Information Systems And Network Security

Chapter-07

Security Attacks

Security Services

Security Mechanisms

Model of Network security

-Sanket Mohan Pandhare

What security is about in general?

- Security is about protection of assets
  - D. Gollmann, Computer Security, Wiley
- Prevention
  - take measures that prevent your assets from being damaged (or stolen)
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction
  - take measures so that you can recover your assets

Real world example

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard
- Detection
  - missing items, burglar alarms, closed circuit TV(CCTV) Cameras
- Reaction
  - attack on burglar, call the police, replace stolen items, make an insurance claim

Internet shopping example

- Prevention
  - encrypt your order and card number, enforce merchants to do some extra checks, using PIN even for Internet transactions, don’t send card number via Internet
- Detection
  - an unauthorized transaction appears on your credit card statement
- Reaction
  - complain, dispute, ask for a new card number, sue
  - Or, pay and forget

Information security in past & present

- Traditional Information Security
  - keep the cabinets locked
  - put them in a secure room
  - human guards
  - electronic surveillance systems
  - in general: physical and administrative mechanisms
- Modern World
  - Data is in computers
  - Computers are interconnected

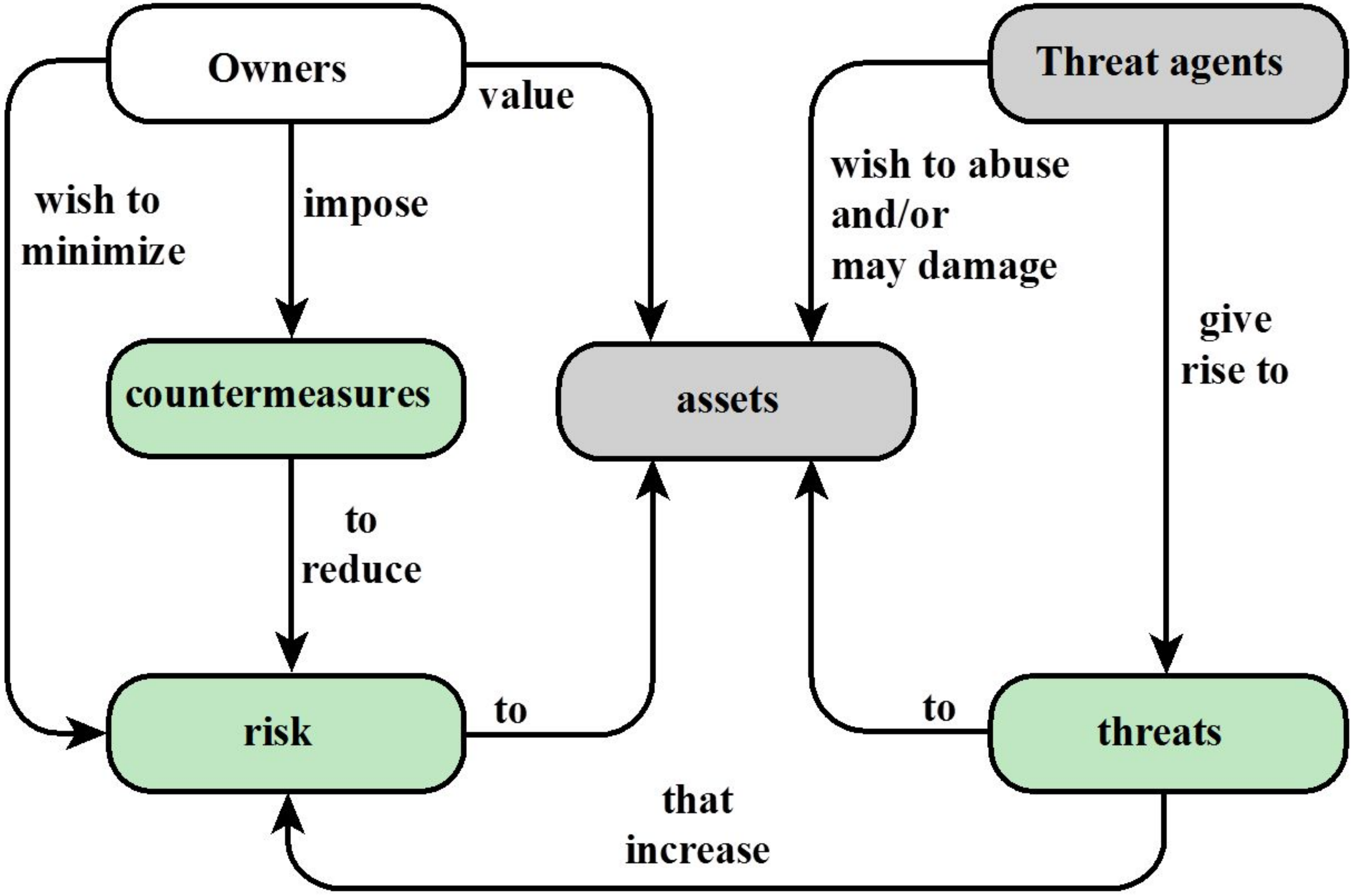
Terminology

- Computer Security
  - 2 main focuses: Information and Computer itself
  - tools and mechanisms to protect data in a computer (actually an automated information system), even if the computers/system are connected to a network
  - tools and mechanisms to protect the information system itself (hardware, software, firmware, *ware ☺)
- Against?
  - against hackers (intrusion)
  - against viruses
  - against denial of service attacks
  - etc. (all types of malicious behavior)

