Cryptography and Network Security Overview & Chapter 1

Fifth Edition

by William Stallings

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—*The Art of War,* Sun Tzu

Δομή Παρουσίασης

- Αλγόριθμοι Κρυπτογράφησης
  - Συμμετρικοί
  - Ασύμμετροι
  - Συναρτήσεις Κατακερματισμού (hash functions)
- Αμοιβαία Εμπιστοσύνη (Mutual Trust)
- Ασφάλεια Δικτύων
- Ασφάλεια Υπολογιστών

Standards Organizations

- National Institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)

Εισαγωγή

- *The combination of **space**, **time**, and **strength** that must be considered as the basic elements of this theory of defense makes this a fairly **complicated** matter. Consequently, it is not easy to find a fixed point of departure..*

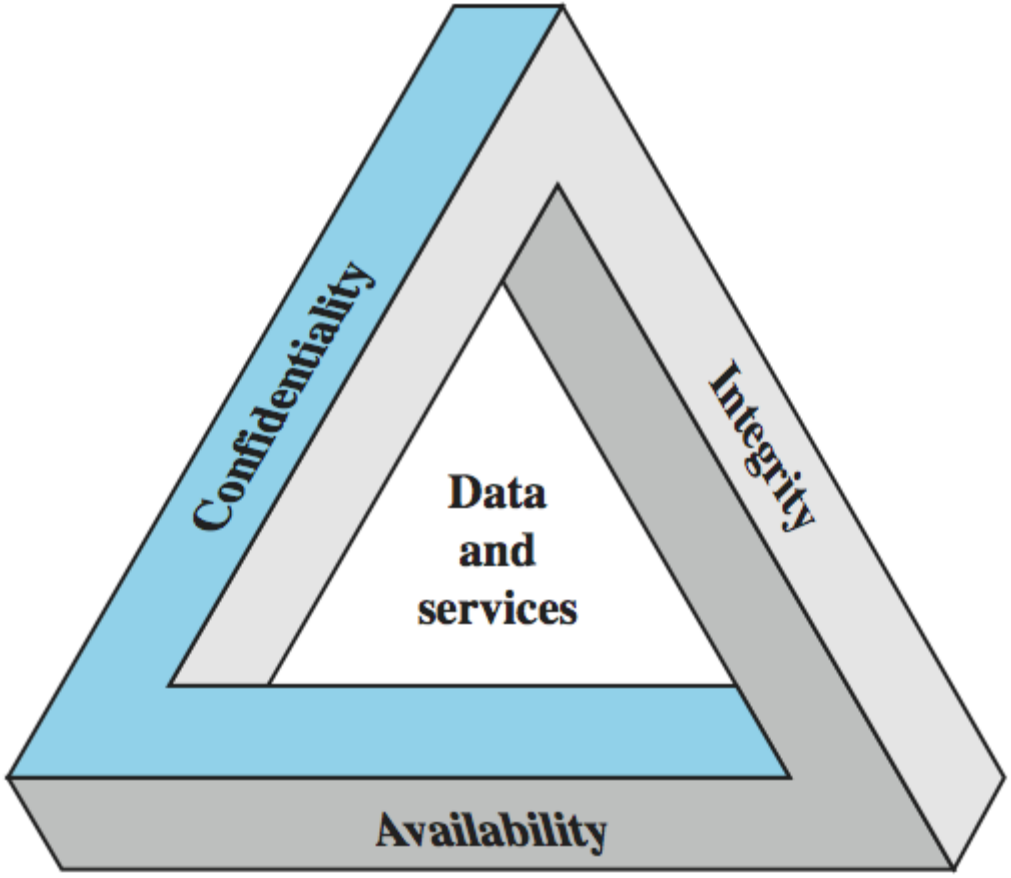
  — On War, Carl Von Clausewitz

Ασφάλεια Υπολογιστών

Η προστασία παρέχεται σε ένα πληροφοριακό σύστημα, προκειμένου να επιτευχθούν οι στόχοι:

