ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΤΜΗΜΑ ΙΣΤΟΡΙΑΣ ΑΡΧΑΙΟΛΟΓΙΑΣ
ΠΠΣ ΔΙΑΧΕΙΡΙΣΗΣ ΠΟΛΙΤΙΣΜΙΚΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΑΙ ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗΣ ΣΕ ΠΟΛΙΤΙΣΜΙΚΑ ΠΕΡΙΒΑΛΛΟΝΤΑ

Δ’ ΕΤΟΣ

ΑΚΑΔΗΜΑΪΚΟ ΕΤΟΣ 2021-22

Δρ. Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

ΣΚΟΠΟΣ ΜΑΘΗΜΑΤΟΣ

- Μελέτη των μηχανισμών ασφάλειας και εμπιστοσύνης σε υπολογιστικά συστήματα όπου διακινείται πολυμεσική πληροφορία, όταν αυτά χρησιμοποιούνται σε διάφορα πολιτισμικά περιβάλλοντα.

- Παρουσίαση των απειλών που αντιμετωπίζουν τα υπολογιστικά συστήματα και των τρόπων αντιμετώπισής τους είτε σε επίπεδο διαχείρισης πληροφορίας, είτε σε τεχνικό και νομικό επίπεδο.

- Ο φοιτητής μέσω του μαθήματος θα έρθει σε επαφή με μια καινούργια φιλοσοφία Διαχείρισης Πολυμεσικών Υπολογιστικών Συστημάτων, όπου η ανάγκη για την ύπαρξη μέτρων ασφάλειας επηρεάζει άμεσα τον τρόπο διαχείρισής τους.

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ 1/2

- Βασικές έννοιες ασφάλειας και εμπιστοσύνης.
- Είδη επιθέσεων: ιοί, σκουλήκια, δούρειοι ίπποι, επιθέσεις άρνησης υπηρεσίας.
- Κρυπτογράφηση. Ασύμμετρα και συμμετρικά κρυπτοσυστήματα. Αλγόριθμος Καίσαρα. Συστήματα δημόσιου-ιδιωτικού κλειδιού. Diffee-Hellman.
- Πιστοποίηση ταυτότητας χρήστη. Έλεγχος πρόσβασης. Ασφάλεια σε πολιτισμικά πληροφοριακά συστήματα και βάσεις δεδομένων.
- Ασφάλεια στο διαδίκτυο: ψηφιακά πιστοποιητικά, ψηφιακές υπογραφές, κρυπτογραφία (SSL)
- Προστασία πνευματικών δικαιωμάτων (ψηφιακή υδατογράφηση εικόνας, ήχου, βίντεο).

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ 2/2

- Ασφάλεια λειτουργικών συστημάτων: είδη επιθέσεων, μηχανισμοί προστασίας, έμπιστα συστήματα.
- Ασφάλεια δικτύων: Υπηρεσίες και Μηχανισμοί Ασφάλειας (κατά ISO 7498-2).
- Συστήματα διαχείρισης εμπιστοσύνης.
- Ευστάθεια και εμπιστοσύνη σε κατανεμημένα ετερογενή πολυμεσικά δίκτυα.
- Νομικά Θέματα Προστασίας Προσωπικών Δεδομένων.
- Εφαρμογές.

ΒΙΒΛΙΟΓΡΑΦΙΑ 1/2

- W. Stallings, L. Brown, Ασφάλεια Υπολογιστών: Αρχές και Πρακτικές, ISBN: 978-960-461-668-8, Εκδ. Κλειδάριθμος, 2016.
- Ι. Μαυρίδης, Ασφάλεια Πληροφοριών στο Διαδίκτυο, ISBN: 978-960-603-193-9, Εκδ. Ελληνικά Ακαδημαϊκά Συγγράμματα και Βοηθήματα-Αποθετήριο «Κάλλιπος», 2016.
- Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, Ασφάλεια Πληροφοριακών Συστημάτων, ISBN: 960-8105-57-9, Εκδ. Νέων Τεχνολογιών, 2004.
- A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.
- E. Gerck, Overview of Certification Systems, 2000.
- Γ. Πάγκαλος, Ι. Μαυρίδης, Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων.
- A. Tanenbaum, Σύγχρονα Λειτουργικά Συστήματα, Εκδ. Κλειδάριθμος, 2002.

