεμημένου συστήματος ομαδοποιούνται ευρέως με βάση τα λειτουργικά μπλοκ που ορίζουν το κατανεμημένο σύστημα. Λογικά, αυτά τα λειτουργικά μπλοκ και οι λειτουργίες τους αποτελούν επίσης την επιφάνεια απειλής/επίθεσης για τα συστήματα όπου ένας εισβολέας/αντίπαλος μπορεί να εκμεταλλευτεί μια ευπάθεια για να θέσει σε κίνδυνο το σύστημα. Σε υψηλό επίπεδο, η επιφάνεια επίθεσης σχετίζεται με τους συμβιβασμούς των φυσικών πόρων, του σχήματος επικοινωνίας, των μηχανισμών συντονισμού, των ίδιων των παρεχόμενων υπηρεσιών και των πολιτικών χρήσης των δεδομένων στα οποία βασίζονται οι υπηρεσίες. Παρακάτω αναλύονται μερικές βασικές κατηγορίες Ευπαθειών-Απειλών

Ευπάθειες-Απειλές ελέγχου πρόσβασης/ Διαχείριση ταυτότητας

Ο έλεγχος πρόσβασης ή εισαγωγής καθορίζει την εξουσιοδοτημένη συμμετοχή ενός πόρου, ενός χρήστη ή μιας υπηρεσίας σε ένα κατανεμημένο σύστημα. Αυτό μπορεί να περιλαμβάνει την παροχή δικαιωμάτων πρόσβασης για ανάγνωση/εγγραφή και χρήση πάνω σε δεδομένα και λειτουργικότητες κατά τη διάρκεια ζωής μιας υπηρεσίας.

Οι πιθανές απειλές και οι επακόλουθες επιθέσεις περιλαμβάνουν την μεταμφίεση ή την πλαστογράφηση ταυτότητας για την απόκτηση δικαιωμάτων πρόσβασης στα δεδομένα. Μπορούν επίσης να περιλαμβάνουν επιθέσεις άρνησης υπηρεσίας (DoS) που περιορίζουν επιζήμια την πρόσβαση (π.χ. εξάντληση υπολογιστικών πόρων και καναλιών επικοινωνίας) που οδηγούν σε αδυναμία πρόσβασης και μη διαθεσιμότητας των κατανεμημένων πόρων/υπηρεσιών. Αξίζει να τονιστεί ότι η διανομή πόρων συχνά συνεπάγεται περισσότερα σημεία ελέγχου πρόσβασης, καθώς και περισσότερες πληροφορίες που μεταφέρονται στο σύστημα για υποστήριξη ελέγχου πρόσβασης, αυξάνοντας έτσι την επιφάνεια επίθεσης του συστήματος.

Μια οντότητα κατανεμημένου συστήματος (πόρος, υπηρεσία, χρήστης ή στοιχείο δεδομένων) συμμετέχει σε ένα κατανεμημένο σύστημα με φυσική ή λογική ταυτότητα. Η ταυτότητα, που εκχωρείται στατικά ή δυναμικά, μπορεί να είναι ένα αναγνωριστικό πόρου, όπως ένα αναγνωριστικό όνομα ή ένας αριθμός . Εδώ, η εξουσιοδότηση μπορεί να καθοριστεί ως προς την ταυτότητα του χρήστη ή/και του πόρου, συμπεριλαμβανομένης της χρήσης ονομάτων σύνδεσης και κωδικών πρόσβασης. Έτσι, μια δραστηριότητα που περιλαμβάνει παραποίηση της ταυτότητας αποτελεί πιθανή απειλή.

Μεταφορά Δεδομένων

Οι απειλές σε επίπεδο δικτύου καλύπτουν τη δρομολόγηση, τη μετάδοση μηνυμάτων, τις μεθόδους δημοσίευσης-εγγραφής και αλληλεπίδρασης πόρων, την ενεργοποίηση απόκρισης βάσει συμβάντων και τις απειλές σε όλη τη στοίβα του ενδιάμεσου λογισμικού. Επιπλέον,

αυτές μπορεί να είναι παθητικές (ακρόαση) ή ενεργητικές επιθέσεις (τροποποίηση δεδομένων). Χαρακτηριστικό παράδειγμα είναι η επίθεση Man In the Middle (επίθεση) (MITM) όπου ο εισβολέας εισάγεται μεταξύ του προγράμματος περιήγησης του θύματος και του διακομιστή ιστού για να δημιουργήσει δύο ξεχωριστές συνδέσεις μεταξύ τους. Αυτό δίνει τη δυνατότητα στον εισβολέα να καταγράφει ενεργά όλα τα μηνύματα και να τροποποιεί επιλεκτικά δεδομένα χωρίς να ενεργοποιεί συναγερμό ύποπτης δραστηριότητας εάν το σύστημα δεν επιβάλλει έλεγχο ταυτότητας τελικού σημείου.

Υπηρεσίες Διαχείρισης και Συντονισμού Πόρων

Αυτή η κρίσιμη ομάδα περιλαμβάνει το φάσμα των απειλών για τους μηχανισμούς (συνήθως πρωτόκολλα ενδιάμεσου λογισμικού) που παρέχουν το συντονισμό των πόρων. Αυτό περιλαμβάνει, μεταξύ άλλων, τις πτυχές του συγχρονισμού, της διαχείρισης αναπαραγωγής, των αλλαγών προβολής, της ταξινόμησης χρόνου/συμβάντος, της γραμμικοποίησης, της συναίνεσης και της δέσμευσης συναλλαγών.

Ασφάλεια δεδομένων

Καθώς ένα κατανεμημένο σύστημα ουσιαστικά λειτουργεί με δεδομένα (σε ηρεμία ή σε κίνηση) στις πτυχές της προέλευσης δεδομένων, της διανομής δεδομένων, της αποθήκευσης δεδομένων ή της χρήσης δεδομένων σε υπηρεσίες, οι κλασικές ιδιότητες της CIA (Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα) άμεσα εφαρμόζονται σε κάθε στοιχείο (και διεπαφές) αυτής της αλυσίδας δεδομένων. Οι απειλές για την εμπιστευτικότητα περιλαμβάνουν απειλές διαρροής πληροφοριών, όπως επιθέσεις σε πλευρικό κανάλι ή επιθέσεις κρυφών καναλιών. Οποιαδήποτε καθυστέρηση ή άρνηση πρόσβασης στα δεδομένα αποτελεί απειλή για τη Διαθεσιμότητα. Οι πτυχές της ακεραιότητας αφορούν οποιονδήποτε συμβιβασμό της ορθότητας των δεδομένων, όπως η παραβίαση της συνέπειας των δεδομένων, όπως παρατηρείται από τους διανεμημένους συμμετέχοντες. Αυτό περιλαμβάνει τους διαφορετικούς τύπους συνέπειας (ισχυρή, ασθενής, χαλαρή, ενδεχόμενη κ.λπ.) σχετικά με τις υπηρεσίες αποθήκευσης και συναλλαγών. Κατά συνέπεια, η αντιμετώπιση της ασφάλειας των στοιχείων δεδομένων ενός κατανεμημένου συστήματος απαιτεί την εξέταση των απειλών που αναφέρονται παραπάνω σε πόρους, έλεγχο πρόσβασης, μεταφορά δεδομένων και υπηρεσίες συντονισμού, καθώς και απειλές δεδομένων με τη μορφή κακόβουλων εφαρμογών, κώδικα και ιών

8.2.2 Επιθέσεις Ασφαλείας

Ένα στοιχείο λογισμικού μπορεί να είναι ανασφαλές, να μην υποστηρίζεται πλέον από τον προμηθευτή λογισμικού ή να χρειάζεται ενημερώσεις ασφαλείας. Εάν το στοιχείο περιέχει ευπάθειες, αυτό μπορεί να θέσει σε κίνδυνο ολόκληρη την εφαρμογή. Τα κοινά χρησιμοποιούμενα στοιχεία τρίτων περιλαμβάνουν διακομιστές εφαρμογών και διαδικτύου, λειτουργικά συστήματα, συστήματα διαχείρισης βάσεων δεδομένων (DBMS), APIs, βιβλιοθήκες ανοιχτού κώδικα και περιβάλλοντα χρόνου εκτέλεσης. Στην παρούσα ενότητα θα μελετήσουμε ορισμένες απο τις επιθέσεις που στοχεύουν στην εκμετάλευση των απειλών και αδυναμιών των κατανεμημένων συστημάτων σε επίπεδο δικτύου και εφαρμογής αλλαι και στο πλαίσιο των πρωτόκολλων δρομολόγησης.

Επιθέσεις σε επίπεδο δικτύου

Τα κατανεμημένα συστήματα χαρακτηρίζονται από τη διασυνδεσιμότητα τους, συνεπώς οι υπάρχουσες επιθέσεις στο επίπεδο δικτύου δύναται να επηρεάσουν άμεσα την ασφάλεια τους, παρακάτω αναλύονται ορισμένες από τις πιο διαδεδομένες επιθέσεις σε επίπεδο δικτύου.

Επιθέσεις με "Κρυφάκουσμα": Αυτές οι επιθέσεις αποτελούνται από την αναρμόδια παρεμπόδιση επικοινωνίας δικτύων και της κοινοποίησης των ανταλλαγμένων πληροφοριών. Αυτό μπορεί να εκτελείται σε αρκετά διαφορετικά στρώματα, για παράδειγμα, στο στρώμα

δικτύων με sniffing στα ανταλλαγμένα πακέτα ή στο φυσικό στρώμα με φυσική υποκλοπή του μέσου πρόσβασης (ενσύρματο ή ασύρματο μέσο).

Επιθέσεις κατάχρησης σύνδεσης: Μια επιτυχής επίθεση κατάχρησης σύνδεσης θα παρέκαμπτε την επικύρωση και των μηχανισμών ελέγχου πρόσβασης και επιτρέπουν σε έναν χρήστη να λάβει την πρόσβαση με περισσότερους προνόμια από τις εξουσιοδοτημένες.

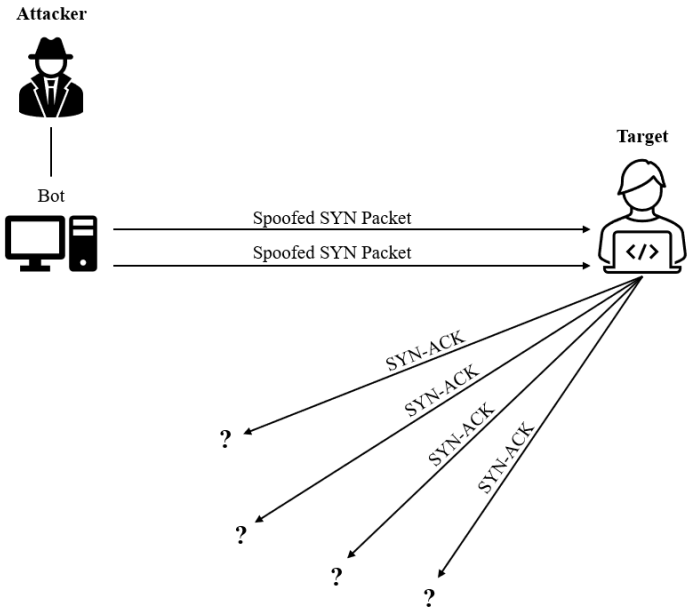
Επιθέσεις Εξαπάτησης: Χαρακτηριστικό παράδειγμα τέτοιου είδους επιθέσεων είναι το IP spoofing, μέσω του οποίου ένα σύστημα είναι πεπεισμένο ότι επικοινωνεί με μία γνωστή αρχή και παρέχει έτσι την πρόσβαση στον επιτιθέμενο. Ο επιτιθέμενος στέλνει ένα πακέτο με μια διεύθυνση προέλευσης IP ενός γνωστού εμπιστευμένου οικοδεσπότη με την αλλαγή του πακέτου στο στρώμα μεταφορών. Ο οικοδεσπότης στόχων θα εξαπατηθεί εφόσον κάνει αποδοχή του πακέτου που έχει μετατραπεί σαν έγκυρο.

Επιθέσεις εισβολής: Οι επιθέσεις εισβολής είναι επιθέσεις όπου ένας κακόβουλος χρήστης αποκτά πρόσβαση σε πόρους ενός συστήματος χωρίς να έχει τα απαραίτητα δικαιώματα μέσω δικτυακής υποδομής Η όλη λογική είναι η εκμετάλλευση των ευπαθειών του δικτύου και των συστημάτων.

Επιθέσεις Πειρατείας: Αυτές οι επιθέσεις είναι ουσιαστικά προσπάθειες να ανακτηθεί αναρμόδια πρόσβαση σε ένα σύστημα με τη χρησιμοποίηση της υπάρχουσας σύνδεσης μιας νόμιμης οντότητας. Παραδείγματος χάριν, στο στρώμα συνόδου, εάν ένας χρήστης αποχωρεί από μια ανοικτή σύνοδο, αυτό μπορεί να υπόκειται στη σύνοδο πειρατεία από έναν επιτιθέμενο. Π.χ πειρατεία συνόδου είναι η TCP ακολουθία αριθμού επίθεσης: Αυτή η επίθεση εμπλέκεται στη σύνοδο επικοινωνίας που τέθηκε μεταξύ του στόχου-αρχής και ενός νόμιμου οικοδεσπότη που άρχισαν τη σύνοδο. Οι επιτιθέμενοι κλέβουν την σύνοδο του νόμιμου οικοδεσπότη με την πρόβλεψη ενός αριθμού ακολουθίας που επιλέγεται από τον οικοδεσπότη στόχων, το οποίο χρησιμοποιείται από το TCP.

Επιθέσεις Άρνησης Υπηρεσιών (DOS): Αυτές οι επιθέσεις στοχεύουν στο να εξαντλήσουν το δίκτυο ή τους πόρους κεντρικών υπολογιστών προκειμένου να το καταστήσουν άχρηστο για τους νόμιμους οικοδεσπότες και τους χρήστες. Περισσότερο ο τύπος προόδου είναι οι διανεμημένες επιθέσεις άρνησης υπηρεσιών (DDoS), όπου ο επιτιθέμενος χρησιμοποιεί τους πόρους από ένα διανεμημένο περιβάλλον ενάντια σε έναν οικοδεσπότη στόχων. Μερικοί γνωστοί τύποι επιθέσεων DOS είναι οι ακόλουθες:

Επίθεση SYN: Σε μια επίθεση SYN, ο επιτιθέμενος εκμεταλλεύεται την ανικανότητα μίας διαδικασίας ενός κεντρικού υπολογιστή να χειριστεί τα εν αναμονή αιτήματα σύνδεσης. Ο επιτεθείς υπερχειλίζει μία διαδικασία του κεντρικού υπολογιστή με τα αιτήματα σύνδεσης, αλλά αυτός δεν αποκρίνεται όταν απαντά ο κεντρικός υπολογιστής εκείνα τα αιτήματα. Αυτό αναγκάζει το επιτιθέμενο σύστημα να καταρρεύσει, περιμένοντας κατάλληλες βεβαιώσεις των αρχικών αιτημάτων.