Terminology

- Network and Internet Security
  - measures to prevent, detect, and correct security violations that involve the transmission of information in a network or interconnected networks

Relationships among the security Concepts



Owners

value

wish to minimize

impose

Threat agents

wish to abuse and/or may damage

give rise to

countermeasures

assets

to reduce

risk

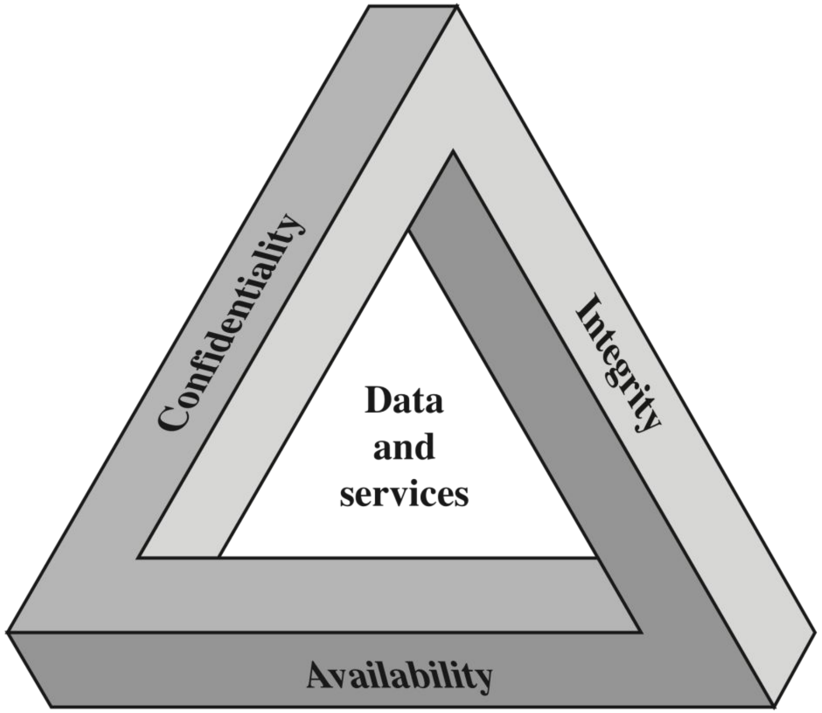
to

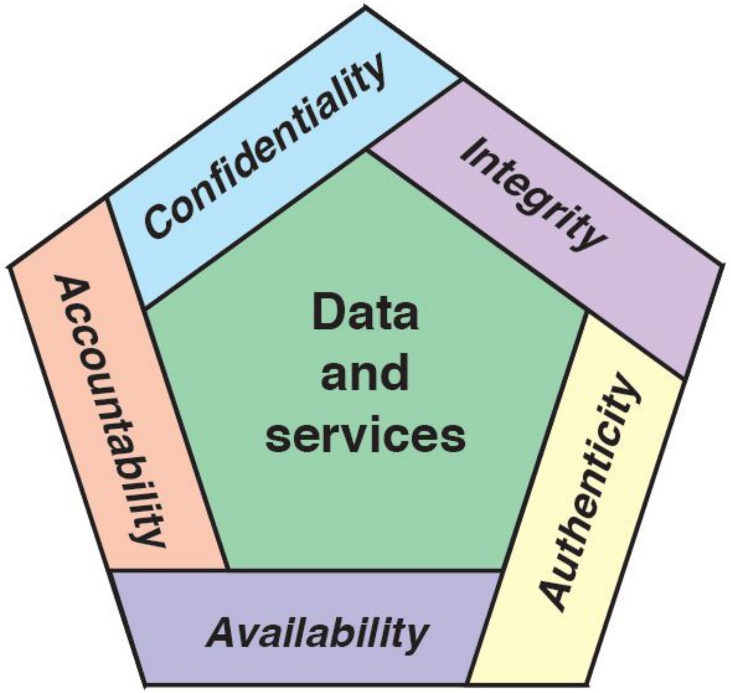
to

threats

that increase

Security Objectives: CIA Triad and Beyond





Additional concepts:

Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- Being able to trace the responsible party/process/entity in case of a security incident or action.