ΒΙΒΛΙΟΓΡΑΦΙΑ 2/2

- Σ. Δημητριάδης, Α. Πομπόρτσης, Ε. Τριανταφύλλου, Τεχνολογία Πολυμέσων, Εκδ. Τζιόλα, 2004.
- Δ. Χριστοφιλόπουλος, Προστασία Πολιτιστικών Αγαθών, Εκδόσεις Δίκαιο & Οικονομία, 2005.
- Α. Σουρής, Δ. Πατσός, Ν. Γρηγοριάδης, Ασφάλεια της Πληροφορίας, Εκδ. Νέων Τεχνολογιών, 2004.
- C.P. Pfleeger, Security in Computing, Prentice-Hall, 1997.
- W. Cheswick, S. Bellovin, Firewalls and Internet Security: Repelling the Wily Hacker, Addison Wesley, 1995.
- D. Gollmann, Computer Security, J.Wiley & Sons, 1999.
- B. Schneier, Applied Cryptography, J.Wiley & Sons, 1997.
- W. Ford, Computer Communications Security», Prentice-Hall, 1994.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΤΜΗΜΑ ΙΣΤΟΡΙΑΣ ΑΡΧΑΙΟΛΟΓΙΑΣ
ΠΠΣ ΔΙΑΧΕΙΡΙΣΗΣ ΠΟΛΙΤΙΣΜΙΚΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΑΙ ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗΣ ΣΕ ΠΟΛΙΤΙΣΜΙΚΑ ΠΕΡΙΒΑΛΛΟΝΤΑ

ΔΙΔΑΚΤΙΚΕΣ ΕΝΟΤΗΤΕΣ 1-2

ΘΕΜΑ: ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗΣ

Δρ. Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

ΠΕΡΙΕΧΟΜΕΝΑ

- Βασικές Έννοιες Ασφάλειας
- Γενικά Θέματα Ασφάλειας
- Επιθέσεις στην Επικοινωνία Υπολογιστών
- Επιθέσεις Κακής Χρήσης
- Βασικές Έννοιες Εμπιστοσύνης
- Βιβλιογραφία

Άτυπος Ορισμός Ασφάλειας

- Ασφάλεια υπολογιστικών συστημάτων είναι η προστασία αυτών των συστημάτων είτε από μη πιστοποιημένη πρόσβαση είτε από κακόβουλους χρήστες (χάκερς) και λογισμικά (ιοί).

- Όχι πλήρης ορισμός.

Απειλές από Κακόβουλες Ενέργειες 1/2

- Κλοπή (theft) υλικού, λογισμικού, δεδομένων από εισβολή (intrusion) ή κλοπή υπηρεσίας με υπεξαίρεση (misappropriation) ή κακή χρήση (misuse)
- Απάτη (fraud) με μεταμφίεση (masquerade), πλαστογράφηση (falsification) και αποκήρυξη (repudiation)
- Απώλεια αξιοπιστίας (reliability lost) συστήματος από διαρροή στοιχείων χρηστών (έκθεση-exposure)
- Κατασκοπία (espionage) από τρίτους με παρεμβολή (interception)
- Εξαγωγή συμπεράσματος (inference)

Απειλές από Κακόβουλες Ενέργειες 2/2

- Βανδαλισμοί (vandalism) από κακόβουλους χρήστες ή δυσαρεστημένους διαχειριστές με πρόκληση αναπηρίας (incapacitation), αλλοίωση (corruption) και παρεμπόδιση (obstruction).
- Ηλεκτρονική τρομοκρατία (e-terrorism)
- Ηλεκτρονική εχθροπραξία (e-warfare)

Μη Κακόβουλες Απειλές

- Ανθρώπινη βλακεία
- Ανάμιξη
- Άγνοια
- Ατυχήματα
- Αφηρημάδα
- Καταστροφές
- Χαλασμένος εξοπλισμός