1. **Εμπιστευτικότητα (Confidentiality)**
   - α. Εμπιστευτικότητα δεδομένων (Data Confidentiality)
   - β. Ιδιωτικότητα (Privacy)
2. **Ακεραιότητα (Integrity)**
   - α. Ακεραιότητα Δεδομένων (Data Integrity)
   - β. Ακεραιότητα Συστήματος (System Integrity)
3. **Διαθεσιμότητα (availability)** των πόρων του πληροφοριακού συστήματος (υλικό, λογισμικό, firmware, δεδομένα, και τηλεπικοινωνίες)

Βασικές Έννοιες Ασφάλειας



Επίπεδα Επιπτώσεων

- Μπορουμε να ορίσουμε 3 επίπεδα επιπτώσεων απο τυχόν παραβίαση της ασφάλειας
  - **Χαμηλό** (διατηρειται η ικανοτητα να επιτελουνται οι βασικες λειτουργιες του οργανισμου)
  - **Μέσο** (σημαντικη υποβαθμιση της ικανοτητας του οργανισμου να φερει σε περας την αποστολη του)
  - **Υψηλό** (απωλεια της ικανοτητας του οργανισμου να φερει σε περας την αποστολη του)

Παραδείγματα Απαιτήσεων Ασφάλειας

- Εμπιστευτικότητα (confidentiality) – βαθμοί μαθητών
- Ακεραιότητα (Integrity) – πληροφορίες ασθενούς
- Διαθεσιμότητα (availability) – υπηρεσία πιστοποίησης αυθεντινότητας

Προκλήσεις Ασφάλειας Υπολογιστών (1/2)

1. Δεν είναι απλή

2. Πρέπει να λαμβάνει υπόψη τις πιθανές απειλές

3. Οι διαδικασίες είναι συχνά φαινομενικα παράδοξες

4. Χρησιμοποιούνται αλγόριθμοι και μυστικές πληροφορίες

5. Πρέπει να αποφασίσουμε που θα αναπτυχθούν οι μηχανισμοί ασφάλειας

Προκλήσεις Ασφάλειας Υπολογιστών (2/2)

6. Ειναι μια πνευματική μάχη ανάμεσα στον επιτιθέμενο και τον διαχειριστη ασφάλειας

7. τα ωφέλη της ασφάλειας δεν γινονται εύκολα αντιληπτά, μέχρι κάποια φορά να αποτύχει.

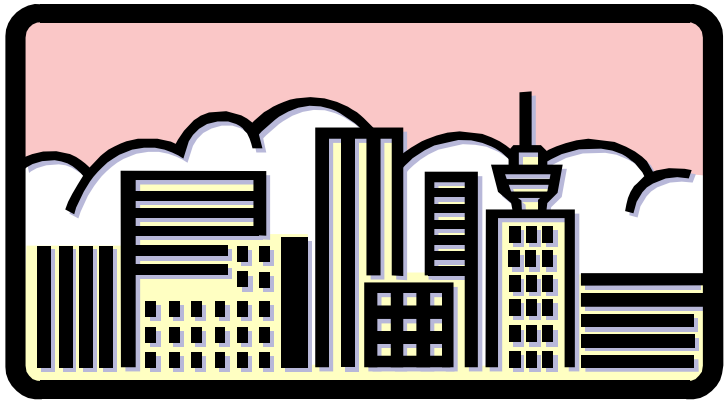
8. Απαιτεί διαρκή παρακολούθηση

9. Συχνά η ασφάλεια ζητείται να εγκατασταθεί σε ένα σύστημα, εκ των υστέρων.

10. Καθιστά τη χρήση του συστήματος δυσκολότερη.