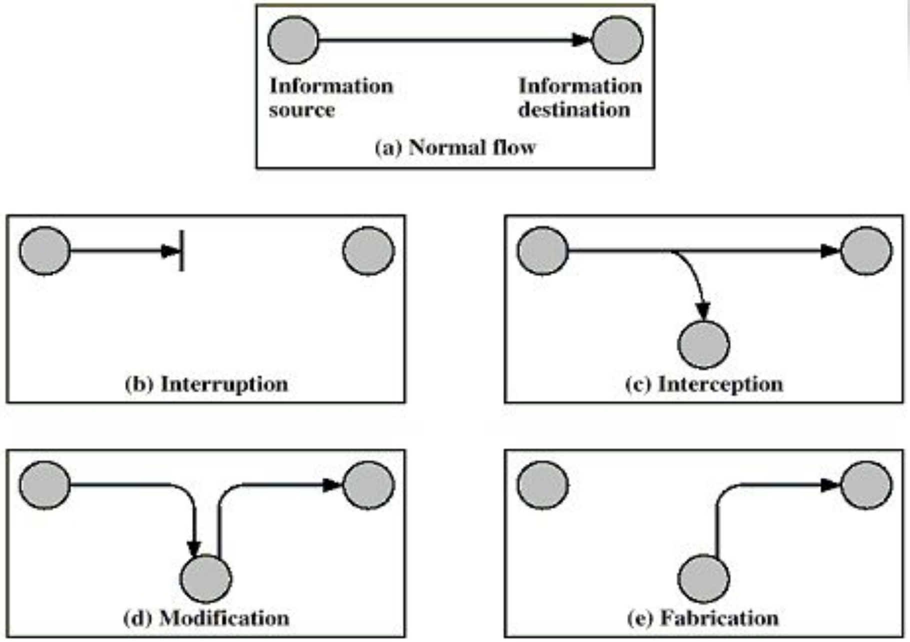
Attacks, Services, Mechanisms

- 3 aspects of information security:
  - security attacks (and threats)
    - actions that (may) compromise security
  - security services
    - services counter to attacks
  - security mechanisms
    - used by services
    - e.g. secrecy is a security service, encryption (a.k.a. encipherment) is a security mechanism

Attacks

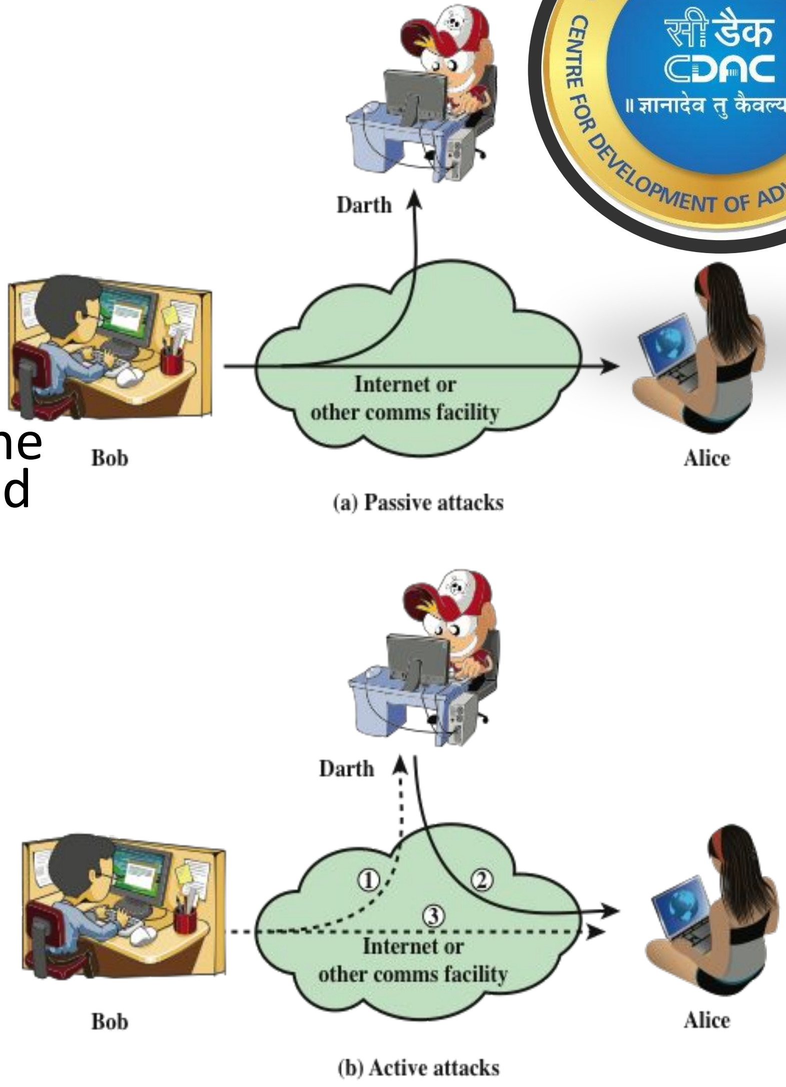
- Attacks on computer systems
  - break-in to destroy information
  - break-in to steal information
  - blocking to operate properly
  - malicious software

- Source of attacks
  - Insiders
  - Outsiders



Attacks

- Network Security
  - Active attacks
  - Passive attacks
- Passive attacks
- A **passive attack** is characterized by the interception of messages without modification. There is no change to the network data or systems. The message itself may be read or its occurrence may simply be logged.
- interception of the messages
- What can the attacker do?
  - use information internally
    - hard to understand
    - release the content
      - can be understood
    - traffic analysis
      - hard to avoid
  - Hard to detect, try to prevent