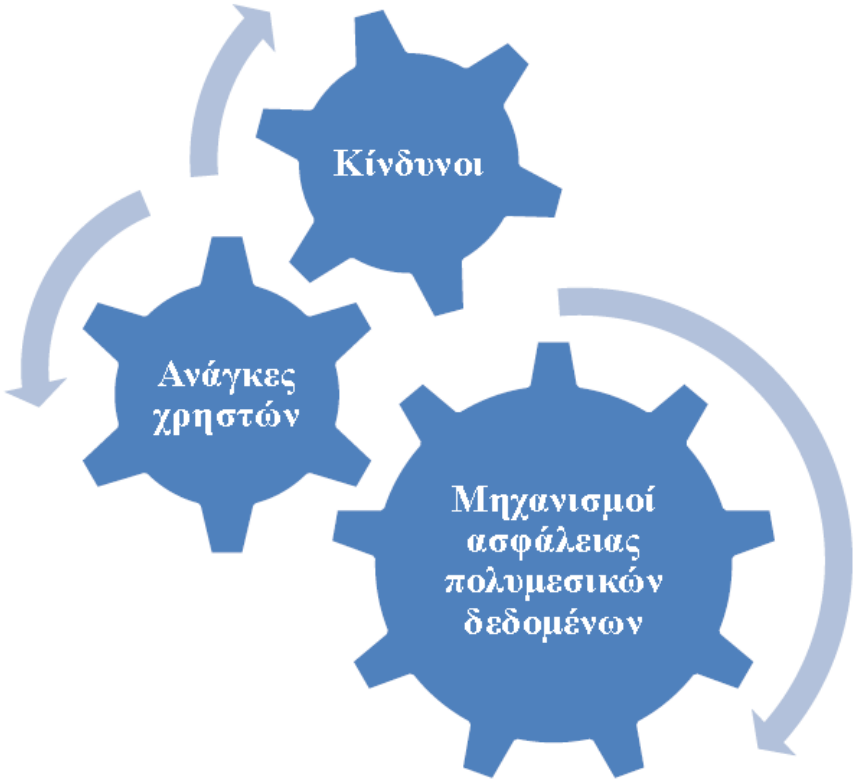
Συνέπειες Απειλών

- Μη εξουσιοδοτημένη αποκάλυψη (unauthorized disclosure)
- Σφετερισμός (usurpation)
- Διατάραξη (disruption)
- Παραπλάνηση (deception)

Πρακτικές Ασφάλειας

- Ανταπόκριση σε νομικές υποχρεώσεις για αποφυγή έκθεσης σε κίνδυνο μήνυσης και αντιδικίας.
- Ένα ασφαλές σύστημα πρέπει να εξασφαλίζει τη συμμόρφωση σε νόμους και κώδικες δεοντολογίας. Πρέπει να φαίνεται ότι υπακούμε στο νόμο.
- Υιοθέτηση πολιτικών πρόληψης.
- Προσδιορισμός και εκτίμηση κινδύνων.
- Λήψη φθηνών μέτρων ελαχιστοποίησης κινδύνων.

Κίνδυνοι vs. Ανάγκες χρηστών vs. Ασφάλεια



Δρ. Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Ασφάλεια Υπολογιστών σε Πληροφοριακά Συστήματα (NIST)

Ασφάλεια υπολογιστών είναι η προστασία που παρέχεται σε αυτοματοποιημένα πληροφοριακά συστήματα, έτσι ώστε να επιτύχουν τους εφαρμόσιμους στόχους της διατήρησης της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των πόρων των πληροφοριακών συστημάτων (υλικό, λογισμικό, δεδομένα, τηλεπικοινωνίες).

Γενικός Ορισμός Ασφάλειας

- Η ασφάλεια ενός υπολογιστικού συστήματος αφορά όλα τα θέματα ακεραιότητας του συστήματος, νομικά, ηθικά, οικονομικά, λειτουργικά και πληροφοριακά.

- Η ασφάλεια αφορά την επιβολή της απαιτούμενης συμπεριφοράς, την παρεμπόδιση ανεπιθύμητης συμπεριφοράς και την παρακολούθηση της συμπεριφοράς για να εξασφαλισθεί ότι υπάρχει συμμόρφωση σε νόμους και αρχές.

Βασικές Απαιτήσεις Ασφάλειας

- **Εμπιστευτικότητα** (confidentiality)
  - **Εμπιστευτικότητα δεδομένων**: μη αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένους χρήστες
  - **Ιδιωτικότητα** (privacy): Οι χρήστες ελέγχουν ποιες προσωπικές πληροφορίες και από ποιους μπορούν να συλλεχθούν, να αποθηκευθούν, να επεξεργασθούν και να αποκαλυφθούν.
- **Ακεραιότητα** (integrity)
  - **Ακεραιότητα δεδομένων**: προστασία δεδομένων και προγραμμάτων από μη εξουσιοδοτημένη τροποποίηση.
  - **Ακεραιότητα συστήματος**: το σύστημα εκτελεί την προγραμματισμένη του λειτουργία χωρίς σκόπιμες ή ακούσιες παρεμβολές.
- **Διαθεσιμότητα** (availability): το σύστημα λειτουργεί όταν χρειάζεται και δεν αρνείται εξυπηρέτηση σε εξουσιοδοτημένους χρήστες

Πρόσθετες Απαιτήσεις Ασφάλειας

- **Αυθεντικότητα** (authenticity): έλεγχος της γνησιότητας χρήστη μέσω μηχανισμού επικύρωσης.

- **Λογοδοσία** (accountability): απόδοση ευθυνών σε χρήστη, αποτροπή αποκήρυξης, απομόνωση σφαλμάτων, εντοπισμό και παρεμπόδιση εισβολών, επανόρθωση, νομικές ενέργειες.