Αρχιτεκτονική Ασφάλειας για το OSI

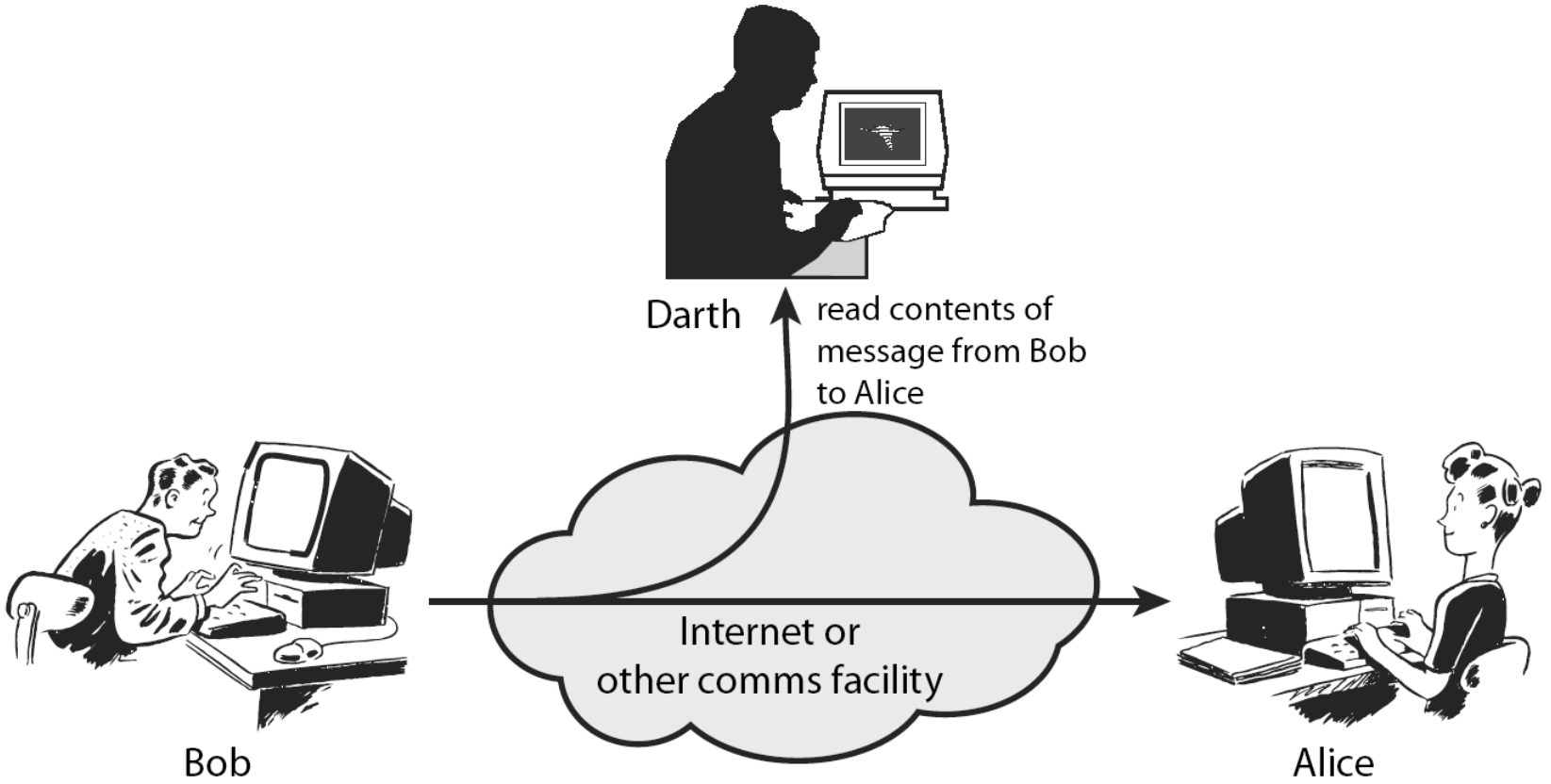
- ITU-T X.800 “Αρχιτεκτονική Ασφάλειας για το OSI”
- Ορίζει ένα συστηματικό τρόπο για τον ορισμό και την παροχή απαιτήσεων ασφάλειας
- Για μας, παρέχει μια χρήσιμη επισκόπιση των θεμάτων που θα μελετήσουμε