Εικόνα 1:

PING θανάτου: Αυτό είναι μια πρόωρη επίθεση DOS στην οποία ένας επιτεθείς κάνει αίτηση για ping > 65.536 bytes, το οποίο είναι το μέγιστο που επιτρέπεται μέγεθος για τη IP, προκαλώντας στο σύστημα τη συντριβή ή το καινούριο ξεκίνημα. Τέτοιες επιθέσεις δεν είναι σε λειτουργία σήμερα, δεδομένου ότι τα περισσότερα λειτουργικά συστήματα έχουν εφαρμόσει τα μέτρα ενάντια σε το.

Επιθέσεις σε επίπεδο εφαρμογής

Αυτές οι επιθέσεις ενδιαφέρονται για την εκμετάλλευση των αδυναμιών στο στρώμα εφαρμογής και πραγματικά εστιάζουν στην επίθεση εισβολής στις περισσότερες περιπτώσεις, για παράδειγμα, αδυναμίες ασφάλειας στον κεντρικό υπολογιστή δικτύου, στην συγκεκριμένη τεχνολογία που χρησιμοποιείται για τον ιστοχώρο, ή στους ελαττωματικούς ελέγχους φιλτραρίσματος μιας εισαγωγής από την μεριά του κεντρικού υπολογιστή. Τα παραδείγματα αυτών των επιθέσεων περιλαμβάνουν τις κακόβουλες επιθέσεις λογισμικού (ιοί, Trojans, κ.λπ.), επιθέσεις κεντρικών υπολογιστών δικτύου, απομακρυσμένη εκτέλεση εντολής, έγχυση δομημένης γλώσσας διατύπωσης ερωτημάτων (SQL), και cross-site scripting (XSS). Σαν χαρακτηριστικά παραδείγματα αναλύουμε σύντομα παρακάτω τις 10 επιθέσεις που συμπεριέλαβε ο οργανισμός OWAST στην λίστα με τις δέκα πιο επικίνδυνες ευπάθειες για διαδικτιακές εφαρμογές:

A1:2021-Broken Access Control: Όταν παραβιάζεται ο έλεγχος πρόσβασης, ένας εισβολέας μπορεί να αποκτήσει πρόσβαση σε λογαριασμούς χρηστών, πίνακες διαχειριστή, βάσεις δεδομένων, διακομιστές, ευαίσθητες πληροφορίες, κρίσιμες για τις επιχειρήσεις εφαρμογές και άλλα ευαίσθητα στοιχεία. Μπορεί να επιτρέψει σε μη εξουσιοδοτημένους χρήστες να τροποποιήσουν τα προνόμια προς όφελός τους και να εκτελούν καταστροφικές λειτουργίες όπως η παραβίαση δεδομένων ή η καταστροφή τους.

A2. Cryptographic Failures: Οι κρυπτογραφικές αποτυχίες δίνουν έμφαση σε σφάλματα κρυπτογράφησης ή έλλειψη κρυπτογράφησης που μπορεί να οδηγήσουν στην έκθεση ευαίσθητων δεδομένων.

A3. Injections: Η έγχυση είναι μια επίθεση εναντίον ενός ιστότοπου που εκμεταλλεύεται τρωτά σημεία στη βάση δεδομένων ή σε άλλο μέρος του λειτουργικού περιβάλλοντος. Οι περισσότερες επιθέσεις έγχυσης βασίζονται στην αδυναμία μιας εφαρμογής Ιστού να

διακρίνει τις εισαγωγές χρήστη από τον δικό της κώδικα. Ο εισβολέας μπορεί στη συνέχεια να εκτελέσει κακόβουλο κώδικα στο πλαίσιο της εφαρμογής, αποκτώντας πρόσβαση σε προστατευμένες περιοχές και ευαίσθητα δεδομένα.

A4. Insecure Design: Ο μή ασφαλής σχεδιασμός εστιάζει σε σχεδιαστικά και αρχιτεκτονικά ελαττώματα. Η αποφυγή τους απαιτεί προσεκτική μοντελοποίηση απειλών, λαμβάνοντας υπόψη την ασφάλεια στο στάδιο του σχεδιασμού του λογισμικού και τη χρήση αρχιτεκτονικών αναφοράς.

A5. Security Misconfigurations: Τα συνήθη ζητήματα εγκατάστασης, όπως η εσφαλμένη διαμόρφωση του ελέγχου πρόσβασης, μπορούν να επιτρέψουν στους εισβολείς να αποκτήσουν γρήγορα και εύκολα πρόσβαση σε ευαίσθητα δεδομένα και λειτουργίες εφαρμογών. Αυτά περιλαμβάνουν ακατάλληλα δικαιώματα, περιττή ενεργοποίηση λειτουργιών, χρήση προεπιλεγμένων λογαριασμών και κωδικών πρόσβασης, εσφαλμένες διαμορφωμένες κεφαλίδες HTTP και λεπτομερή μηνύματα σφάλματος.

A6. Vulnerable and Outdated Components: Οι περισσότερες εφαρμογές Ιστού χρησιμοποιούν στοιχεία τρίτων, είτε ανοιχτού κώδικα είτε ιδιόκτητα. Αυτά τα στοιχεία περιέχουν κώδικα που βρίσκεται εκτός του ελέγχου του οργανισμού, ο οποίος μπορεί να οδηγήσει σε ανεπιθύμητα αποτελέσματα, όπως παραβιάσεις ελέγχου προφοράς και επιθέσεις ένεσης.

A7. Identification and Authentication Failures: Λειτουργίες που σχετίζονται με τον έλεγχο ταυτότητας χρήστη και τη διαχείριση περιόδων σύνδεσης, εάν δεν εφαρμοστούν σωστά, μπορούν να εκθέσουν τους χρήστες σε διαπιστευτήρια ασφαλείας, να παραχωρήσουν υπερβολικά δικαιώματα ή να επιτρέψουν στους χρήστες να πλαστοπροσωπήσουν άλλες ταυτότητες.

A8. Software and Data Integrity Failures: Η ακεραιότητα των δεδομένων γίνεται πρωταρχικό μέλημα για την ασφάλεια του λογισμικού, εστιάζει στην ακεραιότητα των ενημερώσεων λογισμικού, των κρίσιμων δεδομένων εφαρμογών και των αγωγών CI/CD. Μια αποτυχία ακεραιότητας λογισμικού και δεδομένων προκύπτει όταν κάποιο από αυτά παραβιάζεται από έναν εισβολέα και άλλα στοιχεία εντός της εφαρμογής δεν επαληθεύουν την ακεραιότητά τους.

A9. Security Logging and Monitoring Failures: Όταν εμφανίζεται ύποπτη συμπεριφορά σε μια εφαρμογή και δεν υπάρχει καταγραφή και παρακολούθηση, οι παραβιάσεις ασφαλείας είναι πολύ πιο πιθανό να είναι επιτυχείς. Αυτή η κατηγορία εστιάζει στον εντοπισμό, την κλιμάκωση και την επίλυση περιστατικών ασφαλείας. Ο εντοπισμός μιας παραβίασης είναι σχεδόν αδύνατος χωρίς καταγραφή και παρακολούθηση.

A10. Server-side Request Forgery (SSRF): Μια ευπάθεια SSRF επιτρέπει σε έναν εισβολέα να έχει πρόσβαση σε δεδομένα που βρίσκονται σε έναν απομακρυσμένο πόρο που βασίζεται σε μια μη επαληθευμένη, προσαρμοσμένη διεύθυνση URL. Ακόμη και οι διακομιστές που προστατεύονται από τείχος προστασίας ή VPN μπορεί να είναι ευάλωτοι σε αυτήν την ευπάθεια, εάν δέχονται μη επικυρωμένα στοιχεία χρήστη.

Καταλήγουμε ότι αναγκαίο είναι στα σύγχρονα δίκτυα να τηρούνται πολιτικές ασφάλειας και να εξελίσσονται συνεχώς αφού και οι επιθέσεις αλλάζουν μορφή και στόχους. Οι διαχειριστές των δικτύων θα πρέπει να είναι σε εγρήγορση γιατί όσο έξυπνες και σύγχρονες υλοποιήσεις άμυνας και να υπάρχουν ο κίνδυνος πάντα ελλοχεύει. Ίσως να μην υπάρχει πουθενά το ασφαλέστερο δίκτυο , το δίκτυο δηλαδή που δεν μπορεί κάποιος να εισέλθει. Εάν η ασφάλεια του δικτύου παραβιάζεται, θα μπορούσαν να υπάρξουν σοβαρές συνέπειες, όπως η απώλεια μυστικότητας, η κλοπή των πληροφοριών, ακόμη και η νομική ευθύνη. Οι τύποι απειλών στην ασφάλεια δικτύων εξελίσσονται συνεχώς.

8.3 Μηχανισμοι Προστασιας Κατανεμημένων συστημάτων

Όπως είδαμε στις παραπάνω ενότητες και υποενότητες τα κατανεμημένα συστήματα καταλαμβάνουν κεντρικό ρολο στις σημερινές επιχειρήσεις, οργανισμούς, ερευνητικά κέντρα και άλλες υποδομές. Συνεπώς η δημιουργία και η εφαρμογή μηχανισμών ασφάλειας που θα προστατεύσουν τα κατανεμημένα συστήματα απο τις απειλές και επιθέσεις που αναλύθηκαν παραπάνω κρίνεται απαραίτητη. Παρακάτω αναλύεται μια σειρά από μηχανισμούς προστασίας που βρίσκουν εφαρμογή στα κατανεμημένα συστήματα.

8.3.1 Κρυπτογραφία

Η κρυπτογραφία είναι απαραίτητη, αλλά από μόνη της δεν είναι πανάκεια. Η χρήση της δεν διασφαλίζει δηλαδή ότι ένα σύστημα είναι ασφαλές. Ωστόσο, αποτελεί δομικό στοιχείο στην κατασκευή ασφαλών κατανεμημένων συστημάτων.

Χρησιμοποιείται για την εφαρμογή μηχανισμών για:

- Εμπιστευτικότητα: κρυπτογράφηση δεδομένων έτσι ώστε οι άλλοι να μην μπορούν να διαβάσουν τα περιεχόμενα ενός μηνύματος (ή αρχείου).
- Έλεγχο ταυτότητας: απόδειξη της προέλευσης ενός μηνύματος (ή της οντότητας που στέλνει αυτό το μήνυμα).
- Ακεραιότητα: επικύρωση ότι το μήνυμα δεν έχει τροποποιηθεί, είτε κακόβουλα είτε κατά λάθος.
- Nonrepudiation: διασφάλιση ότι οι αποστολείς δεν μπορούν να αρνηθούν ψευδώς ότι συνέγραψαν ένα μήνυμα.

Ένας καλός αλγόριθμος κρυπτογραφίας (cryptosystem) έχει τρεις ιδιότητες:

1. Το κρυπτογραφημένο κείμενο πρέπει να φαίνεται τυχαίο. Δεν θα πρέπει να υπάρχουν διακριτά στατιστικά μοτίβα σε αυτό και δεν θα πρέπει να υπάρχουν υποδείξεις για το περιεχόμενο του αρχικού μηνύματος.
2. Δεν υπάρχει τρόπος να εξαγάγετε το αρχικό απλό κείμενο ή κλειδί από το κρυπτογραφημένο κείμενο. Ο μόνος τρόπος για να βρείτε το μήνυμα και το κλειδί θα πρέπει να είναι μέσω μιας επίθεσης brute-force, η οποία είναι μια εξαντλητική αναζήτηση σε όλα τα πιθανά κλειδιά.
3. Τα κλειδιά πρέπει να είναι αρκετά μακριά ώστε να μην είναι εφικτή μια επίθεση ωμής βίας. Ένα "σύντομο" κλειδί AES είναι 128 bit. Με τον ταχύτερο υπερυπολογιστή, θα χρειαστούν ένα δισεκατομμύριο δισεκατομμύρια χρόνια για να σπάσει αυτό το κλειδί. Εάν αξιοποιήσετε ένα δισεκατομμύριο υπολογιστές, τότε μπορείτε να το σπάσετε σε ένα δισεκατομμύριο χρόνια. Κάθε επιπλέον bit ενός κλειδιού διπλασιάζει τον αριθμό των πιθανών πλήκτρων (ένα κλειδί μήκους n έχει 2n~ πιθανά πλήκτρα). Το πιο κοινό μέγεθος κλειδιού AES είναι τα 256 bit, το οποίο θα διαρκέσει 2128 ή 3,4x1038 φορές περισσότερο από το σπάσιμο ενός κλειδιού 128 bit.

8.3.2 Μηχανισμοί προστασίας στο επίπεδο δικτύου

IDPS and Firewalls

Τα συστήματα ανίχνευσης εισβολής (Intrusion Detection Systems, IDS) είναι ειδικό λογισμικό, το οποίο παρακολουθεί αναλυτικά την λειτουργία ενός δικτύου, ώστε να

ανιχνευθεί μια ανώμαλη συμπεριφορά σε αυτό ως επίθεση εισβολέα. Οι επιθέσεις μπορεί να αφορά και χρήστες του εσωτερικού δικτύου. Σε κάθε περίπτωση καταγράφονται οι ύποπτες κινήσεις και δημιουργούνται οι αντίστοιχες αναφορές ή και ενέργειες. Ενδεχόμενα μερικές φορές να δημιουργούνται λάθος συναγερμοί. Αυτό όμως θα πρέπει να είναι το κατά το δυνατόν περιορισμένο για να μην δημιουργηθεί η εντύπωση πως μια πραγματική επίθεση είναι ψεύτικη (false). Είναι προφανέστατο ότι η πρόσβαση στο IDS είναι υψίστης σημασίας και δεν θα πρέπει σε καμία περίπτωση να αλωθεί το ίδιο. Γι' αυτό το σκοπό θα πρέπει να είναι ιδιαίτερα ευαίσθητο και στις παραμικρές περίεργες κινήσεις. Να σημειωθεί ότι τα IDS δεν περιορίζονται μόνο στην κίνηση των δικτύων αλλά και στο έλεγχο των αρχείων, όπως π.χ. αυτών της καταγραφής.