Οντότητες σε Κίνδυνο

- **Χρήστες**: έλλειψη διαθεσιμότητας, ακεραιότητας, εμπιστευτικότητας

- **Πόροι**
  - Υλικό: έλλειψη διαθεσιμότητας (ακούσια, εκούσια ζημιά, κλοπή), απώλεια εμπιστευτικότητας (κλοπή)
  - Λογισμικό: έλλειψη διαθεσιμότητας, απώλεια ακεραιότητας / αυθεντικότητας (ιοί, πειρατεία)
  - Δεδομένα: έλλειψη διαθεσιμότητας, ακεραιότητας, εμπιστευτικότητας
  - Τηλεπικοινωνίες/δίκτυα: παθητικές και ενεργείς επιθέσεις

Δημοφιλείς Απειλές

- Εισβολέας
- Κακόβουλο λογισμικό

Εισβολείς

Χρήστες που προσπαθούν να αποκτήσουν πρόσβαση σε ένα σύστημα ή να αυξήσουν το εύρος των προνομίων πρόσβασης σε ένα σύστημα.

Παραδείγματα Εισβολών 1/2

- Εκτέλεση απομακρυσμένης πρόσβασης σε e-mail server.
- Παραποίηση σελίδων Web server.
- Πρόβλεψη και σπάσιμο συνθηματικών.
- Αντιγραφή βάσης δεδομένων με αριθμούς πιστωτικών καρτών.
- Παρατήρηση ευαίσθητων δεδομένων.
- Υποκλοπή ονομάτων χρηστών και κωδικών από σταθμό εργασίας.

Παραδείγματα Εισβολών 2/2

- Χρήση ανεπιτήρητου σταθμού εργασίας χωρίς άδεια.
- Κλήση μη ασφαλούς modem και απόκτηση εσωτερικής δικτυακής πρόσβασης.
- Χρήση σφάλματος αδειοδότησης σε ανώνυμο FTP server για διανομή πειρατικού λογισμικού και αρχείων μουσικής.

Τεχνικές Εισβολής

- Χρήση τρωτών σημείων συστήματος ή λογισμικού για απόκτηση πρόσβασης σε σύστημα ή αύξησης των προνομίων πρόσβασης.

- Δυο είδη εισβολής:
  - Αξιοποίηση επιθέσεων, όπως οι υπερχειλίσεις απομονωτών σε προγράμματα που εκτελούνται με συγκεκριμένα προνόμια.

  - Απόκτηση προστατευμένων πληροφοριών, όπως συνθηματικών χρήση.

Κακόβουλο Λογισμικό

- Προγράμματα που αξιοποιούν αδυναμίες των υπολογιστικών συστημάτων (malware).
- Προκαλούν ζημιές ή καταναλώνουν τους πόρους του υπολογιστή στόχου.
- Εξάπλωση σε άλλους υπολογιστές μέσω e-mail ή μολυσμένων δισκετών.

Αντιμετώπιση Εισβολών

- Πιστοποίηση και έλεγχος πρόσβασης
- Χρήση firewalls (τείχη προστασίας)
- Συστήματα εντοπισμού εισβολής

Κατευθύνσεις Ψηφιακής Ασφάλειας

- Κρυπτογραφία (μετατροπή ψηφιακού προϊόντος σε μορφή προσβάσιμη, αλλά όχι αναγνωρίσιμη από μη εξουσιοδοτημένο χρήστη)

- Ψηφιακές υπογραφές/πιστοποιητικά (αναγνώριση δημιουργού, ενσωμάτωση πληροφορίας σε επικεφαλίδα προϊόντος ή σε ανεξάρτητο αρχείο που συνοδεύει το προϊόν)

- Υδατογράφηση (ένθεση πρόσθετης πληροφορίας σε δεδομένα χωρίς αλλοίωση της ποιότητας με σκοπό την προστασία των πνευματικών δικαιωμάτων και την αυθεντικότητα του περιεχομένου)

Επιθέσεις vs. Απαιτήσεις Ασφάλειας

Απαίτηση ασφάλειας \ Είδος επίθεσης	Πειρατεία	Επιθέσεις υποκλοπής	Επιθέσεις διακοπής	Επιθέσεις αλλοίωσης	Επιθέσεις εισαγωγής
Προστασία πνευματικής ιδιοκτησία	•				
Ασφαλής διανομή πολυμεσικού περιεχομένου	•				
Εμπιστευτικότητα		•			
Διαθεσιμότητα			•		
Ακεραιότητα				•	
Αυθεντικότητα					•

Δρ. Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Ανάγκη Έμπιστων Συστημάτων

Η εμπιστοσύνη είναι μια ιδιότητα που διευκολύνει τις τεχνολογίες που στηρίζουν την επικοινωνία στο Διαδίκτυο, τις παρεχόμενες υπηρεσίες σε αυτό και κάνει δυνατή την ανάπτυξη κατανεμημένων ασφαλών εφαρμογών που στηρίζονται σε τεχνολογίες πρακτόρων.