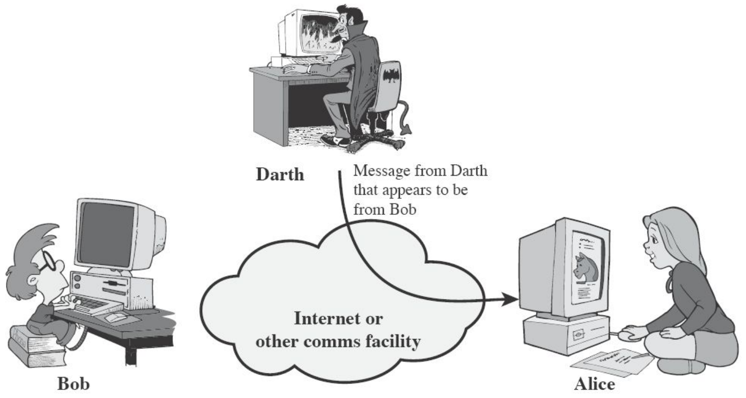
(a) Passive attacks

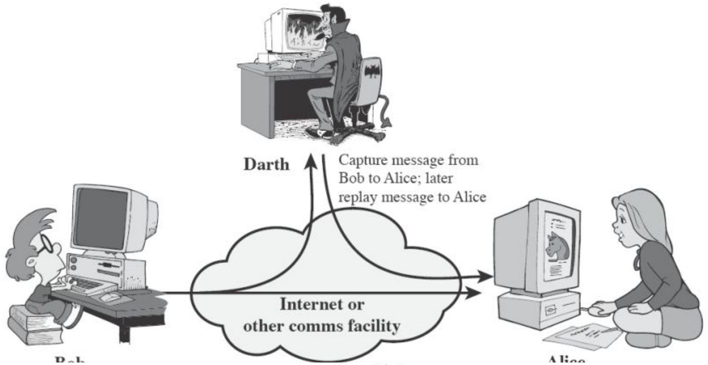
(b) Active attacks

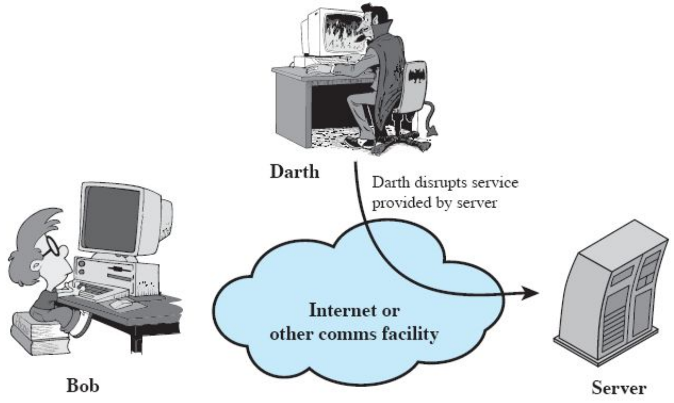
Figure 1.2 Security Attacks

Attacks

- Active attacks
  - Attacker actively manipulates the communication
  - Masquerade
    - pretend as someone else
    - possibly to get more privileges
  - Replay
    - passively capture data and send later
  - Denial-of-service
    - prevention the normal use of servers, end users, or network itself

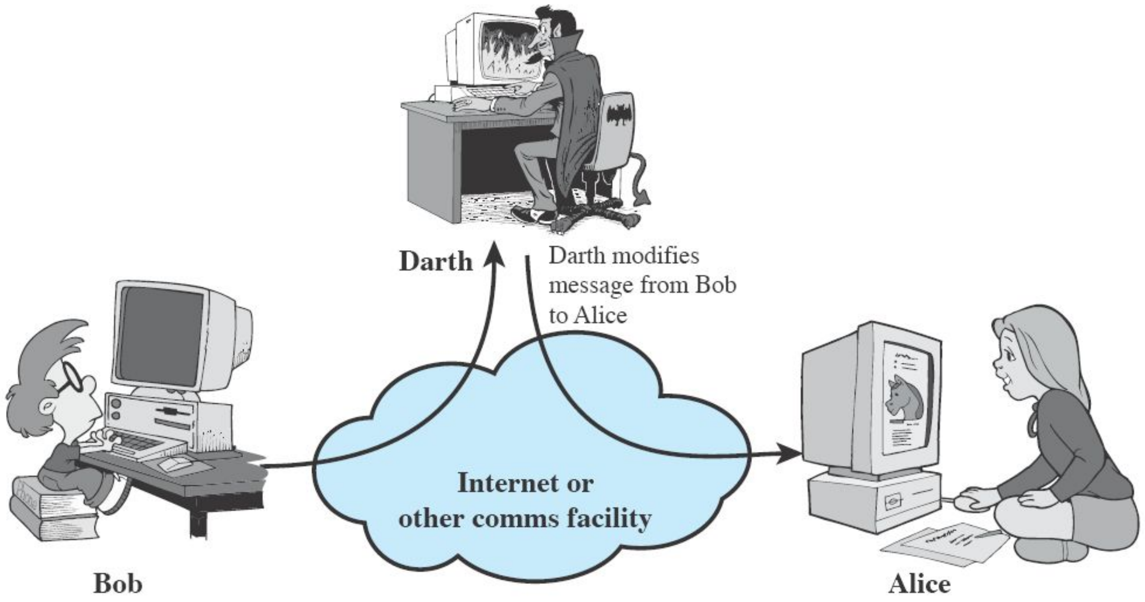

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

Attacks

- Active attacks (cont’d)
  - modification
    - change the content of a message


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Security Services

- to prevent or detect attacks
- to enhance the security
- replicate functions of physical documents
  - e.g.
    - have signatures, dates
    - need protection from disclosure, tampering, or destruction
    - notarize
    - record