Πτυχές της Ασφάλειας

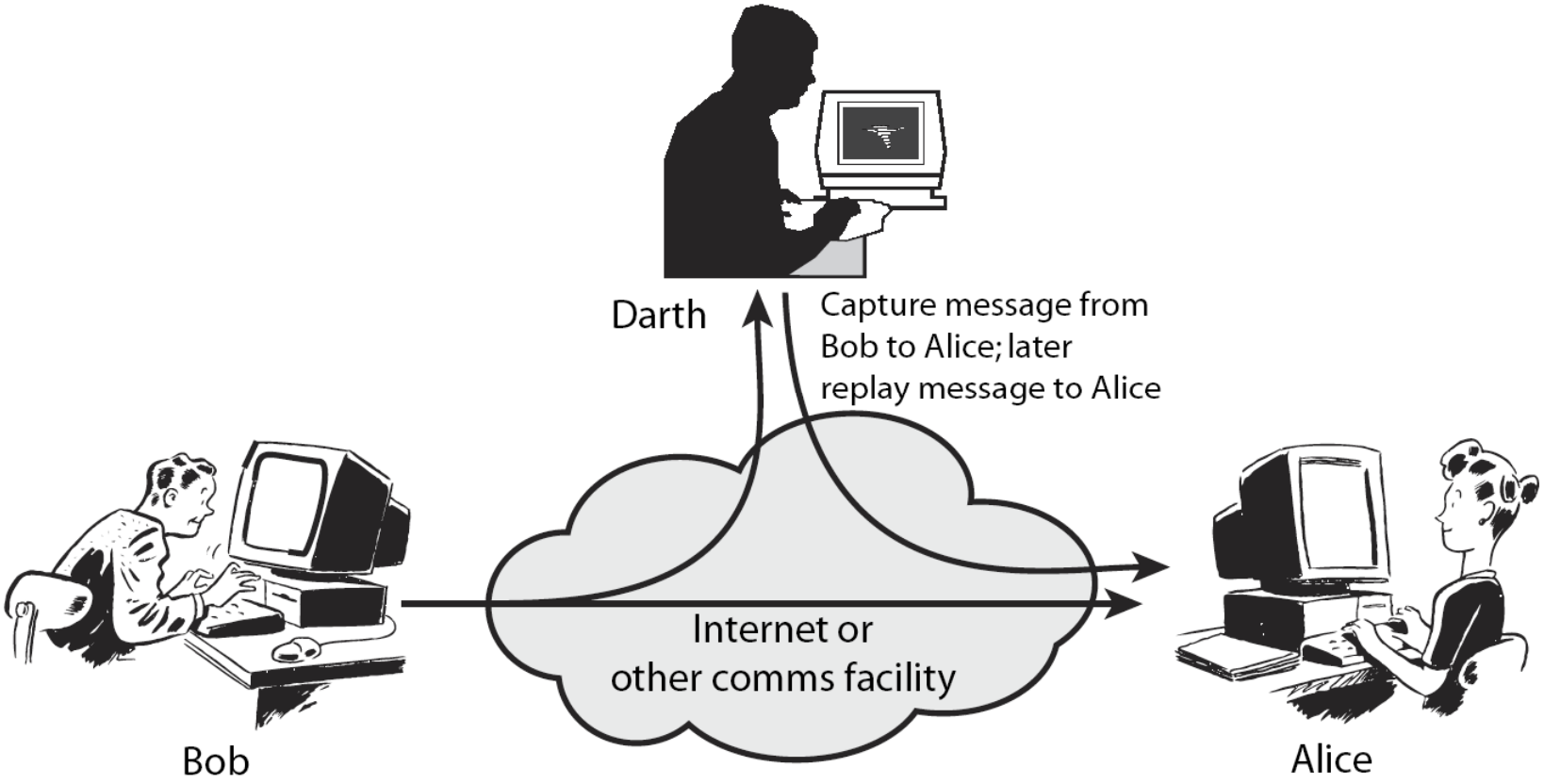
- Θεωρούμε 3 πτυχές της ασφάλειας πληροφοριών:
  - **Επιθέσεις ασφάλειας**
  - **Μηχανισμοί Ασφάλειας**
  - **Υπηρεσίες ασφάλειας (χρησιμοποιουν τους μηχανισμούς)**
- Σημειώστε τους όρους:
  - *Απειλή (threat)* – μια ενδεχόμενη παραβίαση της ασφάλειας
  - *Επίθεση (attack)* – μια προσβολή της ασφάλειας του συστήματος, μια εσκεμμένη προσπάθεια αποφυγής των υπηρεσιών ασφαλείας