Τα συστήματα ανίχνευσης εισβολών σε δίκτυα (Network Intrusion Detection System,- NIDS) αναλύουν τα πακέτα που διακινούνται σ' ένα δίκτυο και προσπαθούν να εξακριβώσουν εάν κάποιος εισβολέας προσπαθεί να διεισδύσει σε έναν υπολογιστή ή να προκαλέσει μία επίθεση άρνησης εξυπηρέτησης (DoS). Ένα σύστημα NIDS τρέχει συνήθως σε ένα στοιχείο μεταγωγής (hub ή switch) ή ένα δρομολογητή αναλύοντας όλη την κυκλοφορία που διέρχεται από αυτή την συσκευή.

Για να κατανοήσουμε τη λειτουργία ενός τυπικού NIDS, μπορούμε να σκεφτούμε το εξής: Έχουμε έναν ή περισσότερους ειδήμονες στα πρωτόκολλα δικτύων εξοπλισμένους με ειδικά εργαλεία ανάλυσης της κυκλοφορίας ενός δικτύου, οι οποίοι κάθονται και παρακολουθούν την κυκλοφορία που διακινείται στο δίκτυο. Αυτοί γνωρίζουν τα πάντα ακόμη και για τις νεότερες μορφές επιθέσεων που μπορεί να εκκινήσει ένας εισβολέας εναντίον του δικτύου, και ελέγχουν σχολαστικά κάθε πακέτο για να εξακριβώσουν εάν διέρχεται ύποπτη κυκλοφορία από το καλώδιο δικτύου. Εάν βρουν ύποπτη κυκλοφορία, επικοινωνούν αμέσως με τον επόπτη του δικτύου και του γνωστοποιούν τα ευρήματά τους.

Εάν απομακρυνθεί ο ανθρώπινος παράγοντας από το παραπάνω σενάριο, αυτό που απομένει είναι ένα σύστημα ανίχνευσης εισβολών σε δίκτυα, ένα NIDS. Ένα σύστημα NIDS καταγράφει όλη την διερχόμενη κυκλοφορία του δικτύου, με τρόπο παρόμοιο με αυτόν που χρησιμοποιείται από το εργαλείο ανάλυσης. Αφού διαβαστούν οι πληροφορίες στην μνήμη, το σύστημα συγκρίνει τα πακέτα με μοτίβα γνωστών επιθέσεων. Για παράδειγμα, εάν το NIDS παρατηρήσει ότι ένας συγκεκριμένος υπολογιστής στέλνει κατ' επανάληψη πακέτα SYN σ' έναν άλλον υπολογιστή χωρίς να επιχειρήσει ποτέ να ολοκληρώσει την σύνδεση, το NIDS θα χαρακτηρίσει αυτή τη δραστηριότητα σαν επίθεση κατακλυσμού σημάτων SYN και θα κάνει τις κατάλληλες αποτρεπτικές ενέργειες. Ένα καλό NIDS μπορεί να έχει 100 και πλέον μοτίβα αποθηκευμένα στη βάση δεδομένων του.

Τα αποτρεπτικά μέτρα που λαμβάνονται εξαρτώνται από το συγκεκριμένο σύστημα NIDS που χρησιμοποιείται και από τον τρόπο που είναι διαμορφωμένο. Όλα τα συστήματα NIDS έχουν τη δυνατότητα καταγραφής των ύποπτων συμβάντων. Ορισμένα μάλιστα μπορούν να αποθηκεύσουν σε ακατέργαστη μορφή (πακέτα) την κυκλοφορία του δικτύου έτσι ώστε να μπορεί να την αναλύσει κατόπιν ο επόπτης. Άλλα μπορεί να διαμορφωθούν ώστε να στέλνουν στον επόπτη ένα μήνυμα προειδοποίησης, π.χ. μέσω e-mail. Πολλά συστήματα NIDS προσπαθούν να παρεμποδίσουν την ύποπτη επικοινωνία, διακόπτοντας την σύνδεση. Χρησιμοποιώντας, τέλος, ένα firewall ή έναν δρομολογητή, έχουν την ικανότητα να τροποποιούν τους κανόνες φιλτραρίσματος και να μπλοκάρουν το επιτιθέμενο σύστημα.

IPS. Ενα Intrusion Prevention System (IPS) έχει την ίδια λειτουργικότητα με τα συστήματα IDS όσον αφορά τον εντοπισμό, αλλά περιέχει επιπλέον δυνατότητες απόκρισης. Το IPS αναλαμβάνει δράση όταν εντοπίζεται πιθανή επίθεση, κακόβουλη συμπεριφορά ή μη εξουσιοδοτημένος χρήστης. Ουσιαστικά είναι μια συσκευή, η οποία παρακολουθεί τη ροή του δικτύου και βρίσκει πακέτα «επικίνδυνα» τα οποία απορρίπτει. Όλη η κυκλοφορία περνά μέσω του IPS για επιθεώρηση. Η κυκλοφορία φτάνει σε ένα Interface του IPS και βγαίνει σε ένα άλλο interface. Όταν το IPS ανιχνεύσει την κακόβουλη κυκλοφορία, το IPS στέλνει ένα alert στο διοικητικό σταθμό και διαμορφώνει για την παρεμπόδιση της κακόβουλης κυκλοφορίας αμέσως. Το IPS αμύνεται με το φράξιμο της αρχικής και επόμενης κακόβουλης

κυκλοφορίας. Οι περισσότεροι διαχειριστές εγκαθιστούν ένα IPS ακριβώς πίσω από το τείχος προστασίας. Αλλά είναι σαφές ότι μπορεί να ρυθμιστεί σε διαφορετικές διαμορφώσεις ανάλογα τις ανάγκες του οργανισμού.

Firewalls. Το firewall ή το τείχος προστασίας είναι ένας μηχανισμός ασφαλείας δικτύων που έχει τη δυνατότητα να παρακολουθεί την εισερχόμενη και εξερχόμενη κίνηση ενός δικτύου και παρέχει ένα αυτοματοποιημένο/βελτιστοποιημένο σύστημα αποφάσεων το οποίο επιτρέπει ή αποκλείει τους διάφορους τύπους δικτυακής κίνησης βάσει ενός καθορισμένου συνόλου κανόνων ασφαλείας που δημιουργούνται και προσαρμόζονται βάσει των αναγκών και των δυνατοτήτων του κάθε οργανισμού.

Τα τείχη προστασίας αποτελούν την πρώτη γραμμή άμυνας στην ασφάλεια δικτύων. Δημιουργούν εμπόδια μεταξύ ασφαλών και ελεγχόμενων εσωτερικών δικτύων που τηρούν υψηλό βαθμό αξιοπιστίας και μη αξιόπιστων εξωτερικών δικτύων, όπως το Διαδίκτυο. Ένα τείχος προστασίας μπορεί να είναι υλικό, λογισμικό ή και τα δύο. Η προτεινόμενη θέση για την τοποθέτηση ενός firewall είναι πίσω από το gateway router.

Τα τείχη προστασίας είναι ένα θεμελιώδες εργαλείο για τη διαχείριση και την προστασία των δικτύων υπολογιστών. Δεν επιτρέπουν μόνο τον καθορισμό των πακέτων που επιτρέπεται να εισέλθουν σε ένα δίκτυο, αλλά και τον τρόπο τροποποίησης αυτών των πακέτων μεταφράζοντας διευθύνσεις IP και εκτελώντας ανακατεύθυνση θύρας (NAT). Υπάρχουν διάφορα συστήματα τειχών προστασίας διαθέσιμα τα οποία παρέχουν διάφορες δυνατότητες στο πλαίσιο διαθέσιμων εργαλείων και γλωσσών διαμόρφωσης. Επιπλέον τα firewall παρέχουν δυνατότητες προστασίας απέναντι σε ιομορφικά λογισμικά (computer virus-malware) και σε προγράμματα "κατασκοπίας" (spyware).

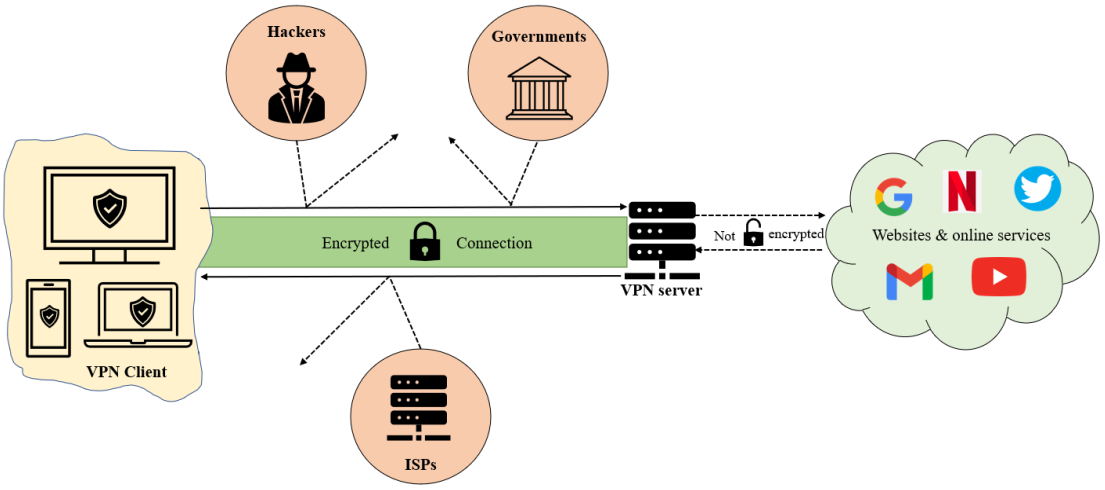
Υπάρχει επίσης η δυνατότητα ελέγχου προγραμμάτων που είναι εγκατεστημένα σε έναν υπολογιστή και ανταλλάσσουν διαδικτυακά πακέτα που ενδέχεται να περιέχουν ευαίσθητα προσωπικά δεδομένα του χρήστη. Σε ορισμένες περιπτώσεις υπάρχει το ενδεχόμενο τα παραπάνω προγράμματα να δημιουργούν ένα κενό ασφαλείας στο πλαίσιο μιας κερκόπορτας (backdoor) η οποία συνήθως προκύπτει από αδυναμίες λογισμικού, τις οποίες ενδέχεται να εκμεταλλευτούν κακόβουλοι χρήστες. Ένα σωστά ρυθμισμένο firewall έχει τη δυνατότητα να ακυρώσει αιτήματα προς τις πιθανές κερκόπορτες, όταν αυτά δεν προέρχονται από την κατάλληλη πηγή, ενώ παράλληλα μπορεί να καταγράφει τις ύποπτες κινήσεις και να ενημερώνει τους χρήστες.

Η κάθε εταιρία ή οργανισμός που έχει συναλλαγές μέσω Internet, οφείλει να εφαρμόσει μια πολιτική ασφαλείας (security policy). Βασικό στοιχείο αυτής της πολιτικής ασφαλείας βρίσκεται το firewall. Για να θεωρηθεί μια εφαρμογή firewall επιτυχημένη, απαιτείται να παρέχει δυνατότητες ελέγχου πάνω στις αιτήσεις εσωτερικών εφαρμογών και υπηρεσιών που στέλνουν αιτήματα προς το Internet και όχι μόνο σε αυτές που τα δέχονται.

Εικονικά Ιδιωτικά Δίκτυα (VPN)

Γενικά, ένα VPN μπορεί να οριστεί σαν ένα δίκτυο που παρέχει μια ασφαλή σύνδεση μεταξύ δύο ιδιωτικών δικτύων. Το δίκτυο είναι ιδεατό επειδή τα data μεταδίδονται μέσω μιας σήραγγας μέσω ενός δημόσιου δικτύου, όπως είναι το Διαδίκτυο, εξομοιώνοντας έτσι μία απ άκρη σε άκρη (point to point) σύνδεση. Το δίκτυο είναι ιδιωτικό επειδή η σήραγγα παρέχει εμπιστευτικότητα δεδομένων, ακεραιότητα, επικύρωση, έλεγχο πρόσβασης. Η έννοια ενός ασφαλούς μηχανισμού σηράγγων είναι απλή. Το ωφέλιμο φορτίο ενθυλακώνεται με μια νέα επικεφαλίδα (header) από το τελικό σημείο της σήραγγας όταν εισάγεται στη σήραγγα και αποθυλακώνεται όταν αφήνει τη σήραγγα. Από την προσθήκη της νέας επικεφαλίδας, το ωφέλιμο φορτίο μπορεί να κρυπτογραφηθεί και να επικυρωθεί. Επιπλέον, τα τελικά σημεία σηράγγων παρέχουν τον έλεγχο πρόσβασης. Οι σήραγγες VPN μπορούν να καθιερωθούν στα διαφορετικά ενδιάμεσα δίκτυα και πρωτόκολλα όπως το IP, το ATM (τρόπος ασύγχρονης μεταφοράς), το Frame Relay και το MPLS (Multi-protocol Label Switching). Περιορίζουμε

τη συζήτηση σε αυτό το κεφάλαιο στα βασισμένα στα IP- VPN που έχουν το Internet σαν υποδομή δημόσιου δικτύου.



Εικόνα 4

Τα VPN έχει διάφορα οφέλη στα ιδιωτικά δίκτυα τα οποία οφέλη είναι βασισμένα σε συγκεκριμένες συνδέσεις από σημείο σε σημείο (point-to-point).

Μείωση κόστους: Ίσως το μεγαλύτερο όφελος των VPN είναι η οικονομική αποτελεσματικότητά τους. Με ένα VPN, οι μισθωμένες γραμμές μεγάλης απόστασης μπορούν να αντικατασταθούν από μια σύντομη αφιερωμένη σύνδεση στο κοντινότερο σημείο της παρουσίας (point of presence, POP) του φορέα παροχής υπηρεσιών Διαδικτύου (isp). Με τον ίδιο τρόπο, οι μακρινοί χρήστες μπορούν να καλέσουν τον κοντινότερο isp κάνοντας μια τοπική κλήση σε αντιδιαστολή με την κλήση μεγάλης απόστασης. Επιπλέον, τα VPN μπορούν να μειώσουν τις δαπάνες εξοπλισμού, τις λειτουργικές δαπάνες και τις δαπάνες διοικητικής υποστήριξης.