- Ένα κρίσιμο ζητούμενο στο Διαδίκτυο είναι αν αξίζει να δείχνουμε εμπιστοσύνη σε διάφορες υπηρεσίες και ποιες είναι αυτές.
- Οι υπηρεσίες στο Διαδίκτυο επιτρέπουν την αλληλεπίδραση με πολλούς οργανισμούς και πεδία τα οποία δεν έχουν όλα τον ίδιο βαθμό εμπιστοσύνης.
- Μια υπηρεσία στο Διαδίκτυο πρέπει να υποστηρίζει ένα ευρύ φάσμα σχέσεων εμπιστοσύνης και πολιτικών ασφαλείας.

Εφαρμογές που Απαιτούν Εμπιστοσύνη

- Ηλεκτρονική διακυβέρνηση
- Επιλογή περιεχομένου για έγγραφα στο Web
- Ιατρικά συστήματα
- Τηλεσυζήτηση και ηλεκτρονική αλληλογραφία
- Κινητός υπολογισμός
- Ηλεκτρονικό εμπόριο

Παράγοντες Εμπιστοσύνης

- Τιμιότητα
- Φιλαλήθεια
- Επάρκεια
- Αξιοπιστία
- Ασφάλεια
- Έγκαιρη διεκπεραίωση

Γενικός Ορισμός Εμπιστοσύνης

- Υπάρχουν διάφοροι ορισμοί της εμπιστοσύνης σε ένα σύστημα που εξαρτώνται από τις συγκεκριμένες ανάγκες αυτού του συστήματος.

- Ένας γενικός ορισμός δίνεται στο λεξικό Webster: “Η εμπιστοσύνη είναι μια υποτιθέμενη πίστη σε κάποιο πρόσωπο ή αντικείμενο. Μια έμπιστη εξάρτηση από το χαρακτήρα, την ικανότητα, τη δύναμη ή την αλήθεια κάποιου προσώπου ή αντικειμένου. Είναι μια επιφόρτιση ή καθήκον που επιβάλλεται από την πίστη ή την εμπιστοσύνη ή ως μιας προϋπόθεσης μιας σχέσης. Είναι να δείχνεις εμπιστοσύνη σε μια οντότητα.”

Κοινωνιολογικός Ορισμός Εμπιστοσύνης

Η εμπιστοσύνη είναι ένα συγκεκριμένο επίπεδο της υποκειμενικής πιθανότητας με την οποία ένας πράκτορας θα εκτελεί μια συγκεκριμένη ενέργεια, πριν εμείς μπορέσουμε να ελέγξουμε μια τέτοια ενέργεια και σε ένα περιεχόμενο το οποίο να επηρεάζει τη δικιά μας ενέργεια. [Κοινωνιολόγος Diego Gambetta]

Ορισμός ECJRC

Η εμπιστοσύνη είναι η ιδιότητα μιας επιχειρηματικής σχέσης όπου η εμπιστοσύνη είναι κοινός τόπος μεταξύ των συνεργατών και των επιχειρηματικών συναλλαγών που διενεργούνται μεταξύ τους.

Ορισμός Oxford Reference Dictionary

- Εμπιστοσύνη είναι η σταθερή πίστη στην αξιοπιστία ή την αλήθεια ή τη δύναμη μιας οντότητας.

- Μια οντότητα άξια εμπιστοσύνης θα είναι αξιόπιστη και δε θα αποτύχει κατά τη διάρκεια μιας αλληλεπίδρασης, θα διεκπεραιώσει μια υπηρεσία ή ενέργεια μέσα σε σύντομο χρόνο, θα πει την αλήθεια και θα είναι τίμια σε σχέση με τυχόν αλληλεπιδράσεις και δε θα αποκαλύψει εμπιστευτικές πληροφορίες.

Εμπιστοσύνη vs. Εξουσιοδότηση vs. Αυθεντικοποίηση

Υπάρχει σύγχυση πολλές φορές μεταξύ των εννοιών εμπιστοσύνη, εξουσιοδότηση και αυθεντικοποίηση.

