Πληροφοριακά Συστήματα

Διάλεξη 11 (4 Ιουνίου 2024)

Διονύσης Μάργαρης
Επίκουρος Καθηγητής ΤΨΣ ΠΑΠΕΛ

Τι θα συζητήσουμε σήμερα;

Εισαγωγή στην Ασφάλεια των ΠΣ

Βασικοί ορισμοί (1/4)

Με τον όρο «ασφάλεια πληροφοριακών συστημάτων» εννοούμε την προστασία πόρων (δεδομένων και προγραμμάτων) από συμπτωματική ή κακόβουλη τροποποίηση, καταστροφή ή διαρροή.

Βασικοί ορισμοί (2/4)

Έννοια	Ορισμός
Αγαθό	Ο όρος αυτός περιλαμβάνει οτιδήποτε χρήζει προστασίας, είτε πρόκειται για υλικό (υπολογιστής, καλώδιο επικοινωνίας) είτε άυλο (π.χ. δεδομένα, υπηρεσία).
Ιδιοκτήτης	Το φυσικό ή νομικό πρόσωπο που κατέχει το αγαθό
Εξουσιοδότηση	Η παροχή από τον ιδιοκτήτη δικαιώματος χρήσης πάνω σε ένα συγκεκριμένο αγαθό. Η εξουσιοδότηση μπορεί να παρέχεται είτε σε κάποιο φυσικό πρόσωπο είτε σε κάποια διαδικασία (π.χ. η διαδικασία τήρησης εφεδρικών αντιγράφων)
Χρήστης	Ονομάζεται το φυσικό ή νομικό πρόσωπο ή η διαδικασία που χρησιμοποιεί ένα συγκεκριμένο αγαθό. Ένας χρήστης μπορεί να είναι εξουσιοδοτημένος, να χρησιμοποιεί δηλαδή το αγαθό κατόπιν εξουσιοδότησης του ιδιοκτήτη, ή όχι.
Αξία	Πρόκειται για ένα μέτρο έκφρασης της σπουδαιότητας του αγαθού. Η αξία μπορεί να εκφράζεται ως οικονομικό μέγεθος ή με οποιοδήποτε άλλο πρόσφορο τρόπο.
Ζημιά	Η υποβάθμιση της αξίας ενός αγαθού.

Βασικοί ορισμοί (3/4)

Έννοια	Ορισμός
Επίπτωση	Οι συνέπειες που μπορεί να έχει μία ζημιά σε ένα αγαθό. Οι επιπτώσεις μπορεί να είναι οικονομικές ή και άλλης φύσεως, π.χ. αρνητική δημοσιότητα.
Κίνδυνος	Η πιθανότητα να υποστεί ζημιά κάποιο αγαθό
Παραβίαση	Ένα συμβάν κατά το οποίο κάποιο αγαθό υπόκειται ζημιά
Αδυναμία	Ένα χαρακτηριστικό το συστήματος που είναι δυνατόν να επιτρέψει την εμφάνιση κάποιας παραβίασης
Απειλή	Ένας παράγοντας που μπορεί να προξενήσει ζημιά σε ένα αγαθό. Μία *απειλή* μπορεί να αξιοποιήσει μία *αδυναμία* οδηγώντας σε κάποια *παραβίαση*.
Μέσο προστασίας	Οι ενέργειες που γίνονται και οι μηχανισμοί που χρησιμοποιούνται από τον ιδιοκτήτη προκειμένου να περιορισθούν οι κίνδυνοι για τα αγαθά.

Βασικοί ορισμοί (4/4)

Έννοια	Ορισμός
Πρόληψη	Η διαδικασία εφαρμογής μέσων προστασίας με στόχο την παρεμπόδιση της εμφάνισης παραβιάσεων
Ανίχνευση	Ο εντοπισμός παραβιάσεων και των επιπτώσεών τους
Επανόρθωση	Η αποκατάσταση των επιπτώσεων μιας παραβίασης
Κόστος μέτρου	Το αντίκτυπο που έχει η χρήση ενός μέσου προστασίας. Μπορεί να είναι οικονομικό, συστημικό (π.χ. Υποβάθμιση της απόδοσης του συστήματος), ψυχολογικό (π.χ. δυσαρέσκεια από τη χρήση του μέτρου) κ.λπ.

Συνδυασμός - Προσέγγιση

Για να προστατεύσουμε κάποια **αγαθά** που έχουν συγκεκριμένη **αξία** και να μην υποστούμε τις **επιπτώσεις** που θα έχει μία **παραβίαση** που θα τα αφορά, θα πρέπει να χρησιμοποιήσουμε κάποια **μέσα προστασίας** που έχουν κάποιο **κόστος**.

Είναι σαφές ότι το κόστος που συνεπάγονται μέσα προστασίας δεν θα πρέπει να είναι δυσανάλογο της αξίας των αγαθών ή των επιπτώσεων που σχετίζονται με αυτά. Είναι έτσι πιθανόν να επιλέξει ο ιδιοκτήτης ενός πληροφοριακού συστήματος να μην εφαρμόσει κάποια μέσα προστασίας, διότι εκτιμά ότι το κόστος τους είναι υπερβολικό, σε σχέση με την αξία τους και τους κινδύνους που διατρέχουν.