Εξελιξιμότητα: Τα VPN μπορούν εύκολα να επεκτείνουν τη γεωγραφική προσιτότητα των δικτύων της επιχείρησης δεδομένου ότι οι νέες συνδέσεις μπορούν να προστεθούν εύκολα. Επιπλέον, η μόνιμη ή περιοδική συνδετικότητα μπορεί να παρέχεται κατόπιν παραγγελίας και χρήστες τρίτων όπως οι επιχειρησιακοί συνεργάτες μπορεί να ενσωματωθεί εύκολα.

Ευελιξία: Τα VPN προσφέρουν ευελιξία εξ αιτίας του ότι οι χρήστες σηράγγων δεν εγκλωβίζονται στη χρησιμοποίηση πολύ λίγου ή πάρα πολύ εύρους ζώνης. Οι νέες προστιθεμένης αξίας υπηρεσίες μπορούν να επεκταθούν εύκολα με VPN. Επιπλέον, οι σήραγγες VPN μπορούν να σχεδιαστούν για να παρέχουν ποικίλα επίπεδα ασφάλειας. Αυτό θα επιτρέψει στο χρήστη να προσαρμόσει τη σήραγγα για να εξασφαλίσει μια καλή ισορροπία μεταξύ της ασφάλειας και της απόδοσης για τις διαφορετικές εφαρμογές.

Εμπιστευτικότητα: Αυτή η απαίτηση συνεπάγεται την πρόληψη του κρυφακούσματος των δεδομένων σηράγγων καθώς ταξιδεύουν μέσω του Διαδικτύου. Ολοκληρώνεται με το ανακάτωμα των δεδομένων χρησιμοποιώντας τις μηχανές κρυπτογράφησης.

Ακεραιότητα: Ο στόχος είναι να εξασφαλιστεί ότι το λαμβανόμενα δεδομένα σηράγγων είναι ίδια με τα σταλμένα δεδομένα. Αυτό τυπικά επιτυγχάνεται με την χρήση των μονόδρομων? (one way) hash λειτουργιών οι οποίες δημιουργούν αφομοιώσεις μηνυμάτων.

Επικύρωση: Ο στόχος είναι να εξασφαλιστεί ότι οποιοδήποτε αίτημα για τη δημιουργία σηράγγων προέρχεται από έναν νόμιμο πελάτη. Επιπλέον, μόλις δημιουργηθεί η σήραγγα, ένας μηχανισμός πρέπει να οριστεί για να εξασφαλίσει ότι το στοιχείο έχει προέλθει από έναν

εξουσιοδοτημένο αποστολέα και δεν έχει τροποποιηθεί στη σήραγγα. Οι ψηφιακές υπογραφές χρησιμοποιούνται για να επιτύχουν αυτόν τον στόχο.

Πιστοποίηση: Ο στόχος είναι να καθιερωθεί η ταυτότητα των απ' άκρη σε άκρη οντοτήτων της σήραγγας προτού να ανταλλαχθούν τα κλειδιά. Αυτό γίνεται δυνατό με την χρήση των ψηφιακών πιστοποιητικών που εκδίδονται από έναν εμπιστευμένο τρίτο.

Έλεγχος πρόσβασης: Τα σημεία τέλους της σήραγγας πρέπει να περιορίσουν την πρόσβαση στους νόμιμους χρήστες. Αυτό εξασφαλίζεται από τις αντιπυρικές ζώνες ή άλλους μηχανισμούς φίλτρων στα σημεία τέλους σηράγγων.

Διαχείριση κλειδιών: Ο στόχος είναι να υπάρξει ένας αποδοτικός μηχανισμός από τον οποίο τα κλειδιά συζητιούνται και ανταλλάσσονται κατά τη διάρκεια μιας συνόδου. Αποδοτική διανομή και η διαχείριση των κλειδιών είναι κρίσιμες για τη επίτευξη άλλων στόχων ασφάλειας.

IP Security (IPsec)

Το πρωτόκολλο IPsec (Internet Protocol Security) ασχολείται με την ασφάλεια των επικοινωνιών σε επίπεδο δικτύου (network layer) και ειδικότερα στο πρωτόκολλο IP. Στην αρχή κάθε συνεδρίας επιτυγχάνεται αμοιβαία αυθεντικοποίηση μεταξύ των μερών και ανταλλαγής κρυπτογραφικών κλειδιών για να χρησιμοποιηθούν Το IPsec περιλαμβάνει επίσης και πρωτόκολλα για την επίτευξη αμοιβαίας αυθεντικοποίησης μεταξύ των επικοινωνούντων μερών στην αρχή κάθε συνεδρίας (session) και ανταλλαγής κρυπτογραφικών κλειδιών που θα χρησιμοποιηθούν σε αυτήν.. Το IPsec παρέχει ένα σχήμα ασφαλείας μεταξύ δύο υπολογιστών ή δύο πυλών δικτύου ή μεταξύ ενός υπολογιστή και μιας πύλης δικτύου.

Το IPsec παρέχει υπηρεσίες, όπως

- Εμπιστευτικότητα Δεδομένων (Data Confidentiality) – Ο IPsec αποστολέας μπορεί να κρυπτογραφήσει τα IP πακέτα πριν τα στείλει.
- Χωρίς Σύνδεση Ακεραιότητα Δεδομένων (Connectionless Data Integrity) – Ο IPsec παραλήπτης μπορεί να επικυρώσει ότι τα IP πακέτα που έλαβε, δεν έχουν αλλοιωθεί ή αλλαχθεί κατά την μετάδοση.
- Αυθεντικοποίηση Αποστολέα (Origin Authentication) – Ο IPsec παραλήπτης μπορεί να αυθεντικοποίησει την πηγή από την οποία εστάλησαν τα IP πακέτα. Προστασία απέναντι στην Επανάληψη (Antireplay) – Ο IPsec παραλήπτης μπορεί εντοπίσει και απορρίψει πακέτα που ήδη έχει λάβει.
- Έλεγχος Πρόσβασης Access Control) – Έλεγχος πρόσβασης χρηστών στα δεδομένα. Πλεονέκτημα του IPsec αποτελεί το γεγονός ότι οποιαδήποτε εγκατάσταση του αφορά αποκλειστικά το επίπεδο δικτύου και δεν επηρεάζει καθόλου τις ήδη εγκατεστημένες εφαρμογές του συστήματος. Οι νέες τεχνολογίες προφανώς αν μπορούν να καλύψουν ένα ευρύ πεδίο, δηλαδή έχουν μία διαλειτουργικότητα, επωφελούνται από αυτό. Είναι πολύ σημαντικό δηλαδή ένας IPsec συμβατός router μιας οποιαδήποτε εταιρείας να μπορεί να επικοινωνήσει με έναν άλλον IPsec συμβατό router μιας άλλης εταιρείας.Έτσι το IPsec είναι σχεδιασμένο για να είναι διαλειτουργικό.. Σωστή εφαρμογή του, δεν έχει επίδραση στα υπόλοιπα δίκτυα και υπολογιστές που δεν το υποστηρίζουν. Είναι ανεξάρτητο από τους τρέχοντες κρυπτογραφικούς αλγόριθμους και μπορεί να χρησιμοποιήσει καινούριους όταν γίνουν διαθέσιμοι. Η ομοιότητα των κρυπτογραφημένων πακέτων με τα κανονικά IP πακέτα, τα κάνει εύκολα στην δρομολόγηση μέσα από κάθε IP δίκτυοΟι συσκευές στα ακραία σημεία είναι οι μόνες οι οποίες γνωρίζουν για την κρυπτογράφηση, γεγονός πολύ σημαντικό για τη μείωση του κόστους υλοποίησης και διαχείρισης.

Το IPsec μπορεί να χρησιμοποιηθεί για την προστασία ενός ή περισσοτέρων καναλιών επικοινωνίας:

- Host-to-Host επικοινωνία (επικοινωνία μεταξύ δύο Πελατών).
- Gateway-to-Gateway επικοινωνία (επικοινωνία μεταξύ δύο Κόμβων).
- Host-to-Gateway επικοινωνία (επικοινωνία μεταξύ Πελάτη - Κόμβου).

Για να εξασφαλίζει την ασφαλή κίνηση σε ένα δίκτυο, το IPsec χρησιμοποιεί δυο πρωτόκολλα ασφαλούς μετάδοσης. Το πρωτόκολλο Επικεφαλίδας Πιστοποίησης (Authentication Header, AH) και το πρωτόκολλο Ασφαλούς Ενθυλάκωσης Πακέτου (Encapsulation Security Payload, ESP). Επίσης έχουμε τον ορισμό των παραμέτρων επικοινωνίας μεταξύ δύο συσκευών που είναι η Διαχείριση Κλειδιών (Key Management) και οι Συσχετίσεις Ασφαλείας (Security Associations, SA).

Ενώ η κάθε υλοποίηση IPsec πρέπει να περιέχει το ESP, για το AH δεν ισχύει το ίδιο (είναι προαιρετικό). Και τα δύο πρωτόκολλα μπορούν να χρησιμοποιηθούν μεμονωμένα ή σε συνδυασμό. Όμως το ESP διασφαλίζει όλες τις απαιτήσεις ασφαλείας, ενώ το AH παρέχει μόνο αυθεντικοποίηση, ακεραιότητα και αποφυγή επανάληψης πακέτου.

Μια πολύ βασική έννοια για το IPsec, όπως αναφέραμε, είναι οι Συσχετίσεις ή Συσχετισμοί Ασφαλείας (SA, RFC 2408). Ένας Συσχετισμός Ασφαλείας είναι μια συσχέτιση που υφίσταται σε πλήθος οντοτήτων που περιγράφει πώς οι οντότητες θα χρησιμοποιήσουν τις υπηρεσίες ασφαλείας για να επικοινωνήσουν. Για την ασφαλή επικοινωνία μεταξύ δύο συστημάτων απαιτούνται δύο διαφορετικές SAs, μια για κάθε διεύθυνση προορισμού (κατεύθυνση). Αυτό γιατί η SA είναι μια μονόδρομη σύνδεση και αποτελεί με λίγα λόγια σύνολο παραμέτρων που περιγράφουν πως μια επικοινωνία θα γίνει με ασφαλή τρόπο. Μια SA χαρακτηρίζεται από τρία μέρη:

Security Parameter Index (SPI): Δείκτης Παραμέτρων Ασφαλείας ονομάζεται ένας τυχαία επιλεγμένος αριθμός που αναγνωρίζει μοναδικά τη συσχέτιση ασφαλείας. Κατά την αποστολή (από ένα σύστημα) ενός πακέτου, το οποίο απαιτεί IPsec προστασία, αναζητά την SA στη βάση δεδομένων του, εφαρμόζει την συγκεκριμένη επεξεργασία και προσθέτει τον SPI στηνεπικεφαλίδα του IPsec. Όταν το αντίστοιχο μηχάνημα IPsec λάβει το πακέτο, αναζητά με τη σειρά του την SA της διεύθυνσης προορισμού και του SPI και κατόπιν ακολουθείται η επεξεργασία του πακέτου όπως ορίζεται.

IP Destination Address: Η IP διεύθυνση προορισμού του πακέτου.

Security Protocol: Δηλώνει ποιος θα είναι ο μηχανισμός που θα χρησιμοποιηθεί, δηλαδή αν θα είναι AH ή ESP. Η ακριβής λειτουργία και η συνεργασία των πρωτοκόλλων AH και ESP, καθορίζεται πάντα από τον χρήστη και τις εκάστοτε εφαρμογές του. Ο διαχειριστής του συστήματος έχει την ευχέρεια να διαλέξει για κάθε παρεχόμενη υπηρεσία, τα ακριβή πρωτόκολλα ασφαλείας, να ορίσει τους κρυπτογραφικούς αλγόριθμους και να επιλέξει τα κλειδιά. Γίνονται δηλαδή τοπικά. Υπάρχει όμως ανάγκη για κάποια χαρακτηριστικά να προτυποποιηθούν για λόγους διαλειτουργικότητας και καλύτερης διαχείρισης. Δημιουργούνται λοιπόν τρεις βάσεις δεδομένων:

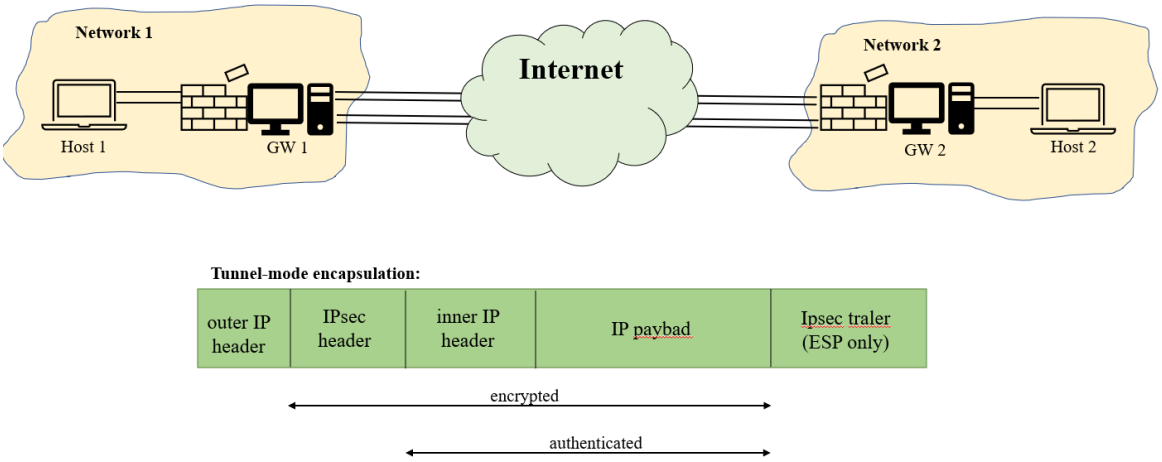
- Security Policy Database (SDP): Ορίζονται ποιες ακριβώς υπηρεσίες ασφαλείας θα παρέχονται σε κάθε IP πακέτο (RFC 4807, 4301).
- Security Association Database (SAD): Δίνει πληροφορίες για τα SA, όπως κρυπτογραφικούς αλγόριθμους και κλειδιά για τα AH και ESP, οι αριθμοί διαδοχής, η κατάσταση του πρωτοκόλλου και ο χρόνος διάρκειας μιας SA (RFC 4301).
- Peer Authorization Database (PAD): Παρέχει την κατάλληλη σύνδεση μεταξύ της SPD και ενός πρωτοκόλλου διαχείρισης SA, όπως το IKE. Περιλαμβάνει λειτουργίες όπως: Παρέχει δεδομένα αυθεντικοποίησης των peers, αναγνωρίζει το πρωτόκολλο αυθεντικοποίησης κάθε peer και διατηρεί την ταυτότητα των peers οι οποίοι είναι εξουσιοδοτημένοι να επικοινωνούν με την IPsec οντότητα (RFC 4301).