Παθητικές Επιθέσεις
(αποκάλυψη περιεχομένου μηνυματος)



Ενεργητικές Επιθέσεις

(masquerade, επανάληψη, τροποποίηση μηνυμάτων, DoS)



Υπηρεσίες Ασφάλειας

- Αυξάνουν την ασφάλεια δεδομένων των συστημάτων επεξεργασίας και της μεταδοσης πληροφοριών σε έναν οργανισμό.
- Αποσκοπούν στην αντιμετώπιση επιθέσεων ασφάλειας
- Χρησιμοποιούν έναν ή περισσότερους μηχανισμούς ασφάλειας
- Συχνά αντικαθιστούν λειτουργίες που κανονικά είναι προσαρτημένες σε φυσικά κείμενα.
  - τα οποία, για παράδειγμα, έχουν υπογραφές, ημερομηνίες, χρειάζονται προστασία από αποκάλυψη, αλλοίωση, ή καταστροφή και χρειάζονται επικύρωση, καταγραφή ή αδειοδότηση.

Υπηρεσίες Ασφάλειας (Security Services)

- X.800:

  “μια υπηρεσία που παρέχεται απο ενα πρωτόκολλο καποιου επιπέδου επικοινωνούντων συστημάτων και εξασφαλίζει την απαραίτητη ασφάλεια των συστημάτων και της μεταφοράς δεδομένων”

- RFC 2828:

  “μια υπηρεσία επεξεργασίας ή επικοινωνίας που παρέχεται από ένα σύστημα για να παράσχει ένα συγκεκριμένο είδος ασφάλειας στους πόρους του συστήματος”

Υπηρεσίες Ασφάλειας (Security Services, X.800)

- **Πιστοποίηση Αυθεντικότητας (Authentication)** – Εξασφάλιση ότι η οντότητα με την οποία επικοινωνούμε είναι αυτή που ισχυρίζεται ότι είναι.
  - Πιστοποίηση Αυθεντικότητας της ομόλογης οντότητας (peer-entity authentication)
  - Πιστοποίηση αυθεντικότητας της προέλευσης των δεδομένων (data origin authentication)

- **Έλεγχος Πρόσβασης (Access Control)** – Πρόληψη της μη εξουσιοδοτημένης χρήσης ενός πόρου του συστήματος.

- **Εμπιστευτικότητα Δεδομένων (Data Confidentiality)** – Προστασία των δεδομένων από μη εξουσιοδοτημένη γνωστοποίησή τους.

- **Ακεραιότητα Δεδομένων (Data Integrity)** – Εξασφάλιση ότι τα δεδομένα που ελήφθησαν είναι όπως στάλθηκαν από μια εξουσιοδοτημένη οντότητα.

- **Μη άρνηση υποχρέωσης ή οφειλής (Non-Repudiation)** – Προστασία έναντι άρνησης της πατρότητας των δεδομένων από μια από τις οντότητες που επικοινωνούν.

- **Διαθεσιμότητα (Availability)** – εξασφάλιση ότι ένας πόρος θα είναι προβάσιμος και διαθέσιμος.