Βασικές διαστάσεις της ασφάλειας των ΠΣ

- ✓ Εμπιστευτικότητα: οι πληροφορίες είναι προσπελάσιμες μόνο από εξουσιοδοτημένους χρήστες
- ✓ Ακεραιότητα: τα δεδομένα και τα προγράμματα τροποποιούνται και καταστρέφονται μόνο με καλά καθορισμένους τρόπους και με κατάλληλη εξουσιοδότηση
- ✓ Διαθεσιμότητα: Οι εξουσιοδοτημένοι χρήστες θα μπορούν να χρησιμοποιήσουν δεδομένα, προγράμματα και υπηρεσίες όταν το επιθυμήσουν
- ✓ Αυθεντικότητα: εξασφάλιση ότι τα δεδομένα είναι απαλλαγμένα ατελειών και ανακριβειών κατά τις εξουσιοδοτημένες τροποποιήσεις
- ✓ Εγκυρότητα: εξασφάλιση ότι τα δεδομένα είναι ακριβή και πλήρη

Συνηθισμένες απειλές στην ασφάλεια

i. Αποκάλυψη συνθηματικών
ii. Πλοήγηση
iii. Αντιποίηση ή μεταμφίεση
iv. Δούρειοι ίπποι
v. Αξιοποίηση προγραμματιστικών σφαλμάτων
vi. Παραπόρτια (trapdoors)
vii. Ιοί
viii. Διαρροή δεδομένων
ix. Συμπερασμός πληροφοριών
x. Πλαστογράφηση
xi. Κανάλια διαρροής
xii. Παρεμπόδιση παροχής υπηρεσιών
xiii. Μη ηθελημένη καταστροφή

Κρυπτογραφία

Οι αλγόριθμοι κρυπτογραφίας χρησιμοποιούνται για δύο σκοπούς:

1. Για να αποδείξει κάποιος στους υπόλοιπους ότι είναι κάτοχος κάποιου συγκεκριμένου κλειδιού. Αν ο εταίρος ή ο επαληθευτής είναι σε θέση να αποκρυπτογραφήσει δεδομένα που έχουν κρυπτογραφηθεί με χρήση του συγκεκριμένου κλειδιού, τότε θεωρείται ότι η κατοχή του κλειδιού έχει αποδειχθεί. Αν επιπρόσθετα μπορεί να εξασφαλισθεί, με άλλα μέσα, ότι κανείς άλλος χρήστης ή οντότητα δεν μπορεί να έχει στη διάθεσή του το ίδιο κλειδί, η χρήση αυτού του κλειδιού συνιστά ταυτόχρονα και σύνδεσμο προς τον χρήστη του κλειδιού. Με τον τρόπο αυτό επιτυγχάνεται η αυθεντικοποίηση.
2. Η απόκρυψη της πληροφορίας, δηλαδή η προσπάθεια να αποφευχθεί η αποκάλυψή της σε μη εξουσιοδοτημένες οντότητες.

Κρυπτογραφία – όροι (1/2)

1. Απλό ή μη κρυπτογραφημένο κείμενο (plain text): Τα δεδομένα όπως χρησιμοποιούνται από τους ανθρώπους ή τις εφαρμογές
2. Κρυπτογραφημένο κείμενο (cipher text): Τα δεδομένα σε ακατάληπτη για τους ανθρώπους ή τις εφαρμογές μορφή.
3. Κρυπτογράφηση: Ο μετασχηματισμός του απλού κειμένου σε κρυπτογραφημένο κείμενο.
4. Αποκρυπτογράφηση: Ο μετασχηματισμός του κρυπτογραφημένου κειμένου σε απλό.
5. Κλειδί: Μια ποσότητα πληροφορίας (σύνολο bytes) που καθορίζει τους μετασχηματισμούς που θα πραγματοποιηθούν κατά τη διαδικασία της κρυπτογράφησης ή αποκρυπτογράφησης.

Κρυπτογραφία – όροι (2/2)

6. Χώρος μη κρυπτογραφημένων μηνυμάτων Μ: Όλα τα δυνατά μηνύματα απλού κειμένου.
7. Χώρος κρυπτογραφημένων μηνυμάτων C: Όλα τα δυνατά μηνύματα κρυπτογραφημένου κειμένου.
8. Χώρος κλειδιών Κ: Όλα τα δυνατά κλειδιά.
9. Οικογένεια μετασχηματισμών κρυπτογράφησης. Μια ομάδα συναρτήσεων E_k με πεδίο ορισμού το Μ και πεδίο τιμών το C.
10. Οικογένεια μετασχηματισμών αποκρυπτογράφησης. Μια ομάδα συναρτήσεων D_k με πεδίο ορισμού το C και πεδίο τιμών το Μ. Υπάρχει μία συνάρτηση για κάθε κλειδί.