Το IPsec χρησιμοποιεί την SPD για να υλοποιήσει μια ή περισσότερες πολιτικές ασφαλείας. Όταν ένα πακέτο δημιουργείται ή λαμβάνεται μπορεί να διαχειριστεί βάση της SPD με έναν από τους 3 παρακάτω τρόπους:

- Protected – Οι υπηρεσίες ασφαλείας τους IPsec εφαρμόζονται σύμφωνα με την πολιτική ασφαλείας.
- Discarded – Πετάμε το πακέτο.
- Bypass – Το πακέτο περνάει χωρίς να εφαρμοστεί καμία υπηρεσία ασφάλειας.
- Tunnel mode και Transport mode

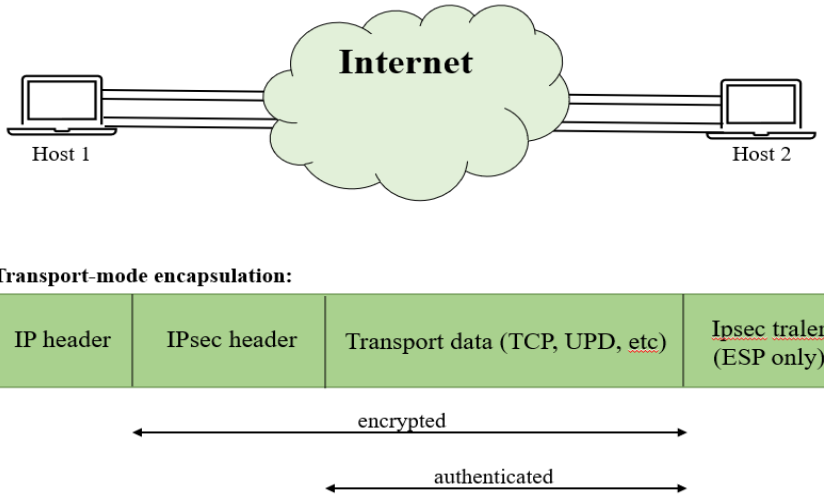
Το IPsec μπορεί να λειτουργήσει με δυο τρόπους:

Tunnel Mode: Όταν το ένα ή και τα δυο άκρα της σύνδεσης είναι ενδιάμεσοι κόμβοι. Η τεχνική του tunneling είναι μια κοινή τεχνική στα packet-switched δίκτυα και χρησιμοποιείται κυρίως σε επικοινωνία gateway-to-gateway ή hostto- gateway. Το σκεπτικό της υλοποίησης είναι η κάλυψη της IP πακέτου μέσα σε ένα άλλο. Αυτό σημαίνει ότι προσθέτει μια νέα επικεφαλίδα στο αρχικό πακέτο έτσι ώστε το αρχικό πακέτο να φαίνεται ως το φορτίου του νέου πακέτου. Όπως γίνεται αντιληπτό, απαιτείται επεξεργασία του πακέτου πριν την αποστολή και μετά τη λήψη. Ο προορισμός καθορίζεται από την καινούρια εξωτερική IP επικεφαλίδα, που περιέχει τη διεύθυνση του router ή ενός firewall. Το κόστος ς επεξεργασίας του πακέτου ισοζυγίζεται από την παραπάνω ασφάλεια (RFC 2709).



Εικόνα 5

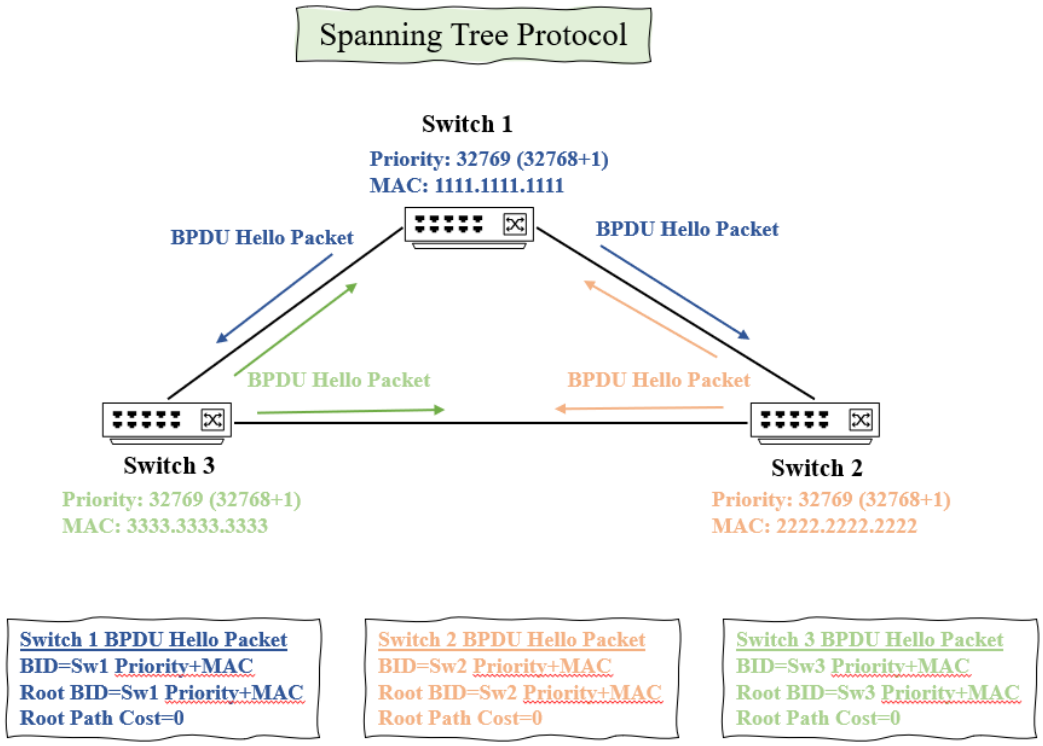
Transport Mode: Όταν και τα δυο άκρα της σύνδεσης είναι τερματικοί σταθμοί. Σε αυτή τη λειτουργία, μόνο στα δεδομένα του πακέτου (payload) εφαρμόζονται οι υπηρεσίες ασφαλείας του IPsec. Συνεπώς η επικεφαλίδα και οι πληροφορίες δρομολόγησης μένουν ανέπαφες. Η μέθοδος αυτή χρησιμοποιείται σε host-to-host επικοινωνία (RFC 3884).



Εικόνα 6

Spanning Tree Protocol

Οι βρόγχοι και τα διπλά πλαίσια μπορούν να έχουν αυστηρές συνέπειες σε ένα δίκτυο. Το πρωτόκολλο spanning-tree (STP) αναπτύχθηκε για να αντιμετωπίσει αυτά τα ζητήματα. Όταν υπάρχουν πολλά μονοπάτια μεταξύ δύο συσκευών στο δίκτυο και το STP έχει τεθεί εκτός λειτουργίας σε εκείνα τα switch , μπορεί να εμφανιστεί ένας Layer 2 βρόγχος (loop) . Εάν το STP ενεργοποιηθεί σε αυτά τα switch Layer 2 βρόγχος δεν θα εμφανιζόταν. Εξασφαλίζει λοιπόν ότι υπάρχει μόνο μια λογική πορεία μεταξύ όλων των προορισμών στο δίκτυο με την φραγή των εναλλακτικών μονοπατιών που θα μπορούσαν να προκαλέσουν έναν βρόχο.



Εικόνα 3

8.4 Παραδείγματα Ασφαλείας στα κατανεμημένα

8.4.1 Cluster Computing

Οι υπολογιστές που επικοινωνούν μέσω δικτύου υψηλής ταχύτητας μπορούν

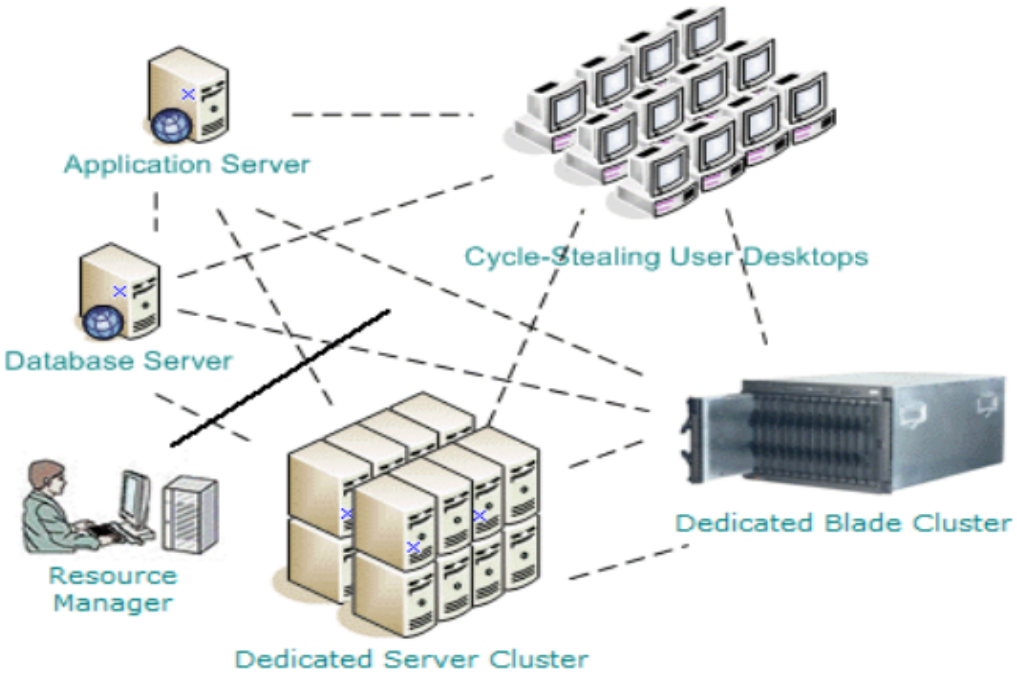
να λειτουργήσει και να παρουσιαστεί ως ένας ενιαίος υπολογιστής τους χρήστες. Ένα σύνολο υπολογιστών που είναι ομαδοποιημένοι σε με τέτοιο τρόπο ώστε να σχηματίζουν μια ενιαία δεξαμενή πόρων είναι ονομάζεται σύμπλεγμα. Κάθε εργασία που έχει ανατεθεί στο Το σύμπλεγμα θα εκτελείται σε όλους τους υπολογιστές του συμπλέγματος στο απαράλληλη μόδα σπάζοντας ολόκληρη την εργασία σε μικρότερο εαυτό περιείχε εργασίες. Στη συνέχεια, το αποτέλεσμα των μικρότερων εργασιών θα συνδυάζονται για να σχηματίσουν το τελικό αποτέλεσμα.

Το Cluster Computing βοηθά τους οργανισμούς να αυξήσουν την υπολογιστική τους ισχύ χρησιμοποιώντας το πρότυπο και συνήθως διαθέσιμη τεχνολογία. Αυτό το υλικό και λογισμικό που είναι συνήθως γνωστά ως εμπορεύματα μπορεί να είναι αγοράστηκε από την αγορά στο σχετικά χαμηλό κόστος. Τα συμπλέγματα χρησιμοποιούνται κυρίως για εκτέλεση επιστημονική, μηχανική, εμπορική και βιομηχανικές εφαρμογές που απαιτούν υψηλή διαθεσιμότητα και υψηλή απόδοση επεξεργασία.

Όταν τα υπολογιστικά συμπλέγματα διατίθενται στο δημόσιο ή τα δίκτυα ρυθμίζονται χρησιμοποιώντας δημόσιους πόρους όπως όπως το Διαδίκτυο, υπόκεινται σε διάφορα είδη επιθέσεις.Οι πιο συνηθισμένοι τύποι επιθέσεων στο Τα συμπλέγματα είναι κλοπή υπολογιστικού κύκλου, μεταξύ κόμβων κατασκοπεία επικοινωνίας και υπηρεσία συμπλέγματος αναστάτωση. Ως εκ τούτου, τα συμπλέγματα προστατεύονται από την ασφάλεια μηχανισμούς που περιλαμβάνουν υπηρεσίες όπως ο έλεγχος ταυτότητας, έλεγχος ακεραιότητας και εμπιστευτικότητας. Ο κύριος σκοπός των μηχανισμών ασφαλείας είναι να προστατεύστε το σύστημα από χάκερ καθώς και για την αντιμετώπιση των απαιτήσεις ασφαλείας των εφαρμογών.

8.4.2 Grid Computing

Το πλέγμα είναι ένας τύπος κατανεμημένου υπολογιστικού συστήματος όπου μεγάλος αριθμός μικρών υπολογιστών χαλαρά συζευγμένων είναι συγκεντρώθηκαν για να σχηματίσουν έναν μεγάλο εικονικό υπερυπολογιστή. Αυτό ο εικονικός υπερυπολογιστής πρέπει να εκτελεί εργασίες που είναι μεγάλες οποιονδήποτε υπολογιστή να λειτουργεί μέσα σε εύλογο χρονικό διάστημα. Το πλέγμα ορίζεται ως ένα παράλληλο και κατανεμημένο σύστημα δηλαδή δυνατότητα επιλογής, κοινής χρήσης και συγκέντρωσης γεωγραφικά κατανέμονται δυναμικά οι πόροι κατά το χρόνο εκτέλεσης με βάση τους διαθεσιμότητα, ικανότητα, απόδοση και κόστος που ανταποκρίνεται στους χρήστες Απαιτήσεις ποιότητας υπηρεσίας (QoS) .