- **Εξουσιοδότηση** είναι το εξαγόμενο του ραφιναρίσματος μιας αφηρημένης σχέσης εμπιστοσύνης. Είναι μια πολιτική απόφασης που αναθέτει δικαιώματα ελέγχου πρόσβασης σε ένα υποκείμενο με σκοπό την εκτέλεση συγκεκριμένων ενεργειών σε ένα συγκεκριμένο στόχο με σαφείς περιορισμούς.
- **Αυθεντικοποίηση** είναι η αξιολόγηση της ταυτότητας μιας οντότητας που μπορεί να εκτελεστεί μέσω ενός κωδικού πρόσβασης, μια έμπιστη υπηρεσία ή με τη χρήση πιστοποιητικών.
- **Εμπιστοσύνη** είναι η σταθερή πίστη στην ικανότητα μιας οντότητας να δρα αξιόπιστα, έγκαιρα και ασφαλή μέσα σε ένα συγκεκριμένο περιβάλλον.

Ιδιότητες Εμπιστοσύνης

Η έννοια της εμπιστοσύνης εξαρτάται από το περιεχόμενο, είναι δυναμική και δε χαρακτηρίζεται από μονοτονικότητα.

Ιδιότητες Σχέσεων Εμπιστοσύνης 1/3

- **Δεν είναι απόλυτες** (ένας χρήστης δεν επιτρέπει σε άλλον χρήστη ή στον ίδιο να κάνει τα πάντα).

- **Μια σχέση εμπιστοσύνης μεταξύ δυο οντοτήτων μπορεί να είναι 1-1, αλλά όχι συμμετρική** (η εμπιστοσύνη ενός χρήστη σε άλλον δεν είναι ίδια με την εμπιστοσύνη του δεύτερου προς τον πρώτο).

- **Μια σχέση εμπιστοσύνης μπορεί να είναι 1-πολλές οντότητες** (ένας χρήστης εμπιστεύεται μια ομάδα χρηστών).

- **Μια σχέση εμπιστοσύνης μπορεί να είναι πολλές-πολλές οντότητες** (αρκετοί χρήστες εμπιστεύονται αρκετούς άλλους).

Ιδιότητες Σχέσεων Εμπιστοσύνης 2/3

- **Μια σχέση εμπιστοσύνης μπορεί να είναι μεταξύ κατανεμημένων οντοτήτων που δεν έχουν άμεση γνώση η μια της άλλης.**

- **Δεν είναι γενικά μεταβατικές, αλλά κάποιες φορές μπορεί να είναι** (εξουσιοδότηση εμπιστοσύνης).

- **Ύπαρξη επιπέδων εμπιστοσύνης** (σε κάποιες οντότητες μπορούμε να επιτρέπουμε περισσότερες ενέργειες από άλλες).

Ιδιότητες Σχέσεων Εμπιστοσύνης 3/3

- Ανάθεση τιμών εμπιστοσύνης σε χρήστες από χρήστες (χρήση Josang Opinion Model).
  - Μια γνώμη είναι η αναπαράσταση μιας πεποίθησης κάποιου και αναπαρίσταται ως τριπλέτα (b, d, i) όπου b είναι ένα μέτρο της πεποίθησης κάποιου, d είναι ένα μέτρο της μη πεποίθησης και i είναι ένα μέτρο της άγνοιας, τέτοια ώστε b+d+i=1.

Εμπιστοσύνη vs. Διαχείριση Ρίσκου

- Το επίπεδο εμπιστοσύνης είναι αντιστρόφως ανάλογο με το βαθμό ρίσκου σε σχέση με μια υπηρεσία ή συναλλαγή.

- Η μελέτη της σχέσης διαχείρισης ρίσκου και εμπιστοσύνης είναι σε νηπιακό επίπεδο.

- Σήμερα η εμπιστοσύνη κυρίως στηρίζεται σε ένα συνδυασμό κρίσης ή γνώμης που προκύπτουν από συναντήσεις πρόσωπο με πρόσωπο ή συστάσεις συναδέλφων, φίλων, συνεργατών.