Basic Security Services

- Authentication
  - assurance that the communicating entity is the one it claims to be
  - peer entity authentication
    - mutual confidence in the identities of the parties involved in a connection
  - Data-origin authentication
    - assurance about the source of the received data
- Access Control/Authorization
  - prevention of the unauthorized use of a resource
  - to achieve this, each entity trying to gain access must first be identified and authenticated, so that access rights can be tailored to the individual

Basic Security Services

- Data Confidentiality
  - protection of data from unauthorized disclosure
  - traffic flow confidentiality is one step ahead
    - this requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility
- Data Integrity
  - assurance that data received are exactly as sent by an authorized sender
  - i.e. no modification, insertion, deletion, or replay

Basic Security Services

- Non-Repudiation
  - Protection against denial by one of the parties in a communication
  - Origin non-repudiation
    - proof that the message was sent by the specified party
  - Destination non-repudiation
    - proof that the message was received by the specified party

Security Mechanisms

- Cryptographic Techniques
- Software and hardware for access limitations
  - Firewalls
- Intrusion Detection and Prevention Systems
- Traffic Padding
  - against traffic analysis
- Hardware for authentication
  - Smartcards, security tokens
- Security Policies / Access Control
  - define who has access to which resources.
- Physical security
  - Keep it in a safe place with limited and authorized physical access

Cryptographic Security Mechanisms

- Encryption (a.k.a. Encipherment)
  - use of mathematical algorithms to transform data into a form that is not readily intelligible
    - keys are involved
  - Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.
  - While for asymmetric encryptions RSA, DSA, Elliptic curve techniques, PKCS are widely used algorithms.

Cryptographic Security Mechanisms

- Digital Signatures and Message Authentication Codes
  - Data appended to, or a cryptographic transformation of, a data unit to prove the source and the integrity of the data
- Authentication Exchange
  - ensure the identity of an entity by exchanging some information

Security Mechanisms

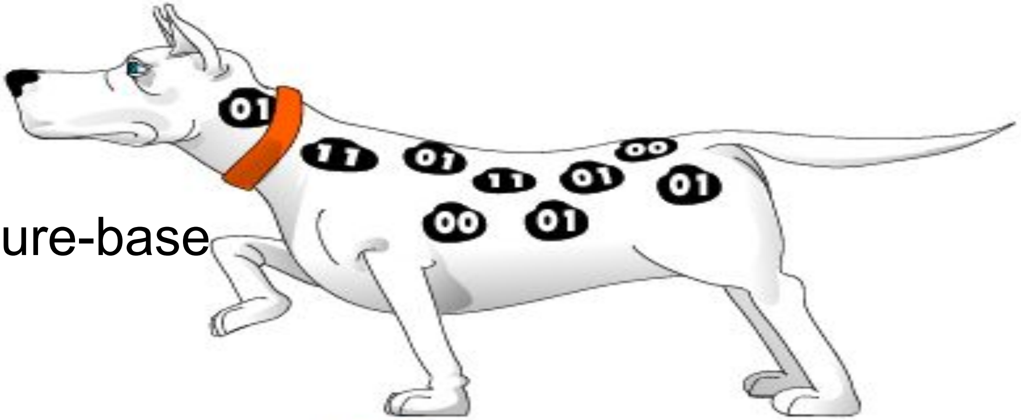
- Notarization
  - use of a trusted third party to assure certain properties of a data exchange
- Timestamping
  - inclusion of correct date and time within messages

Intrusion Detection Systems

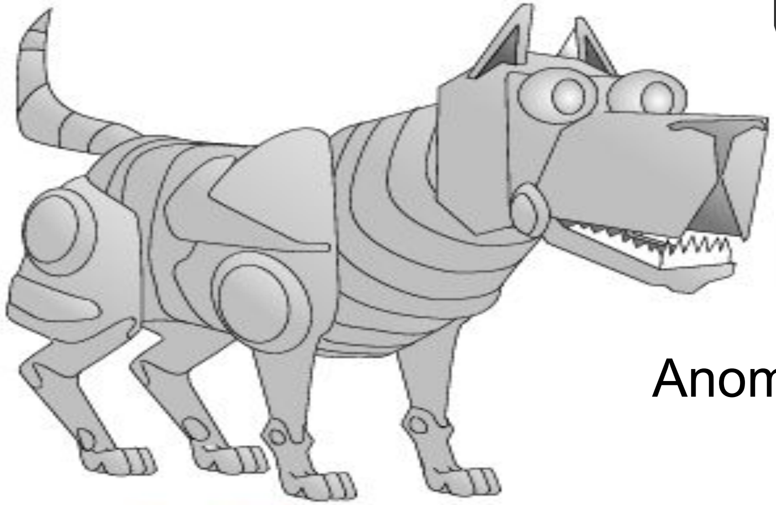
- Firewalls allow traffic only to legitimate hosts and services
- Traffic to the legitimate hosts/services can have attacks