Ασφάλεια υπολογιστικού πλέγματος

Τα συστήματα υπολογιστών πλέγματος παρέχουν αρκετές ασφάλεια μηχανισμών για την προστασία των πόρων του δικτύου από επιθέσεις. Το Middleware είναι ένα από τα κρίσιμα λογισμικά του συστήματος στο δίκτυο υποδομής καθώς παρέχει την κοινή επικοινωνία υποδομής και καθιστά διαθέσιμες τις υπηρεσίες δικτύου εφαρμογές. Το Middleware επιτρέπει επίσης μια ομοιόμορφη ασφάλεια διαμόρφωση σε επίπεδο κοντέινερ ή ανταλλαγής μηνυμάτων.

Ο έλεγχος ταυτότητας πλέγματος βασίζεται στην υποδομή δημόσιου κλειδιού

(PKI) και μπορεί να χειριστεί διαφορετικούς τύπους χρηστών διαπιστευτήρια όπως PKI, SAML, εισιτήρια Kerberos, κωδικός πρόσβασης, κ.λπ., η αντιπροσωπεία είναι ένας από τους απαραίτητους μηχανισμούς σε παροχή υπηρεσιών δικτύου και υλοποιείται με χρήση διακομιστή μεσολάβησης X.509 Πιστοποιητικό. Η εξουσιοδότηση για πρόσβαση σε πόρους του δικτύου βασίζεται σε χαρακτηριστικά εικονικού οργανισμού (VO) που έχουν εκχωρηθεί σε έναν χρήστη και διαχειρίζεται από την Υπηρεσία Μέλους Εικονικού Οργανισμού (VOMS). Η διαχείριση εμπιστοσύνης στα συστήματα πλέγματος γίνεται η χρήση πιστοποιητικών και οι σχέσεις εμπιστοσύνης αντιπροσωπεύονται από αλυσίδα πιστοποιητικών που περιλαμβάνει την Αρχή Πιστοποίησης Πλέγματος πιστοποιητικό (CA) και άλλα διαδοχικά δημιουργημένα πληρεξούσια

Η μονάδα ελέγχου ταυτότητας πλέγματος είναι μία από τις κρίσιμες στοιχεία για την αποτροπή εξωτερικών χρηστών από τυχαία πρόσβαση στο εσωτερικό δίκτυο και προστασία του συστήματος δικτύου από μη εξουσιοδοτημένους χρήστες. Αυτή η ενότητα χειρίζεται απειλές ασφαλείας από το εσωτερικό δίκτυο, όταν οι πιστοποιημένοι χρήστες του δικτύου πραγματοποιούν παράνομες (μη εξουσιοδοτημένες) λειτουργίες εντός του δικτύου.

Αυτοί οι μηχανισμοί ασφάλειας δικτύου εφαρμόζονται όλοι σχεδόν όλα τα συστήματα δικτύου που είναι διαθέσιμα σήμερα. Υπάρχουν πολλά πλέγματα κοινοτικές πρωτοβουλίες σε εξέλιξη στον τομέα του δικτύου διαλειτουργικότητα ενδιάμεσου λογισμικού που τελικά θα ενοποιούσε το ασφάλεια δικτύου ως ενιαία συνεκτική πλατφόρμα ασφαλείας και σχέδιο.

Αρχιτεκτονική Ασφάλειας Κατανεμημένου Συστήματος

Η Αρχιτεκτονική Ασφάλειας Κατανεμημένου Συστήματος ή (DSSA) είναι μια αρχιτεκτονική ασφάλειας υπολογιστή που παρέχει μια σειρά λειτουργιών, όπως σύνδεση, έλεγχος ταυτότητας και έλεγχος πρόσβασης σε ένα κατανεμημένο σύστημα. Για να διαφέρει από άλλες παρόμοιες αρχιτεκτονικές, η αρχιτεκτονική DSSA προσφέρει τη δυνατότητα πρόσβασης σε όλες αυτές τις λειτουργίες χωρίς να είναι ενεργός ο αξιόπιστος διακομιστής (γνωστός ως αρχή πιστοποιητικών).

Στο DSSA, τα αντικείμενα ασφαλείας διαχειρίζονται οι ιδιοκτήτες και η πρόσβαση ελέγχεται από την κεντρική, παγκοσμίως αξιόπιστη, αρχή έκδοσης πιστοποιητικών.

Το DSSA/SPX είναι το πρωτόκολλο ελέγχου ταυτότητας του DSSA. Το CDC είναι ένας διακομιστής χορήγησης πιστοποιητικών, ενώ το πιστοποιητικό είναι ένα δελτίο υπογεγραμμένο από την ΑΠ που περιέχει το δημόσιο κλειδί του μέρους που πιστοποιείται. Δεδομένου ότι το CDC διανέμει απλώς πιστοποιητικά που έχουν υπογραφεί προηγουμένως, δεν είναι απαραίτητο να είναι αξιόπιστο.

8.4.3 Κινητοί Πράκτορες

Τα παραδοσιακά κατανεμημένα συστήματα ήταν βασισμένα στις στατικές διεργασίες (processes) που εκτελούνταν στους μακρινούς κεντρικούς υπολογιστές και η επικοινωνία μεταξύ των κατανεμημένων αυτών συστημάτων γινόταν με σύγχρονες και ασύγχρονες κλήσεις π.χ. μακρινή κλήση προγράμματος (RPC). Εντούτοις, συχνές μακρινές κλήσεις αυξάνουν σημαντικά το κόστος του εύρους ζώνης. Η έννοια της μετανάστευση διεργασίας εισήγαγε την ιδέα της μεταφοράς μιας διεργασίας για εκτέλεση από τον έναν κεντρικό υπολογιστή στον άλλο στον άλλο, έτσι ώστε η τοπική εκτέλεση να μειώσει την ανάγκη για συχνές κλήσεις και μακρινή επικοινωνία. Αν και η μετανάστευση διεργασίας μειώνει πράγματι τις δαπάνες εύρους ζώνης, δεν επιτρέπει την επιστροφή των αποτελεσμάτων υπολογισμού στον αρχικό κεντρικό υπολογιστή, χωρίς την επιστροφή της ίδιας της διεργασίας. Η επιστροφή των αποτελεσμάτων έγινε δυνατή με την αρχή της μακρινής αξιολόγησης, όπου αντί της μεταφοράς μιας διεργασίας, επιτρέπεται η μετανάστευση ενός πλήρους προγράμματος. Μετά από τη μετανάστευση ενός τέτοιου προγράμματος, ο λαμβάνων κεντρικός υπολογιστής εκτελεί το πρόγραμμα και επιστρέφει τα αποτελέσματα.

Οι τεχνολογίες «κινητού κώδικα» και κινητών πρακτόρων επεκτείνουν τις αρχές της μακρινής αξιολόγησης που είναι βασισμένες σε αντικειμενοστραφείς τεχνικές προγραμματισμού, συμπεριλαμβάνοντας περισσότερη συμπεριφορά προγράμματος στο κινητό αντικείμενο. Ο κινητός κώδικας μπορεί να αυτό-μεταφέρεται σε μακρινούς κεντρικούς υπολογιστές (host), ενώ εμπεριέχει εκτελέσιμο κώδικα, data υπό την μορφή αντικειμένων και ενδεχομένως άλλα εμφωλευμένα αντικείμενα.

Υπάρχουν δύο οικογένειες των κινητών τεχνολογιών κώδικα, ισχυρές και αδύναμες κινητές τεχνολογίες. Οι αδύναμες κινητές τεχνολογίες παρέχουν τις υποδομές για απομακρυσμένη εκτέλεση κώδικα. Επιτρέπουν σε μια εφαρμογή να αποστείλει κώδικα σε μια μακρινή περιοχή προκειμένου η εκτέλεση του να πραγματοποιηθεί στον απομακρυσμένο κόμβο, επίσης μπορεί να συνδεθεί δυναμικά ο κώδικας που ανακτάται από μια απομακρυσμένη περιοχή για τοπική εκτέλεση. Ο κώδικας που μεταφέρεται ενδέχεται να συνοδεύεται από κάποια αρχικοποιημένα data, ενώ δεν μπορούν να μεταφερθούν πληροφορίες σχετικά με την εκτέλεση του κώδικα από τον πρώτο στο δεύτερο κόμβο. Παραδείγματα αδύναμων κινητών τεχνολογιών κώδικα περιλαμβάνουν Java applets, ActiveX controls, JavaScript και Aglets platform.

Οι κινητοί πράκτορες (mobile agents) είναι βασισμένοι στις ισχυρές κινητές τεχνολογίες. Αυτές οι τεχνολογίες επιτρέπουν σε μια μονάδα εκτέλεσης, ή σε ένα κινητό πράκτορα, που τρέχει σε ένα ιδιαίτερο κόμβο, να σταματήσει την εκτέλεσή της/ του, να μεταφέρει τον εαυτό

της/ του σε έναν μακρινό κεντρικό υπολογιστή και να συνεχίσει την εκτέλεση του εκεί. Οι κινητοί πράκτορες διαφέρουν από τον κινητό κώδικα σε αυτό το θέμα στο ότι εκτός από το στατικό μέρος, ο εκτελέσιμος κώδικας και τα data, φέρουν επίσης ένα δυναμικό μέρος, την κατάσταση εκτέλεσης όπως η κλήση του σωρού (call stack) και ο δείκτης εντολών (instruction pointer), κατά την διάρκεια της μετανάστευσης σε έναν άλλο κεντρικό υπολογιστή.

Γενικά, ένας πράκτορας είναι μια αυτόνομη οντότητα που εκτελεί μία ή περισσότερες εργασίες προκειμένου να επιτύχει κάποιους στόχους. Στον τομέα της δικτύωσης, ένας πράκτορας μπορεί να εκτελεστεί ακόμα και αν ο χρήστης αποσυνδεθεί από το δίκτυο. Μερικοί πράκτορες λειτουργούν σε αποκλειστικούς διακομιστές ενώ άλλοι εκτελούνται μέσα από τυπικές πλατφόρμες. Ένας πράκτορας επίσης μπορεί να οριστεί ως ένα ανεξάρτητο πρόγραμμα λογισμικού που εκτελείται για έναν χρήστη δικτύου.

Οι φορητοί πράκτορες προσθέτουν στους τακτικούς πράκτορες τη δυνατότητα να ταξιδεύουν σε πολλαπλές τοποθεσίες στο δίκτυο, αποθηκεύοντας την κατάστασή τους και επαναφέροντάς την σε ένα καινούργιο κόμβο. Καθώς ταξιδεύουν, εργάζονται για λογαριασμό των χρηστών, πραγματοποιώντας συλλογή πληροφοριών ή παράδοση αιτημάτων. Αυτή η κινητικότητα ενισχύει σημαντικά την παραγωγικότητα κάθε υπολογιστικού στοιχείου στο δίκτυο και δημιουργεί ένα ισχυρό υπολογιστικό περιβάλλον. Οι φορητοί πράκτορες απαιτούν μια υποδομή λογισμικού που τους παρέχει ασφάλεια και προστασία δεδομένων. Αυτή η υποδομή περιλαμβάνει πρωτόκολλα, κανόνες για ασφαλή κινητικότητα και οδηγίες και καταλόγους με πληροφορίες για όλους τους διαθέσιμους κόμβους.

Ειδικότερα, ένας κινητός πράκτορας (mobile host) που εκτελείται σε έναν κεντρικό υπολογιστή δικτύων μπορεί να πάψει την εκτέλεσή του, να μεταφέρει τον εαυτό του σε μια μορφή κατάλληλη για μετανάστευση (serialization) και να συνεχίσει την εκτέλεσή του μετά από τη μετανάστευση σε ένα άλλο κεντρικό υπολογιστή (host) . Από αυτήν την άποψη, οι κινητοί πράκτορες διαφέρουν από τον κινητό κώδικα στο ότι μπορούν να διατηρούν πληροφορίες κατάστασης κατά τη διάρκεια της μετανάστευσης από τον έναν host στον άλλο. Αυτό επιτρέπει αποτελεσματική χρήση των κατανεμημένων πόρων. Παραδείγματα κινητών τεχνολογιών πρακτόρων είναι οι G πλατφόρμες Grasshopper και Voyager .

Απειλές ασφάλειας της κινητής τεχνολογίας πρακτόρων

Αν και η τεχνολογία κινητών πρακτόρων επεκτείνει τις δυνατότητες των παραδοσιακών κατανεμημένων εφαρμογών δικτύων όπως το client-server model, υπάρχει μια αύξηση στις απαιτήσεις ασφάλειας. Τα κινητά συστήματα βασισμένα σε πράκτορες υπόκεινται σε διάφορες απειλές ασφάλειας. Πράγματι, δεδομένου ότι οι κινητοί πράκτορες μεταναστεύουν μέσω των ανοικτών και επισφαλών δικτύων και εκτελούνται σε υπολογιστές αβέβαιης εμπιστοσύνης, η ασφάλεια είναι μια σημαντική ανησυχία. Οι απειλές ασφάλειας μέσα τα κινητά συστήματα πρακτόρων μπορούν να διαιρεθούν σε τρεις κατηγορίες: απειλές κακόβουλων πρακτόρων, απειλές κακόβουλων hosts και απειλές κατά τη διάρκεια της μετανάστευσης.

Απειλές των κακόβουλων πρακτόρων: Ένας κακόβουλος, πλαστογραφημένος ή ελαττωματικός πράκτορας είναι μια πιθανή απειλή ασφάλειας για τους hosts μέσα στο δίκτυο. Τέτοιοι πράκτορες μπορούν να προσπαθήσουν να μιμηθούν ένα νόμιμο πράκτορα, προκειμένου να επιτευχθεί η αναρμόδια πρόσβαση σε έναν υπολογιστή (host). Μπορούν να κρυφακούσουν τον host εκτέλεσης, παραδείγματος χάριν μέσω ενός κρυμμένου τρωικού αλόγου (Trojan horse), προκειμένου να μεταφερθούν οι εμπιστευτικές πληροφορίες σε έναν άλλο υπολογιστή που ελέγχεται από τον επιτιθέμενο. Επιπλέον, μπορούν να προκαλέσουν επιθέσεις άρνησης ΥΠΗΡΕΣΙΩΝ (denial-of-service attacks) στο εκτελών υπολογιστή εάν οι κατάλληλες προφυλάξεις δεν λαμβάνονται, με κατανάλωση του εύρους ζώνης ή των πόρων

του host. Επίσης, μέρος του κώδικα εκτέλεσης του πράκτορα μπορεί να είναι καταστρεπτικός κώδικας, όπως κώδικας που περιέχει ιούς.