Οντότητες σε ένα Έμπιστο Περιβάλλον

- Εμπιστευόμενος χρήστης (trustor)
- Έμπιστη οντότητα (trustee)

Είδη Εμπιστοσύνης

- **Διαπροσωπική-interpersonal** (εξαρτώμενη από πράκτορες και περιεχόμενο)
- **Δομική-structural** (σύστημα μέσα στο οποίο η εμπιστοσύνη ενυπάρχει)
- **Διαθέσιμη-dispositional** (ανεξάρτητη από πράκτορες και περιεχόμενο)

Είδη Έμπιστων Σχέσεων σε Υπηρεσίες Διαδικτύου

- Πρόσβαση σε πόρους χρήστη (ο χρήστης εμπιστεύεται ένα έμπιστο σύστημα)
- Παροχή υπηρεσιών από έμπιστο σύστημα
- Αυθεντικοποίηση/πιστοποίηση έμπιστου συστήματος
- Εκπροσώπηση
- Εμπιστοσύνη υποδομής

Πρόσβαση σε Πόρους Χρήστη 1/3

- Ένας χρήστης που εμπιστεύεται κάποιον (trustor) εμπιστεύεται ένα έμπιστο σύστημα/χρήστη (trustee) να χρησιμοποιήσει τους πόρους που κατέχει ή ελέγχει (περιβάλλον εκτέλεσης λογισμικού ή εφαρμογή/υπηρεσία).

- Η εμπιστοσύνη σε πρόσβαση πόρων είναι αντικείμενο των ειδικών ασφάλειας για πολλές δεκαετίες από τη σκοπιά του ελέγχου πρόσβασης.

Πρόσβαση σε Πόρους Χρήστη 2/3

- Υπάρχει διαφορά ανάμεσα στην εμπιστοσύνη που δείχνεις σε κάποιον να διαβάσει/γράψει ένα αρχείο σε έναν εξυπηρετητή και στην εμπιστοσύνη που αφορά στην εκτέλεση λογισμικού μέσα στο σύστημά σου.

- Η χρήση λογισμικού σε ένα σύστημα απαιτεί μεγαλύτερο βαθμό εμπιστοσύνης καθώς συναρτάται με τη μη καταστροφή πόρων χρήστη, με τον τερματισμό εκτέλεσης σε λογικό χρόνο και με τη μη κατάχρηση πόρων (μνήμη, χρόνος επεξεργαστή, χώρος τοπικών αρχείων).

Πρόσβαση σε Πόρους Χρήστη 3/3

- Οι αποφάσεις εμπιστοσύνης όσον αφορά την πρόσβαση σε πόρους χρήστη αντιστοιχούνται σε αποφάσεις ελέγχου πρόσβασης.
- Οι αποφάσεις εμπιστοσύνης χρήσης πόρων αποτελούν τη βάση για τον καθορισμό μιας πολιτικής εξουσιοδότησης, που μπορεί να υλοποιηθεί με μηχανισμούς ελέγχου πρόσβασης ή αντιπυρικούς κανόνες σε λειτουργικά συστήματα ή βάσεις δεδομένων.
- Η σχέση εμπιστοσύνης μπορεί να διερμηνευτεί ως κανόνες εξουσιοδότησης που καθορίζουν τις ενέργειες που ένας έμπιστος χρήστης μπορεί να εκτελέσει στους πόρους του χρήστη/trustor και τους περιορισμούς που εφαρμόζονται (χρονική περίοδος επίτρεψης ενεργειών).

Παροχή Υπηρεσιών από Έμπιστο Σύστημα

- Ο χρήστης/trustor εμπιστεύεται το έμπιστο σύστημα να παρέχει μια υπηρεσία που δεν περιλαμβάνει πρόσβαση στους πόρους του χρήστη.

- Οι ASPs χρειάζονται τέτοια σχέση εμπιστοσύνης για να εγκατασταθούν.

- Υπάρχουν τρία είδη σχέσεων εμπιστοσύνης παροχής υπηρεσιών:
  - Εμπιστοσύνη πεποίθησης (confidence trust)
  - Εμπιστοσύνη επάρκειας (competence trust)
  - Εμπιστοσύνη αξιοπιστίας ή ακεραιότητας (reliability or integrity trust)

Εμπιστοσύνη Πεποίθησης

- Ο χρήστης/trustor έχει την πίστη ότι οι υπηρεσίες που παρέχονται από ένα σύστημα έχουν ένα συγκεκριμένο επίπεδο.
- Μοιάζει με έλεγχο πρόσβασης όπου το υποκείμενο έχει την άδεια να προσπελάσει μόνο έμπιστες υπηρεσίες.
- Ο χρήστης έχει εμπιστοσύνη στο σύστημα που θα χρησιμοποιήσει.

Εμπιστοσύνη Επάρκειας

- Ο χρήστης/trustor εμπιστεύεται την επάρκεια ενός συστήματος να παρέχει μια υπηρεσία.

- Το έμπιστο σύστημα μπορεί να εκτελέσει κάποια ενέργεια εκ μέρους του χρήστη επιτυχώς.