- Solution?
  - Intrusion Detection Systems
  - Monitor data and behavior
  - Report when identify attacks

Types of IDS



Signature-based



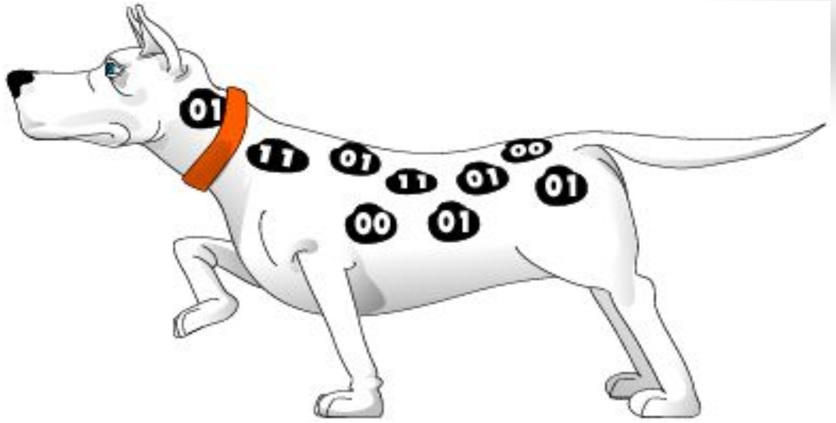
Anomaly-based

Host-based

Network-based

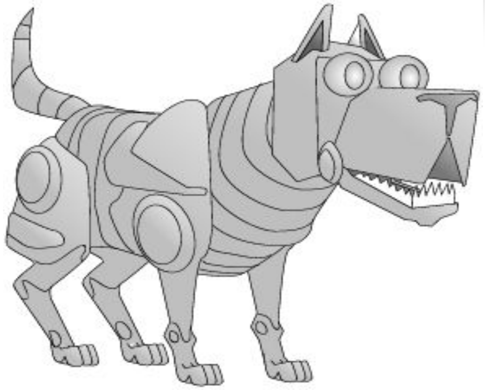
Signature-based IDS

- Characteristics
  - Uses known pattern matching to signify attack
- Advantages?
  - Widely available
  - Fairly fast
  - Easy to implement
  - Easy to update
- Disadvantages?
  - Cannot detect attacks for which it has no signature



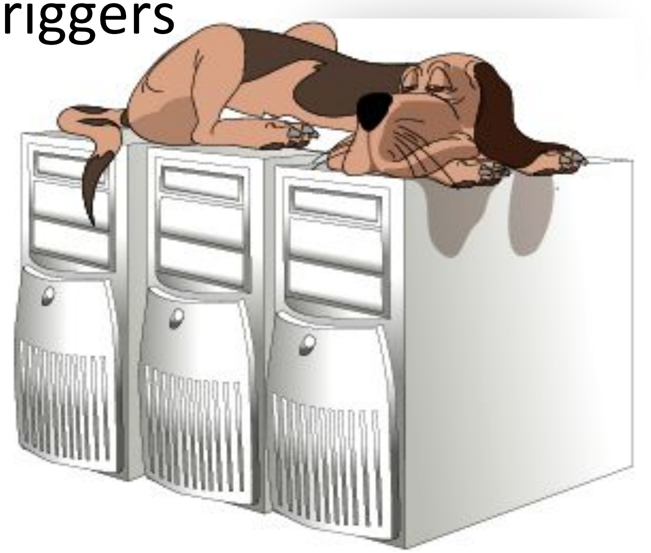
Anomaly-based IDS

- Characteristics
  - Uses statistical model or machine learning engine to characterize normal usage behaviors
  - Recognizes departures from normal as potential intrusions
- Advantages?
  - Can detect attempts to exploit new and unforeseen vulnerabilities
  - Can recognize authorized usage that falls outside the normal pattern
- Disadvantages?
  - Generally slower, more resource intensive compared to signature-based IDS
  - Greater complexity, difficult to configure
  - Higher percentages of false alerts



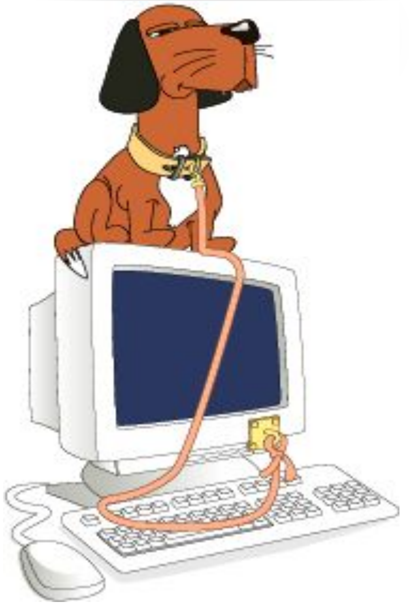
Network-based IDS

- Characteristics
  - NIDS examine raw packets in the network passively and triggers alerts
- Advantages?
  - Easy deployment
  - Can deploy at low level of network operation
- Disadvantages?
  - Different hosts process packets differently
  - NIDS needs to create traffic seen at the end host