Απειλές των κακόβουλων hosts: Αφ' ετέρου, οι κινητοί πράκτορες είναι εξαιρετικά τρωτοί σε επιθέσεις από κακόβουλους hosts, δεδομένου ότι η εκτέλεση του πράκτορα στηρίζεται στον host. Δεδομένου ότι ο host έχει πρόσβαση στον κώδικα, τα data και στην κατάσταση ενός πράκτορα κατά την διάρκεια του χρόνου εκτέλεσης, ένας κακόβουλος host μπορεί να αλλάξει, να πειράξει ή να χειριστεί τον κώδικα, τα data και την κατάσταση toy πράκτορα. Παραδείγματος χάριν, ο host μπορεί να έχει πρόσβαση στις εμπιστευτικές πληροφορίες του πράκτορα, μπορεί να επισυνάψει τον κακόβουλο κώδικα ώστε να επιτεθούν άλλοι hosts μέσω του πράκτορα ή να καταστρέψουν απλά έναν πράκτορα έτσι ώστε ο αποστολέας του πράκτορα να χάσει όλα τα επιμέρους αποτελέσματα της εκτέλεσής του. Αυτή η κατηγορία απειλών θεωρείται δυσκολότερη να διαχειριστεί.

Απειλές κατά τη διάρκεια της μετανάστευσης: Αυτές οι απειλές συσχετίζονται με τις λογικές επιθέσεις σε κινητούς πράκτορες κατά τη διάρκεια της μετάδοσής τους από τον έναν host στον άλλο, όπως οι επιθέσεις man-in-the-middle. Για αυτόν τον λόγο μπορούν να θεωρηθούν ως ειδική περίπτωση των απειλών κακόβουλων hosts.

Μηχανισμοί ασφάλειας για τα κινητά συστήματα πρακτόρων και τις εφαρμογές δικτύων

Σε αυτό το τμήμα παρουσιάζουμε τους μηχανισμούς ασφάλειας και τις κρυπτογραφικές τεχνικές, που υιοθετούνται στις λύσεις που παρουσιάστηκαν στο προηγούμενο τμήμα προκειμένου να ασφαλιστούν τα πράκτορο-βασισμένα συστήματα. Οι μηχανισμοί ασφάλειας παρουσιάζονται σύμφωνα με τους στόχους ασφάλειας που καλύπτουν, δηλ. εμπιστευτικότητα, ακεραιότητα, επικύρωση, έγκριση και non-repudiation.

Όσον αφορά τις εφαρμογές δικτύων ένα πρότυπο ασφάλειας που εξετάζει απειλές στα έξυπνα δίκτυα στηρίζεται στις υπηρεσίες ασφάλειας CORBA και Grasshopper (η αρχιτεκτονική IN είναι βασισμένη στη grasshopper πλατφόρμα πρακτόρων), καθώς επίσης και σε μια υποδομή δημόσιων κλειδιών Public Key Infrastructure (PKI). Τεχνολογίες που αναλύονται στο επόμενο κεφάλαιο.

Μηχανισμοί για την εμπιστευτικότητα

Οι γνωστοί κρυπτογραφικοί μηχανισμοί που χρησιμοποιούνται για την ασφαλή επικοινωνία δικτύων μπορούν επίσης χρησιμοποιηθούν για να προστατεύσουν την εμπιστευτικότητα των κινητών πρακτόρων. Παραδείγματος χάριν, ο κώδικας, τα data και η κατάσταση ενός κινητού πράκτορα μπορούν να ενθυλακωθούν (κρυπτογραφηθούν) με συμμετρικό cipher, χρησιμοποιώντας ένα κλειδί κρυπτογράφησης κοινό μεταξύ του sender host και του receiver host. Κατά συνέπεια, μόνο οι "εμπιστευόμενοι" οικοδεσπότες που μοιράζονται το enciphering μπορούν να αποκρυπτογραφήσουν τον πράκτορα. Δεδομένου ότι αυτό δεν είναι πρακτικό για έναν μεγάλο αριθμό οικοδεσποτών, οι υβριδικοί μηχανισμοί κρυπτογράφησης είναι πιο κατάλληλοι, επειδή επιτρέπουν στους οικοδεσπότες να ανταλλάξουν ένα συμμετρικό κλειδί κρυπτογράφησης μέσω της κρυπτογράφησης του δημόσιου-κλειδιού. Σημειώστε ότι αυτή η μέθοδος κρυπτογράφησης εφαρμόζεται από την σουίτα SSL/ TLS, η οποία χρησιμοποιείται συνήθως στις κινητές πλατφόρμες πρακτόρων για κρυπτογράφηση.

Εντούτοις, η τύπου SSL προσέγγιση προστατεύει τους κινητούς πράκτορες μόνο κατά τη διάρκεια της μετανάστευσης. Σημειώστε ότι σε μερικές περιπτώσεις μέρος των data που ένας πράκτορας μεταφέρει, πρέπει να προστατευθούν από άλλους ενδιάμεσους οικοδεσπότες εκτέλεσης, παραδείγματος χάριν όταν ένας πράκτορας συλλέγει επί μέρους αποτελέσματα εκτέλεσης από τους οικοδεσπότες που πρέπει να παραμείνουν μυστικοί από τους άλλους

οικοδεσπότες εκτέλεσης. Σε αυτές τις περιπτώσεις η κρυπτογράφηση «ολίσθησης» μπορεί να χρησιμοποιηθεί. Η κρυπτογράφηση ολίσθησης είναι ιδιαίτερα κατάλληλη σε περιπτώσεις όταν τα data που συλλέγονται από τον κινητό πράκτορα είναι σχετικά μικρά σε σύγκριση με μέγεθος των κλειδιών κρυπτογράφησης ή με το μέγεθος του τελικού κρυπτογραφήματος. Επιτρέπει σε μικρά κομμάτια δεδομένων να κρυπτογραφηθούν αποτελεσματικά. Ο πράκτορας χρησιμοποιεί ένα δημόσιο κλειδί κρυπτογράφησης του ιδιοκτήτη του, για να κρυπτογραφηθούν οι πληροφορίες που συγκεντρώνονται σε κάθε οικοδεσπότη. Κατόπιν, όταν επιστρέφει ο πράκτορας στην αφετηρία του, ο ιδιοκτήτης του πράκτορα αποκρυπτογραφεί τα data με το μυστικό κλειδί κρυπτογράφησης. Σημειώστε ότι η κρυπτογράφηση δημοσίου κλειδιού (public key) μπορεί επίσης να χρησιμοποιηθεί για μεγαλύτερα ποσά δεδομένων.

Μηχανισμοί για την ακεραιότητα, την επικύρωση και τη μη αποποίηση

Η επικύρωση ακεραιότητας προέλευσης και data integrity ενός κινητού πράκτορα μπορεί να επιτευχθεί με τους γνωστούς κρυπτογραφικούς μηχανισμούς όπως οι κώδικες επικύρωσης μηνυμάτων Message Authentication Codes (MACs). Πριν από τη μετανάστευση του πράκτορα, ο οικοδεσπότης που στέλνεται μπορεί να περιλάβει στην ενθυλάκωση του πράκτορα, την MAC που παράγεται με μια κρυπτογραφική hash συνάρτηση και ένα κλειδί επικύρωσης. Πάλι, το κλειδί επικύρωσης μπορεί είτε να μοιραστεί μεταξύ των οικοδεσποτών είτε να ανταλλαχθεί μεταξύ τους. Σημειώστε ότι αφού μετά από την εκτέλεση του πράκτορα σε έναν οικοδεσπότη η κατάσταση του πράκτορα αλλάζει, η MAC του πράκτορα πρέπει επίσης να επαν-υπολογιστεί από τον οικοδεσπότη. Κατά συνέπεια, η ακεραιότητα του δυναμικού μέρους του πράκτορα στηρίζεται σε μεγάλο ποσοστό στην εμπιστοσύνη των ενδιάμεσων οικοδεσποτών.

Το ίδιο πράγμα μπορεί να επιτευχθεί μέσω των συνηθισμένων ψηφιακών υπογραφών. Το στατικό μέρος του πράκτορα, ο εκτελέσιμος κώδικας και τα αρχικά data, μπορούν να είναι υπογεγραμμένα από τον δημιουργό του πράκτορα ή εκκινητή του πράκτορα Ο υπογεγραμμένος κώδικας βεβαιώνει την ακεραιότητα του πράκτορα, τουλάχιστον για το στατικό μέρος του πράκτορα. Κάθε ενδιάμεσος οικοδεσπότης μπορεί έπειτα ψηφιακά να υπογράψει το δυναμικό μέρος του πράκτορα μετά την μερική εκτέλεσή του στον οικοδεσπότη. Σημειώστε ότι με ψηφιακές υπογραφές επιτυγχάνεται επίσης non-repudiation του αποστέλλοντος οικοδεσπότη, δεδομένου ότι ένας αποστέλλων οικοδεσπότης δεν μπορεί να αρνηθεί τη μερική εκτέλεση του πράκτορα. Εντούτοις, με τις συνηθισμένες ψηφιακές υπογραφές η ακεραιότητα του δυναμικού μέρους του πράκτορα στηρίζεται ακόμα στην εμπιστοσύνη των ενδιάμεσων οικοδεσποτών, όπως συνέβαινε και με η χρήση MACs. Επίσης, για την πιστοποίηση των χρησιμοποιούμενων κλειδιών υπογραφών και επαλήθευσης, είναι απαραίτητος να χρησιμοποιηθεί μια υποδομή δημόσιων κλειδιών και ψηφιακών πιστοποιητικών. Το κλειδί επαλήθευσης κάθε οντότητας, του δημιουργού πρακτόρων, του αρχικού πράκτορα ή του ενδιάμεσου οικοδεσπότη πρέπει να πιστοποιείται μέσω ενός πιστοποιητικού δημοσίων κλειδιών, που εκδίδεται από μια πιστοποιούσα αρχή. Για non-repudiation πρακτόρων, είναι δυνατό να χρησιμοποιηθούν τα σχέδια που είναι συγκεκριμένα για υπογραφές πρακτόρων που παρουσιάστηκαν ανωτέρω, όπως οι undetachable υπογραφές, οι proxy υπογραφές – οι one-time ή μη-οριζόμενες (non-designated) υπογραφές, οι undetachable υπογραφές κατωφλίου ή οι δυναμικές multisignatures. Μερικά από αυτά τα σχέδια παρέχουν επίσης non-repudiation οικοδεσποτών, όπως η μη-οριζόμενη proxy υπογραφή και οι δυναμικές multi-signatures.

Μηχανισμοί για την έγκριση

Αν και γενικά γνωστοί μηχανισμοί έγκρισης μπορούν να χρησιμοποιηθούν για την έγκριση ενός πράκτορα, όπως λίστες ελέγχου πρόσβασης και γλώσσες πολιτικής, αρκετά πρακτορο-συγκεκριμένα πρότυπα έγκρισης έχουν προταθεί. Πρακτορο-συγκεκριμένοι (Agent specific) μηχανισμοί έγκρισης έχουν προταθεί επίσης. Η αξιολόγηση πολιτείας (State appraisal) είναι ένας τέτοιος μηχανισμός που ελέγχει την κατάσταση ενός πράκτορα πριν του χορηγηθούν οποιαδήποτε προνόμια. Η State appraisal εξετάζει τους πράκτορες προκειμένου να ανιχνευθούν οι πιθανές κακόβουλες αλλαγές στην κατάσταση ενός πράκτορα. Σε

περίπτωση θεωρούμενων μεγάλης κλίμακας αλλαγών, κανένα προνόμιο δεν χορηγείται πουθενά, ενώ μικρές αλλαγές μπορούν να επιτρέψουν περιορισμένα προνόμια στον πράκτορα. Οι λειτουργίες της state appraisal είναι βασισμένες στους παράγοντες που εξαρτώνται από την τρέχουσα κατάσταση του πράκτορα, καθώς επίσης και στις σταθερές τιμές του πράκτορα. Αυτές οι λειτουργίες είναι μέρος του πράκτορα και μπορούν να δημιουργηθούν είτε από το δημιουργό του πράκτορα είτε από τον ιδιοκτήτη του πράκτορα. Αν και αυτός ο μηχανισμός μπορεί να αποτρέψει γνωστές επιθέσεις, αυτό δεν είναι αποτελεσματικό για επιθέσεις που δεν έχουν εξεταστεί. Εν τούτοις, η χρήση της μπορεί να υποστηρίξει την έγκριση καθώς επίσης και τους ελέγχους ακεραιότητας σε ένα σύστημα.

Ένας άλλος μηχανισμός ασφάλειας που είναι κατάλληλος για έγκριση πρακτόρων είναι τα πιστοποιητικά ιδιοτήτων. Ένα πιστοποιητικό ιδιοτήτων μπορεί να περιέχει ιδιότητες όπως προνόμια πρόσβασης που χορηγούνται σε ιδιαίτερες οντότητες. Κατόπιν, ο ιδιοκτήτης του πιστοποιητικού ιδιοτήτων μπορεί να εξουσιοδοτήσει αυτό το πιστοποιητικό σε έναν πράκτορα, προκειμένου οι ιδιότητες (προνόμια) που περιέχονται στο πιστοποιητικό να εξουσιοδοτηθούν στον πράκτορα. Ο εξουσιοδοτημένος πράκτορας είναι σε θέση να εκτελεστεί σε έναν οικοδεσπότη με τα προνόμια πρόσβασης του ιδιοκτήτη του. Σημειώστε ότι τα πιστοποιητικά ιδιοτήτων μπορεί επίσης να εκδοθούν για τους οικοδεσπότες εκτέλεσης. Ένα πιστοποιητικό ιδιότητας οικοδεσπότη μπορεί να καθορίσει την πολιτική πρόσβασης ενός οικοδεσπότη, δηλ. τα μέγιστα προνόμια που θα δοθούν σε έναν ιδιαίτερο οικοδεσπότη, σε οποιοδήποτε πράκτορα που θα εκτελεσθεί σε εκείνο τον οικοδεσπότη. Κατόπιν, το πιστοποιητικό ιδιότητας πράκτορα μπορεί περαιτέρω να καθορίσει τους κανόνες πολιτικής για να καλυτερεύσει την πολιτική πρόσβασης. Σημειώστε ότι η χρήση των πιστοποιητικών ιδιοτήτων στηρίζεται επίσης σε μια υποδομή δημόσιων κλειδιών που εκδίδει ή ανακαλεί τα πιστοποιητικά ιδιοτήτων. Το σχήμα 4 συνοψίζει τους μηχανισμούς ασφαλείας για τα κινητά συστήματα πρακτόρων και τους στόχους ασφάλειας που αυτά ικανοποιούν.