Εμπιστοσύνη Αξιοπιστίας ή Ακεραιότητας

Ο χρήστης εμπιστεύεται ένα σύστημα ότι έχει μηχανισμούς που διασφαλίζουν την προστασία προσωπικών δεδομένων και εξασφαλίζουν την ασφάλεια των κάθε είδους συναλλαγών.

Πιστοποίηση Έμπιστων Συστημάτων

- Πιστοποίηση της δυνατότητας εμπιστοσύνης ενός συστήματος από μια άλλη αρχή.
- Η σχέση εμπιστοσύνης στηρίζεται στα πιστοποιητικά που ένα σύστημα μπορεί να παρουσιάσει σε ένα χρήστη.
- Τα πιστοποιητικά χρησιμοποιούνται για την αυθεντικοποίηση της ταυτότητας ή της συμμετοχής μιας ομάδας σε εφαρμογές Διαδικτύου.
- Η αρχή πιστοποίησης παρέχει μια έμπιστη υπηρεσία πιστοποίησης που είναι τύπος σχέσης εμπιστοσύνης παροχής υπηρεσίας.

Εκπροσώπηση

- Ο χρήστης/trustor εμπιστεύεται ένα σύστημα να τον εκπροσωπήσει παίρνοντας αποφάσεις στο όνομά του σχετικά με έναν πόρο ή υπηρεσία που ο χρήστης κατέχει ή ελέγχει.

- Είναι ένας ειδικός τύπος έμπιστης σχέσης παροχής υπηρεσίας (έμπιστη υπηρεσία λήψης αποφάσεων).

Εμπιστοσύνη Υποδομής

- Εμπιστοσύνη χρήση στη βασική του υποδομή.

- Ένας χρήστης πρέπει να εμπιστεύεται τον εαυτό του.
  - Σταθμό εργασίας
  - Τοπικό δίκτυο
  - Τοπικούς εξυπηρετητές

- Το TCB (Trusted Computing Base) είναι ένα σύνολο πόρων που πρέπει να είναι έμπιστες για όλες τις εφαρμογές που εκτελούνται σε μια μηχανή για να υποστηρίξουν την επιθυμητή πολιτική ασφάλειας [U.S. Dept. of Defense].

Μέρη Έμπιστου Συστήματος

- Εγκατάσταση εμπιστοσύνης
- Διαχείριση εμπιστοσύνης
- Ασφάλεια

Διαχείριση Εμπιστοσύνης

- Η διαχείριση εμπιστοσύνης αναφέρθηκε για πρώτη φορά το 1996 [Blaze et. al, 1996] ως ένα συνεκτικό πλαίσιο για τη μελέτη των πολιτικών ασφάλειας, των διαπιστευτηρίων/πιστοποιητικών ασφάλειας και των έμπιστων σχέσεων.

- Δυο από τα πρώτα συστήματα διαχείρισης εμπιστοσύνης είναι τα PolicyMaker και KeyNote.

Είδη Μοντέλων Διαχείριση Εμπιστοσύνης

Υπάρχουν δυο είδη:

- Στηριζόμενα σε πιστοποιητικά
- Βασισμένα σε υπόληψη (η συμπεριφορά παρατηρείται άμεσα ή έμμεσα)
  - Συστάσεις: πληροφορία εμπιστοσύνης μοιράζεται μεταξύ των ομότιμων συστημάτων

Προβλήματα

- Παροχή υπηρεσίας
  - hTRUST, MATE, PolicyMaker, KeyNote
- Δρομολόγηση
  - CONFIDANT, SECURE, STRUDEL

Προσεγγίσεις Διαχείρισης Εμπιστοσύνης

- **Ατομική πρωτοβουλία-individual initiative (αναρχική) [hTrust, STRUDEL, MATE]**
  - Κάθε πράκτορας είναι υπεύθυνος για την τύχη του
- **Σφαιρική εμπιστοσύνη - global trust [EigenTrust]**
  - Κάθε ομότιμο μέλος του συστήματος έχει μια μοναδική σφαιρική τιμή εμπιστοσύνης προσπελάσιμη από τα υπόλοιπα μέλη
- **Ομόσπονδη εμπιστοσύνη - federated trust [Chun and Bavier, 2004]**
  - Διαχείριση σχετικών με εμπιστοσύνη δραστηριοτήτων σε πολλαπλά και ετερογενή πεδία ασφάλειας και αυτόνομα συστήματα
  - Σχετίζεται με στρατηγικές διαχείρισης συμπεριφορών σε περισσότερα του ενός πεδία

Βιβλιογραφία

- W. Stallings, and L. Brown, “Computer Security: Principles and Practice”, Prentice Hall, 2008.
- Computer Security Resource Center
- CERT Coordination Center
- Vmyths