Information Security
CS 3002

Dr. Haroon Mahmood

Assistant Professor

NUCES Lahore

Haroon Mahmood
Ph.D. in Computer and Control Engineering
Politecnico di Torino, Italy

PhD Thesis

Multi-criteria Optimization for Energy-Efficient Multi-Core Systems-on-chip

- Aging-aware power-efficient cache memory design
- Aging, Power and performance Optimization

MS Thesis

Validation Issues in Federated Identity Management System

- Cross domain certificate validation in multi-domain environment
- Centralization of trust management across countries
- STORK (Secure Identity Across Borders Linked)

Research Interest

- Internet of Things Security and Reliability
- Security Auditing and vulnerability analysis of IoT devices
- Intrusion detection Systems
- Digital Forensics
- Differential Privacy
- Mobility modeling for UAVs
- Software Defined Networking
- Blockchain

Research grant

Title	Funding Agency	Role	Grant Amount	Duration
IoT security Lab to develop security audit tool for IoT systems	Planning Commission of Pakistan	Co-PI	~ 92 Million PKR Rupees	Sep 18-July 21

Aim of the course

This course serves as a comprehensive overview to the field of information security at senior undergraduate level.

At the end of the course the students will be able to:

1. **Explain key concepts of information security such as design principles, cryptography, risk management, and ethics**
2. **Discuss legal, ethical, and professional issues in information security**
3. **Apply various security and risk management tools for achieving information security and privacy**
4. **Identify appropriate techniques to tackle and solve problems in the discipline of information security**

Course contents

- Introduction to Information Security
- Security design principles
- Security mechanisms including symmetric and asymmetric cryptography, encryption, hash functions, digital signatures
- Key management, authentication and access control
- Software security, vulnerabilities and protections
- Malware
- Database security
- Network security
- Firewalls
- Intrusion detection
- Security policies, policy formation and enforcement

Course Contents (cont.)

- Risk assessment
- Cybercrime
- Law and ethics in information security
- Privacy and anonymity of data
- Digital Forensics

Course Textbooks

- **Computer Security: Principles and Practice by William Stallings**
- **Official (ISC)2 Guide to the CISSP CBK**

Additional references and books related to the course:

- **Principles of Information Security, 6th edition by M. Whitman and H. Mattord**
- **Computer Security, 3rd edition by Dieter Gollmann**
- **Computer Security Fundamentals, 3rd edition by William Easttom**
- **Research papers**

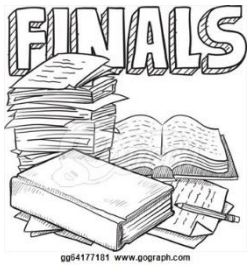
Marks Distribution

Quizzes 10%

Assignments/Labs 10%

Project Presentation 10%

Midterm 25-30%



40-45%

What is Security?

- **"The quality or state of being secure—to be free from danger"**
- **A well secured organization should have multiple layers of security in place:**
  - **Physical security**
  - **Personal security**
  - **Operations security**
  - **Communications security**
  - **Network security**

Information Security

- **The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information**
- **Necessary tools: policy, awareness, training, education, technology**
- **C.I.A. triangle was standard based on confidentiality, integrity, and availability**
- **C.I.A. triangle now expanded into list of critical characteristics of information**