Προαπαιτούμενη Γνώση

1) Πρακτικά Θέματα Ασφάλειας Πληροφοριακών Συστημάτων & Εφαρμογών, Νινέτα Πολέμη, Αλέξανδρος Καλιοντζόγλου
2) Andrew S. Tanenbaum, Maarten Van Steen (2006), Κατανεμημένα Συστήματα: Αρχές και Υποδείγματα, Έκδοση: 1η/2006, Εκδόσεις Κλειδάριθμος.
3) Coulouris, J. Dollimore, T. Kindberg, G. Blair (2020), Κατανεμημένα Συστήματα, Έκδοση: 2η, Da Vinci Μ.Ε.Π.Ε.

Βιβλιογραφικές αναφορές

[1] Ασφάλεια Υπολογιστών: Αρχές και Πρακτικές, William Stallings, Lawrie Brown

[2] Κρυπτογραφία για Ασφάλεια Δικτύων Αρχές και Εφαρμογές, William Stallings

[3] Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο, Σωκράτης Κάτσικας, Στέφανος Γκρίτζαλης, Κωνσταντίνος Λαμπρινουδάκης

[4] Παναπαναγιώτου, Κ. (2008, Ιούνιος 16). OWASP: Ασφάλεια στις Web εφαρμογές. *Linux Format* , σσ. 56-58.

[5] Ασφάλεια Δικτύων Υπολογιστών, Γκρίτζαλης Στέφανος, Γκρίτζαλης Δημήτρης Α., Κάτσικας Σωκράτη

[6] Panayiotis Kotzanikolaou. "Appendix A: Cryptography Primer: Introduction to Cryptographic Principles and Algorithms" , Network Security, 06/06/2007

[7] Ram Sewak Singh, Demissie Jobir Gelmecha, Tadesse Hailu Ayane, Devendra Kumar Sinha. "Functional framework for IoT-based agricultural system" , Elsevier BV, 2022

[8] Network Providers' Resilience Measures, The ENISA Virtual Working Group, Charalampos Koutsouris, Louis Marinos, ENISA Quarterly Review Vol. 5, No. 4 (December 2009)

[9] JavaDude. Ανάκτηση από Getting started with Glassfish V3 and SSL: http://javadude.wordpress.com/2010/04/06/getting-started-with-glassfish-v3-and-ssl/

[10] International Organization for Standardization (ISO). (1996). Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model. *International Standard ISO/IEC 7498-1*, σ. 59. Ανακτήθηκε από http://standards.iso.org/ittf/PubliclyAvailableStandards/s025022_ISO_IEC_7498-3_1997(E).zip

Κριτήρια αξιολόγησης

Ερώτηση 1

Ποιος από τους παρακάτω αλγορίθμους λειτουργεί για RSA κλειδί;

A.

■ Διαλέξτε δυο μεγάλους πρώτους p, q ίσους περίπου στο μήκος και υπολογίστε n= p / q. Οι δυο πρώτοι διατηρούνται μυστικοί.

■ Διαλέξτε έναν τυχαίο αριθμό e έτσι ώστε e και (p - 1)(q-1) είναι σχετικά πρώτοι, πράγμα που σημαίνει ότι ο μεγαλύτερος κοινός διαιρέτης του e και (p + 1)(q +1) ισούται με 1. Το αποτέλεσμα (p + 1)(q + 1)= φ(n) είναι η λειτουργία Euler phi.

■ Υπολογίστε d έτσι ώστε e χ d = 1 mod(p + 1)(q + 1) = 1 mod φ(n). Έτσι, d είναι η αναστροφή του e mod φ (n).

■ Το γνωστό κλειδί κρυπτογράφησης είναι (e,n) και το μυστικό κλειδί αποκρυπτογράφησης είναι (d,n)

B.

■ κλειδί κρυπτογράφησης είναι (e,n) και το μυστικό κλειδί αποκρυπτογράφησης Διαλέξτε δυο μεγάλους πρώτους p,q ίσους περίπου στο μήκος και υπολογίστε n= p mod q. Οι δυο πρώτοι διατηρούνται μυστικοί.

■ Διαλέξτε έναν τυχαίο αριθμό e έτσι ώστε e και (p * 1)(q*1) είναι σχετικά πρώτοι, πράγμα που σημαίνει ότι ο μεγαλύτερος κοινός διαιρέτης του e και (p * 1)(q*1) ισούται με 1. Το αποτέλεσμα (p * 1)(q* 1)= φ(n) είναι η λειτουργία Euler phi.

■ Υπολογίστε d έτσι ώστε e χ d = 1 mod(p * 1)(q * 1) = 1 mod φ(n). Έτσι, d είναι η αναστροφή του e mod φ (n).

■ Το γνωστό είναι (d,n)

Γ.

■ Διαλέξτε δυο μεγάλους πρώτους p,q ίσους περίπου στο μήκος και υπολογίστε n= p χ q. Οι δυο πρώτοι διατηρούνται μυστικοί.

■ Διαλέξτε έναν τυχαίο αριθμό e έτσι ώστε e και (p - 1)(q-1) είναι σχετικά πρώτοι, πράγμα που σημαίνει ότι ο μεγαλύτερος κοινός διαιρέτης του e και (p - 1)(q-1) ισούται με 1. Το αποτέλεσμα (p - 1)(q- 1)= φ(n) είναι η λειτουργία Euler phi.

■ Υπολογίστε d έτσι ώστε e χ d = 1 mod(p - 1)(q - 1) = 1 mod φ(n). Έτσι, d είναι η αναστροφή του e mod φ (n).

■ Το γνωστό κλειδί κρυπτογράφησης είναι (e,n) και το μυστικό κλειδί αποκρυπτογράφησης είναι (d,n)

Δ. Όλοι οι παραπάνω

Ερώτηση 2

Σύμφωνα με τα πρότυπα ISO/IEC 7498-1, ποια είναι τα λειτουργικά πλάνα που αποτελείται κάθε στρώμα πρωτοκόλλου;

Α. φορείς, έλεγχος και δεικτοδότηση

Β. χρήστες, σηματοδότηση, έλεγχος, και διαχείριση

Γ. σηματοδότηση, διαχείριση, ταχύτητα σύνδεσης στο δίκτυο

Δ. Χρήστες και Έλεγχος.

Ερώτηση 3

Ποια από τα παρακάτω αποτελούν οφέλη των VPN στα ιδιωτικά δίκτυα τα οποία είναι βασισμένα σε συγκεκριμένες συνδέσεις από σημείο σε σημείο (point-to-point);

Α. Μείωση κόστους, Εξελιξιμότητα, Ευελιξία

Β. Εμπιστευτικότητα, Ακεραιότητα, Επικύρωση

Γ. Πιστοποίηση, Έλεγχος πρόσβασης, Διαχείριση κλειδιών

Δ. Όλα τα παραπάνω

Ερώτηση 4

Ποιες είναι οι συνέπειες της πλαστογράφησης των πληροφοριών δρομολόγησης;

Α. Επαναπροσανατολίζει την κυκλοφορία για να δημιουργήσει βρόχους δρομολόγησης

Β. Επαναπροσανατολίζει την κυκλοφορία που μπορεί να ελεγχθεί σε μια επισφαλή σύνδεση

Γ. Επαναπροσανατολίζει την κυκλοφορία για να την απορρίψει

Δ. Όλα τα παραπάνω

Ερώτηση 5

Ποια τα πλεονεκτήματα των κρυπτογραφικών συστημάτων συμμετρικού κλειδιού;

Α. Αποτελεσματικότητα, μικρό μέγεθος κλειδιού

Β. Πιστοποίηση, Έλεγχος πρόσβασης, Διαχείριση κλειδιών

Γ. προσδιορισμός φορέων, έλεγχος και δεικτοδότηση

Δ. Όλα τα παραπάνω

Ερώτηση 6

Ποιο από τα παρακάτω εκτελεί κώδικα και εγκαθιστά τα αντίγραφα του στη μνήμη του μολυσμένου υπολογιστή, ο οποίος μπορεί, στη συνέχεια, να μολύνει άλλους υπολογιστές;

Α. Worms

Β. Viruses

Γ. Trojan Horse

Δ. Όλα τα παραπάνω

Ερώτηση 7

Ποια από τα παρακάτω αποτελεί μειονεκτήματα των Κρυπτογραφικών Συστημάτων Γνωστού Κλειδιού;

Α. Η κρυπτογράφηση γνωστού κλειδιού είναι αισθητά πιο αργή από τη συμμετρική κρυπτογράφηση.

Β. Ευάλωτο σε επιθέσεις τύπου

Γ. Ότι είναι γνωστά.

Δ. Όλα τα παραπάνω

Ερώτηση 8

Το IPsec χρησιμοποιεί την SPD για να υλοποιήσει μια ή περισσότερες πολιτικές ασφαλείας. Όταν ένα πακέτο δημιουργείται ή λαμβάνεται βάσει της SPD ποιον από τους παρακάτω τρόπους επιλέγει;

Α. Protected – Οι υπηρεσίες ασφαλείας τους IPsec εφαρμόζονται σύμφωνα με την πολιτική ασφαλείας.

Β. Discarded – Πετάμε το πακέτο.

Γ. Bypass – Το πακέτο περνάει χωρίς να εφαρμοστεί καμία υπηρεσία ασφάλειας.

Δ. Έναν εκ των τριών παραπάνω ανάλογα τις συνθηκες

Ερώτηση 9

Με ποιους δύο τρόπους λειτουργεί το IPsec;

Α. Gateway, Gateway

Β. Tunnel Mode, Transport mode

Γ. Security Mode, Cryptography Mode

Δ. Όλους τους παραπάνω

Ερώτηση 10

Ποιο από τα παρακάτω αποτελεί άμυνα κακόβουλων επιθέσεων;

Α. VPN

Β. IDS

Γ. IPS

Δ. Όλα τα παραπάνω

Ερώτηση 11

Τι είναι το Intrusion Prevention System (IPS);

Α. Είναι μια λύση softarwe ή hardware–based που ακούει παθητικά την κυκλοφορία των δικτύων.

Β. firewall που επιβάλλουν το έλεγχο προσπέλασης μεταξύ δικτύων, τα οποία μπορούν να είναι διαφορετικών τύπων και επιπέδων εμπιστοσύνης

Γ. Είναι μια ενεργός συσκευή στην πορεία της κυκλοφορίας που «ακούει» την κυκλοφορία και επιτρέπει ή αρνείται τις ροές των πακέτων στο δίκτυο.

Δ. Τίποτα από τα παραπάνω

Ερώτηση 12

Τι είναι το Trojan Horse;

Α. Είναι μια ενεργός συσκευή στην πορεία της κυκλοφορίας που «ακούει» την κυκλοφορία και επιτρέπει ή αρνείται τις ροές των πακέτων στο δίκτυο.

Β. Είναι μία επίθεση η οποία δεν διαφέρει από ένα worm ή έναν virus.

Γ. Είναι μια εφαρμογή λογισμικού που τρέχει ένα απλό παιχνίδι σε έναν τερματικό σταθμό. Ενώ ο χρήστης απασχολείται με το παιχνίδι, η εφαρμογή ταχυδρομεί ένα αντίγραφο του σε κάθε διεύθυνση στο βιβλίο διευθύνσεων του χρήστη. Οι άλλοι χρήστες λαμβάνουν το παιχνίδι και το παίζουν, με αυτόν τον τρόπο διαδίδοντας τον Trojan Horse στις διευθύνσεις σε κάθε βιβλίο διευθύνσεων.

Δ. Όλα τα παραπάνω

Ερώτηση 13

Τι είναι το SHH?

Α. Ότι και το Telnet

Β. Ότι και το CDP

Γ. SSH είναι ένα πρωτόκολλο client - server που χρησιμοποιείται για να συνδεθεί κάποιος σε μια άλλη συσκευή σε ένα δίκτυο, να εκτελέσει εντολές σε μια μακρινή συσκευή που δεν είναι άμεσα συνδεδεμένος και να μετακινήσει αρχεία.

Δ. Όλα τα παραπάνω

Ερώτηση 14

Ποιο από τα παρακάτω αποτελεί όφελος του VPN;

Α Μείωση κόστους και Εξελιξιμότητα

Β. Μικρότερη φθορά του Υλικού του Η/Υ

Γ. Ταχύτερη εκτέλεση των αλγορίθμων

Δ. Όλα τα παραπάνω

Ερώτηση 15

Τι από τα παρακάτω ισχύει για το Spanning Tree Protocol;

Α. Οι βρόχοι και τα διπλά πλαίσια μπορούν να έχουν αυστηρές συνέπειες σε ένα δίκτυο. Το πρωτόκολλο spanning-tree (STP) αναπτύχθηκε για να αντιμετωπίσει αυτά τα ζητήματα

Β. Όταν υπάρχουν πολλά μονοπάτια μεταξύ δύο συσκευών στο δίκτυο και το STP έχει τεθεί εκτός λειτουργίας σε εκείνα τα switch , μπορεί να εμφανιστεί ένας Layer 2 βρόγχος (loop) . Εάν το STP ενεργοποιηθεί σε αυτά τα switch Layer 2 βρόγχος δεν θα εμφανιζόταν.

Γ. Εξασφαλίζει ότι υπάρχει μόνο μια λογική πορεία μεταξύ όλων των προορισμών στο δίκτυο με το να μπλοκάρει τα εναλλακτικά μονοπάτια που θα μπορούσαν να προκαλέσουν έναν βρόχο. Μία πόρτα θεωρείται μπλοκαρισμένη όταν η κυκλοφορία του δικτύου αποτρέπεται από να τα εισέλθει ή να εξέλθει από αυτή την πόρτα. Αυτό δεν περιλαμβάνει τα bridge protocol data unit (BPDU) πακέτα που χρησιμοποιούνται από το STP για να αποτρέψουν τους βρόχους

Δ. Όλα τα παραπάνω