Table 1.2 Security Services (X.800)

AUTHENTICATION	DATA INTEGRITY
The assurance that the communicating entity is the one that it claims to be.	The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
Peer Entity Authentication Used in association with a logical connection to provide confidence in the identity of the entities connected.	**Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
Data-Origin Authentication In a connectionless transfer, provides assurance that the source of received data is as claimed.	**Connection Integrity without Recovery** As above, but provides only detection without recovery.
ACCESS CONTROL	**Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).	**Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
DATA CONFIDENTIALITY	**Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.
The protection of data from unauthorized disclosure.	**NONREPUDIATION**
Connection Confidentiality The protection of all user data on a connection.	Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
Connectionless Confidentiality The protection of all user data in a single data block	**Nonrepudiation, Origin** Proof that the message was sent by the specified party.
Selective-Field Confidentiality The confidentiality of selected fields within the user data on a connection or in a single data block.	**Nonrepudiation, Destination** Proof that the message was received by the specified party.
Traffic-Flow Confidentiality The protection of the information that might be derived from observation of traffic flows.	

Μηχανισμός Ασφάλειας (Security Mechanism)

- Χαρακτηριστικό σχεδιασμένο για να ανιχνεύει ή να αποτρέπει μια επίθεση ή να εξασφαλίζει την ανάνηψη από αυτήν.
- Κανένας μηχανισμός δεν υποστηρίζει ΟΛΕΣ τις υπηρεσίες ασφάλειας που απαιτούνται.
- Ωστόσο ένα συγκεκριμένο στοιχείο αποτελεί τη βάση πολλών από τους μηχανισμούς ασφάλειας που χρησιμοποιούνται:
  - **Οι τεχνικές κρυπτογράφησης**
- Θα εστιάσουμε λοιπόν σε αυτές.

Μηχανισμοί Ασφάλειας (Security Mechanisms, X.800) 1/2

- Συγκεκριμένοι μηχανισμοί ασφάλειας (specific security mechanisms):
  - Κρυπτογράφηση (encipherment)
  - Ψηφιακές Υπογραφές (digital signatures)
  - Έλεγχοι πρόσβασης (access controls)
  - Ακεραιότητα Δεδομένων (data integrity)
  - Ανταλλαγή αυθεντικότητας (authentication exchange)
  - traffic padding,
  - Έλεγχος Δρομολόγησης (routing control)
  - Επισημοποίηση (notarization)

Μηχανισμοί Ασφάλειας (Security Mechanisms, X.800) 2/2

- Διάχυτοι Μηχανισμοί Ασφάλειας (Pervasive Security Mechanisms):
  - Έμπιστη Λειτουργικότητα (trusted functionality)
  - Επικεφαλίδες Ασφάλειας (security labels)
  - Ανίχνευση Γεγονότων (event detection)
  - Ίχνη Ελέγχου Ασφάλειας (security audit trails)
  - Ανάκτηση Ασφάλειας (security recovery)

Table 1.3 Security Mechanisms (X.800)