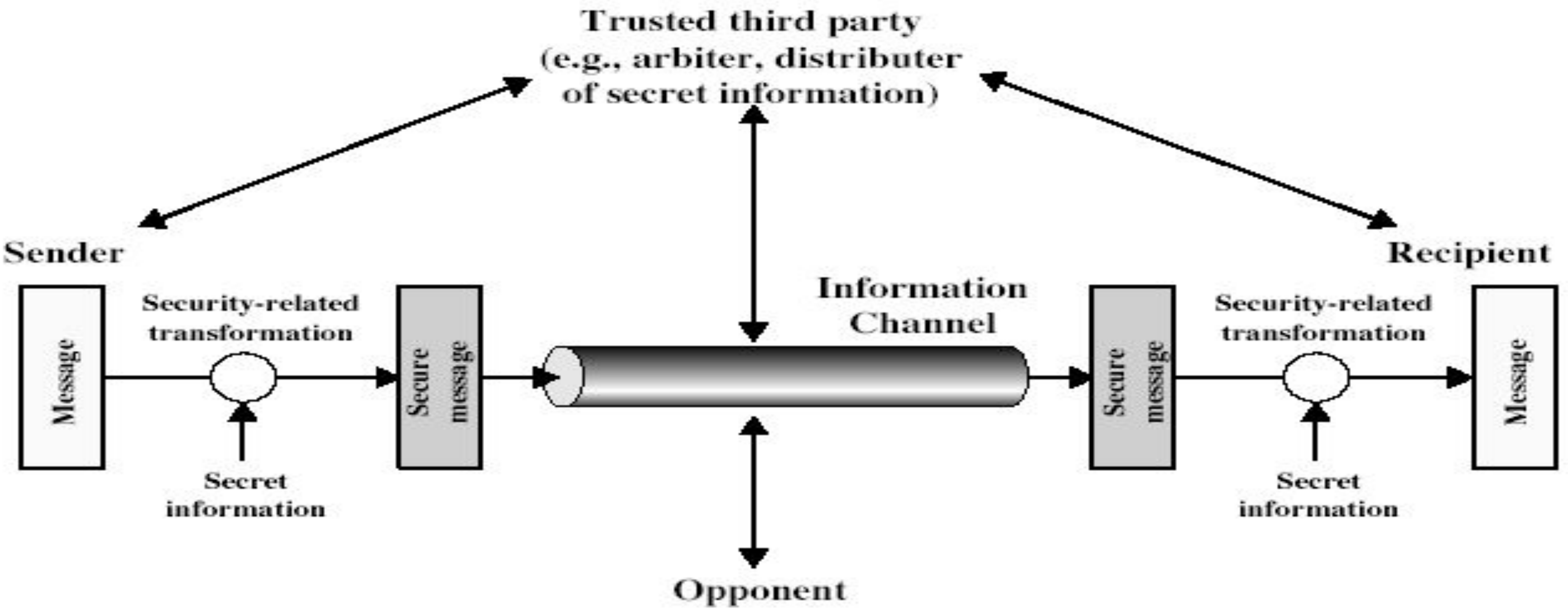


Host-based IDS

- Characteristics
  - Runs on single host
  - Can analyze audit-trails, logs, integrity of files and directories, etc.
- Advantages
  - More accurate than NIDS
  - Less volume of traffic so less overhead
- Disadvantages
  - Deployment is expensive
  - What happens when host get compromised?



A General Model for Network Security



Description

- A message is to be transferred from one party to another across some sort of internet.
- The two parties, who are the principals in this transaction, must cooperate for the exchange to take place.
- A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

- Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

- A security-related transformation on the information to be sent.
- Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender

Cont.

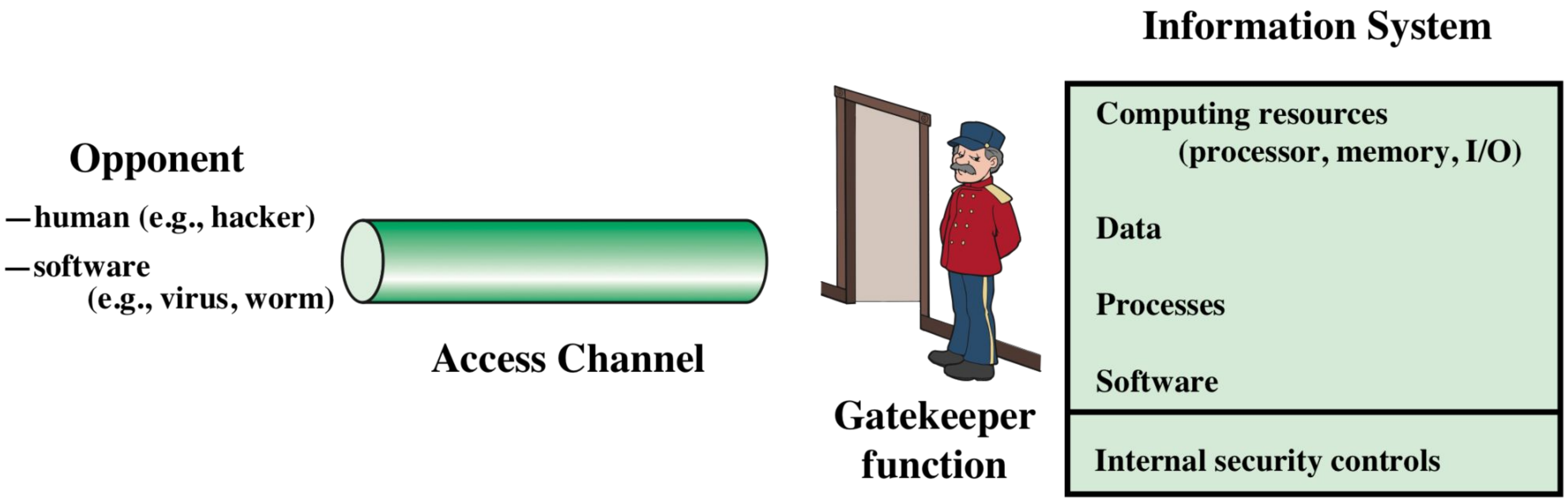
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
- An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.
- public-key encryption, in which only one of the two principals needs to have the secret information.