Αλγόριθμοι Κρυπτογραφίας

- Συμμετρικοί αλγόριθμοι κρυπτογραφίας:
  - Κρυπτογράφηση με μεταθέσεις (Απλή μετάθεση, «Συρματόπλεγμα», Μετάθεση κατά στήλες, κ.α.)
  - Κρυπτογράφηση με αντικατάσταση (Απλή αντικατάσταση, Πολυαλφαβητική αντικατάσταση, Κρυπτογράφηση τρέχοντος κλειδιού, Μέθοδος Vernam, Αλγόριθμος DES)
- Ασύμμετροι αλγόριθμοι κρυπτογραφίας:
  - Ο αλγόριθμος RSA

Μελέτη περίπτωσης - Παρεμπόδιση παροχής υπηρεσιών από επίθεση στην upload speed εξυπηρετητή

Επίθεση στο upload speed ενός πολυμεσικού εξυπηρετητή

Σενάριο: Ένας πολυμεσικός εξυπηρετητής έχει αποθηκευμένα 2000 videos διάρκειας 5 min το καθένα, μεγέθους 50MB το καθένα και upload speed 1 Gbps.

Τι θα συμβεί αν ζητήσουν 10,000 χρήστες να stream-άρουν κάποιο video από τα 200 σχεδόν (αλλά όχι) ταυτόχρονα;

Συγχώνευση Ροών (stream merging)

Λύση 1 :

Συγχώνευση ροών (stream merging): ο χρήστης που ζητάει 2ος (χρονικά) το video, λαμβάνει και νέα ροή (από t=0), αλλά και τη ροή του χρήστη που ζήτησε 1ος (δηλαδή 2 ροές). Την 1η ροή την προβάλει εκείνη την στιγμή, ενώ τη 2η την αποθηκεύει (buff-άρει). Η 1η ροή ολοκληρώνεται μόλις φτάσει στο χρονικό σημείο που ξεκίνησε η 2η ροή, οπότε ο υπολογιστής του παίζει με καθυστέρηση τη 2η ροή (που έχει buff-άρει) μέχρι να ολοκληρωθεί το περιεχόμενο.

Παράδειγμα stream merging

Στις 10:00:00 ο Φίφης ζητάει να δει το video X, που έχει διάρκεια 5 λεπτά.

Ο server ξεκινάει και του στέλνει το video με τη ροή_1 (video X από 0’ 00” έως 5’ 00”) και ο υπολογιστής του Φίφη προβάλει επί τόπου τη ροή αυτή.

Στις 10:00:20 ο Λέλος ζητάει να δει το video X.

Ο server ξεκινάει και του στέλνει το video με τη ροή_2, η οποία περιέχει τα πρώτα 20 seconds του video X και **ταυτόχρονα** του στέλνει και τη ροή_1 (από 0’ 20” έως 5’ 00”).

Ο υπολογιστής του Λέλου από τις 10:00:20 έως και τις 10:00:40 προβάλει τη ροή_2, ενώ αποθηκεύει τη ροή_1.

Ο υπολογιστής του Λέλου από τις 10:00:40 έως τις 10:05:20 προβάλει με καθυστέρηση 20” τη ροή_1.

Άρα, μόνο για 20” ο server στέλνει (upload) 2 ροές!

near Video On Demand (nVoD)

Λύση 2 :

υπηρεσία nVoD: ομαδοποιεί τους χρήστες, ο οποίοι δέχονται μία μικρή καθυστέρηση έναρξης του πολυμεσικού περιεχομένου και όλοι οι χρήστες της ομάδας λαμβάνουν την ίδια ροή

Παράδειγμα nVoD

Video διάρκειας 5 λεπτών.

Η υπηρεσία επιλέγει ανώτερη τιμή καθυστέρησης ανά χρήστη τα 10 seconds.

Αν ξεκινήσουμε το παράδειγμά μας στις 10:00:00, όσοι χρήστες ζητήσουν το video στο διάστημα [10:00:00, 10:00:10) θα «περιμένουν» έως τις 10:00:10, οπότε η ροή_1 θα ξεκινήσει να στέλνει το video.

Η ροή_2 θα «φύγει» από τον server στις 10:00:20 (για να την πάρουν όσοι μπήκαν από [10:00:10, 10:00:20), η ροή_3 στις 10:00:30, κ.ο.κ.

Άρα, θα χρειαστούν συνολικά 30 ροές, όσοι χρήστες και αν ζητήσουν το video.

Γενίκευση παραδείγματος nVoD για server πολυμεσικού περιεχομένου

Διαθέτουμε server με upload speed 100Gbps (δεδομένο).

Η πολιτική της εταιρίας είναι να μη δέχεται ο κάθε πελάτης μας καθυστέρηση πάνω από 20 seconds (δεδομένο).

Τα videos μας έχουν διάρκεια 30 minutes το καθένα (δεδομένο).

Αν χρησιμοποιήσουμε την τεχνική nVoD, για να εμποδίσουμε την παρεμπόδιση παροχής υπηρεσιών από επίθεση στην upload speed του server μας, μέχρι πόσα videos μπορούμε να έχουμε στον server μας;

Αναφορά - Υλικό

ΣΗΜΕΙΩΣΕΙΣ ΜΑΘΗΜΑΤΟΣ

«ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

Κ. Βασιλάκης

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ,

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