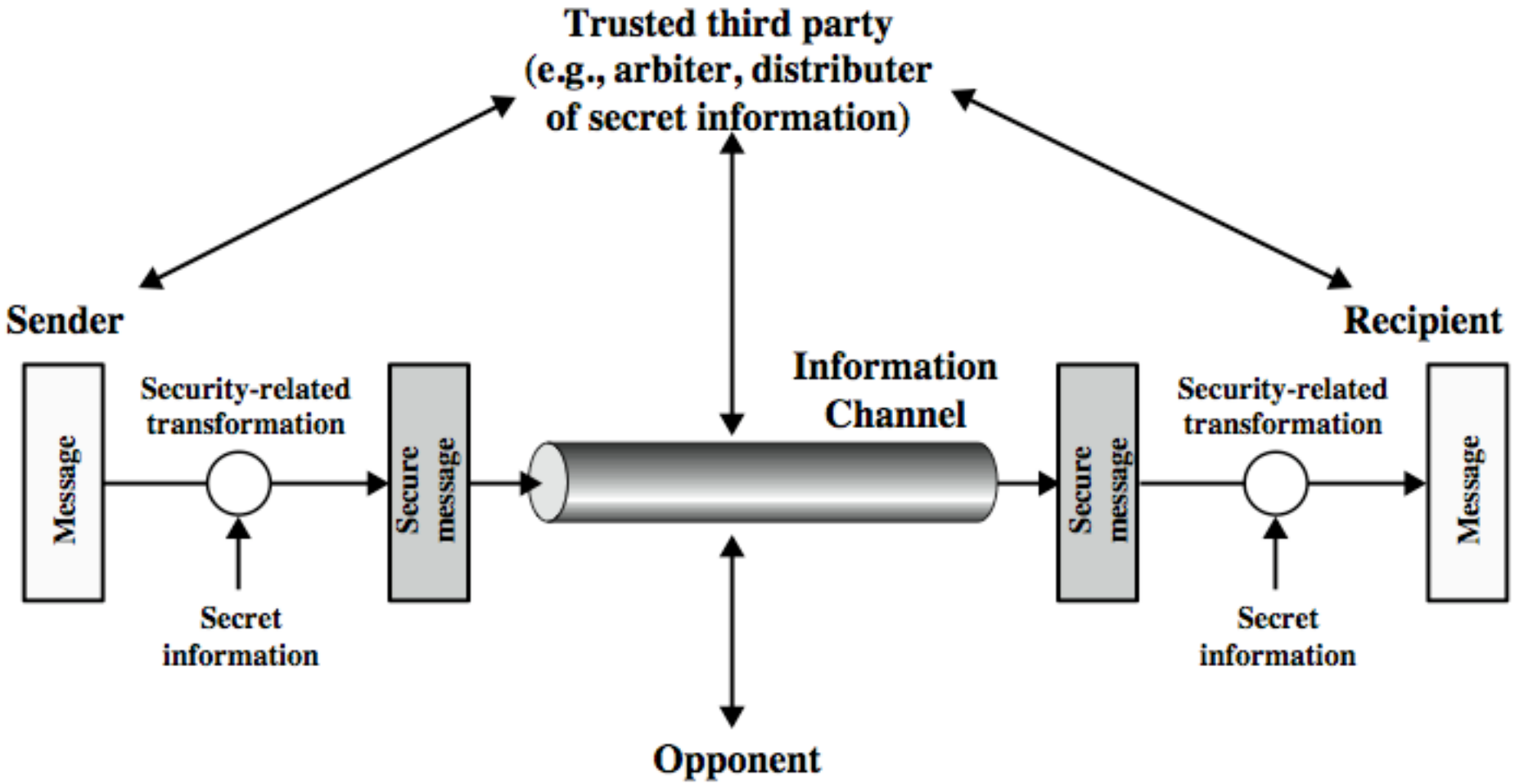
SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

Σχέση μεταξύ υπηρεσιών και μηχανισμών Ασφάλειας

Table 1.4 Relationship Between Security Services and Mechanisms

	Mechanism							
Service	**Enciph-erment**	**Digital signature**	**Access control**	**Data integrity**	**Authenti-cation exchange**	**Traffic padding**	**Routing control**	**Notari-zation**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Πρότυπο για Ασφάλεια Δικτύου



Πρότυπο για Ασφάλεια Δικτύου

Η χρήση αυτού του προτύπου απαιτεί:

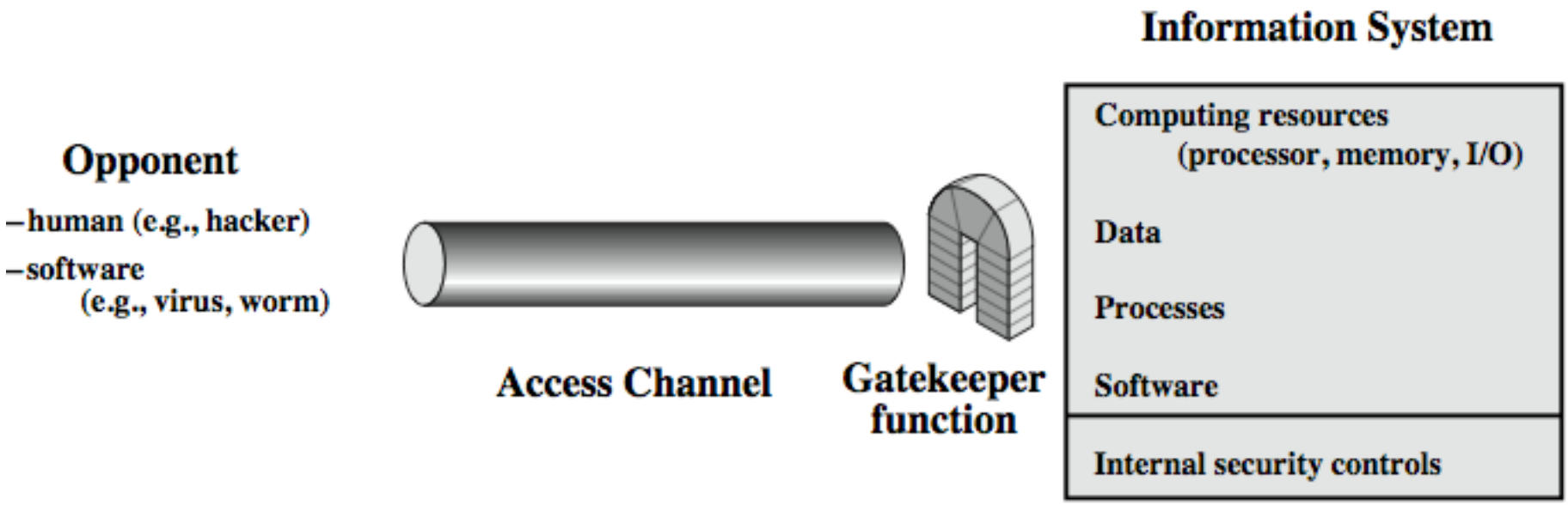
1. Τη χρήση ενός κατάλληλου (κρυπτογραφικού) αλγορίθμου για το μετασχηματισμό ασφάλειας

2. Τη δημιουργία μυστικής πληροφορίας (κλειδιών) που θα χρησιμοποιηθεί από τον παραπάνω αλγόριθμο

3. Την ανάπτυξη μεθόδων για τη διανομή και το διαμοιρασμό της της παραπάνω μυστικής πληροφορίας.

4. Τον ορισμό ενός πρωτοκόλλου που επιτρέπει στους χρήστες του να χρησιμοποιούν τον παραπάνω μετασχηματισμό και τη μυστική πληροφορία για την υλοποίηση μιας υπηρεσίας ασφάλειας.

Πρότυπο Για Ασφάλεια Πρόσβασης στο Δίκτυο (Network Access Security)



Πρότυπο
για Ασφάλεια Πρόσβασης στο Δίκτυο

- Η χρήση αυτού του μοντέλου απαιτεί:

1. Την επιλογή των κατάλληλων gatekeeper functions για τον προσδιορισμό των χρηστών

2. Την υλοποίηση ελέγχων ασφάλειας για να επιβεβαιώσουμε ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση σε συγκεκριμένες πληροφορίες ή πόρους.

Περίληψη

- Περιεχόμενα
- Οργανισμοί προτύπων ασφάλειας
- Θέματα Ασφάλειας:
  - Εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα
- Η Αρχιτεκτονική Ασφαλειας Χ.800
- Επιθέσεις Ασφάλειας, Υπηρεσίες και Μηχανισμοί Ασφάλειας
- Πρότυπα για Ασφάλεια Δικτύων