- A trusted third party may be needed to achieve secure transmission.
- For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.
- Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Opponent

— human (e.g., hacker)

— software (e.g., virus, worm)

Access Channel

Gatekeeper function

Information System

Computing resources (processor, memory, I/O)

Data

Processes

Software

Internal security controls

Figure 1.3 Network Access Security Model

Description

- The second model is concerned with controlled access to information or resources on a computer system, in the presence of possible opponents. Here appropriate controls are needed on the access and within the system, to provide suitable security.

- This diagram reflects a concern for protecting an information system from unwanted access.

- We are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. Or, the intruder can be a disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).

- Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers

Cont.

- Service threats exploit service flaws in computers to inhibit use by legitimate users.
- Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a risk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

- The security mechanisms needed to cope with unwanted access fall into two broad categories (see Figure 1.3). The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access,
- The second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

Model for Network Access Security

- using this model :
  - Appropriate gatekeeper functions to identify users and processes and ensure only authorized users and processes access designated information or resources
  - Internal control to monitor the activity and analyze information to detect unwanted intruders

More on Computer System Security

- Based on “Security Policies”
  - Set of rules that specify
    - How resources are managed to satisfy the security requirements
    - Which actions are permitted, which are not
  - Ultimate aim
    - Prevent security violations such as unauthorized access, data loss, service interruptions, etc.
  - Scope
    - Organizational or Individual
  - Implementation
    - Partially automated, but mostly humans are involved
  - Assurance and Evaluation
    - Assurance: degree of confidence to a system
    - Security products and systems must be evaluated using certain criteria in order to decide whether they assure security or not

Aspects of Computer Security

- Mostly related to Operating Systems
- Similar to those discussed for Network Security
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability

Aspects of Computer Security

- Confidentiality
  - Prevent unauthorized disclosure of information
  - Synonyms: Privacy and Secrecy
- Integrity
  - two types: data integrity and system integrity
  - In general, “make sure that everything is as it is supposed to be”
  - More specifically, “no unauthorized modification, deletion” on data (data integrity)
  - System performs as intended without any unauthorized manipulations (system integrity)

Aspects of Computer Security

- Availability
  - Services should be accessible when needed and without extra delay
- Accountability
  - Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party
  - How can we do that?
    - Users have to be **identified** and **authenticated** to have a basis for access control decisions and to find out responsible party in case of a violation.
    - The security system keeps an **audit log (audit trail)** of security relevant events to detect and investigate intrusions.

Attack Surfaces

- An attack surface consists of the reachable and exploitable vulnerabilities in a system
- Examples:
  - Open ports on outward facing Web and other servers, and code listening on those ports
  - Services available in a firewall
  - Code that processes incoming data, email, XML, office documents, etc.
  - Interfaces and Web forms
  - An employee with access to sensitive information

Attack Surface Categories

- Network attack surface
  - Refers to vulnerabilities over an enterprise network, wide-area network, or the Internet
    - E.g. DoS, intruders exploiting network protocol vulnerabilities
- Software attack surface
  - Refers to vulnerabilities in application, utility, or operating system code
- Human attack surface
  - Refers to vulnerabilities created by personnel or outsiders
  - E.g. social engineering, insider traitors

OSI Security architecture

- To assess effectively the security needs of an organization

and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.

- The OSI security architecture was developed in the context of the OSI protocol architecture.
- The OSI security architecture provides a useful, if abstract, overview of many of the concepts..

Cont.

- The OSI security architecture focuses on security attacks, mechanisms, and services.
  - Security attack – Any action that compromises the security of information owned by an organization.
  - Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.
  - Security service – A service that enhances the security of the data processing systems and the information transfers of an organization.
- The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

Summary

- Prevention-Detection-Action/Reaction
- Security Attacks
  - Passive Attacks
  - Active Attacks
- Security Services
- Security Mechanism
- A General Model for Network Security
- Model for Network Access Security
- Attack Surface