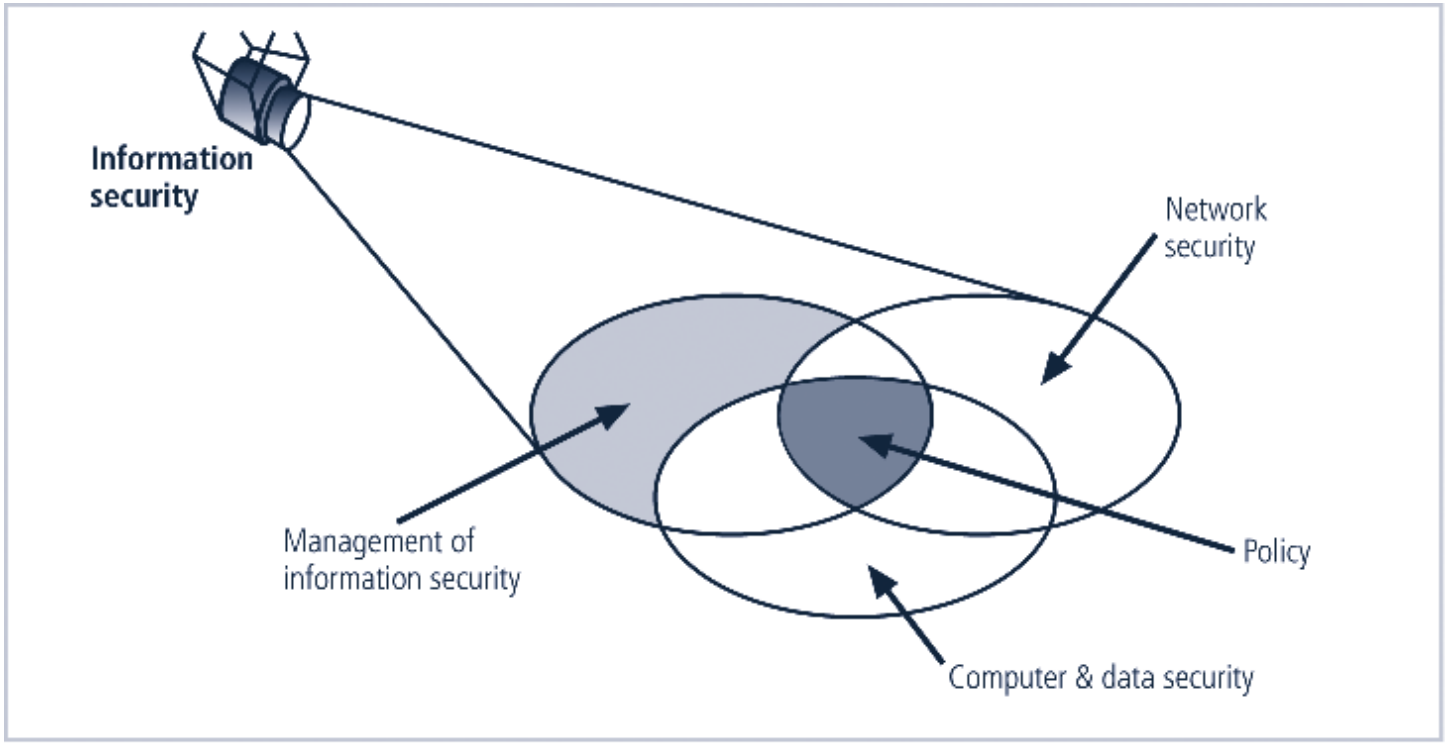


FIGURE 1-3 Components of Information Security

Book: Principles of information Security

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Timeliness
    - No value if it is too late
  - Availability
    - No interference or obstruction
    - Required format
  - Accuracy
    - Free from mistakes
  - Authenticity
    - Quality or state of being genuine, i.e., sender of an email

Critical Characteristics of Information

- **Confidentiality**
  - **Disclosure or exposure to unauthorized individuals or system is prevented**
- **Integrity**
  - **Whole, completed, uncorrupted**
  - **Cornerstone**
  - **Size of the file, hash values, error-correcting codes, retransmission**
- **Possession**
  - **Ownership**
  - **Breach of confidentiality results in the breach of possession**

Components of an Information System

- **Information System (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization**
- **Software**
  - **Perhaps most difficult to secure**
  - **Easy target**
  - **Exploitation substantial portion of attacks on information**
- **Hardware**
  - **Physical security policies**
  - **Securing physical location important**
  - **Laptops**
  - **Flash memory**

Components of an Information System

- Data
  - Often most valuable asset
  - Main target of intentional attacks
- People
  - Weakest link
  - Social engineering
  - Must be well trained and informed
- Procedures
  - Threat to integrity of data
- Networks
  - Locks and keys won't work

Securing Components

- Computer can be subject of an attack and/or the object of an attack
  - When the subject of an attack, computer is used as an active tool to conduct attack
  - When the object of an attack, computer is the entity being attacked
- Types of attack
  - Direct
    - Hacker uses their computer to break into a system
  - Indirect
    - System is compromised and used to attack other systems

Risk estimation

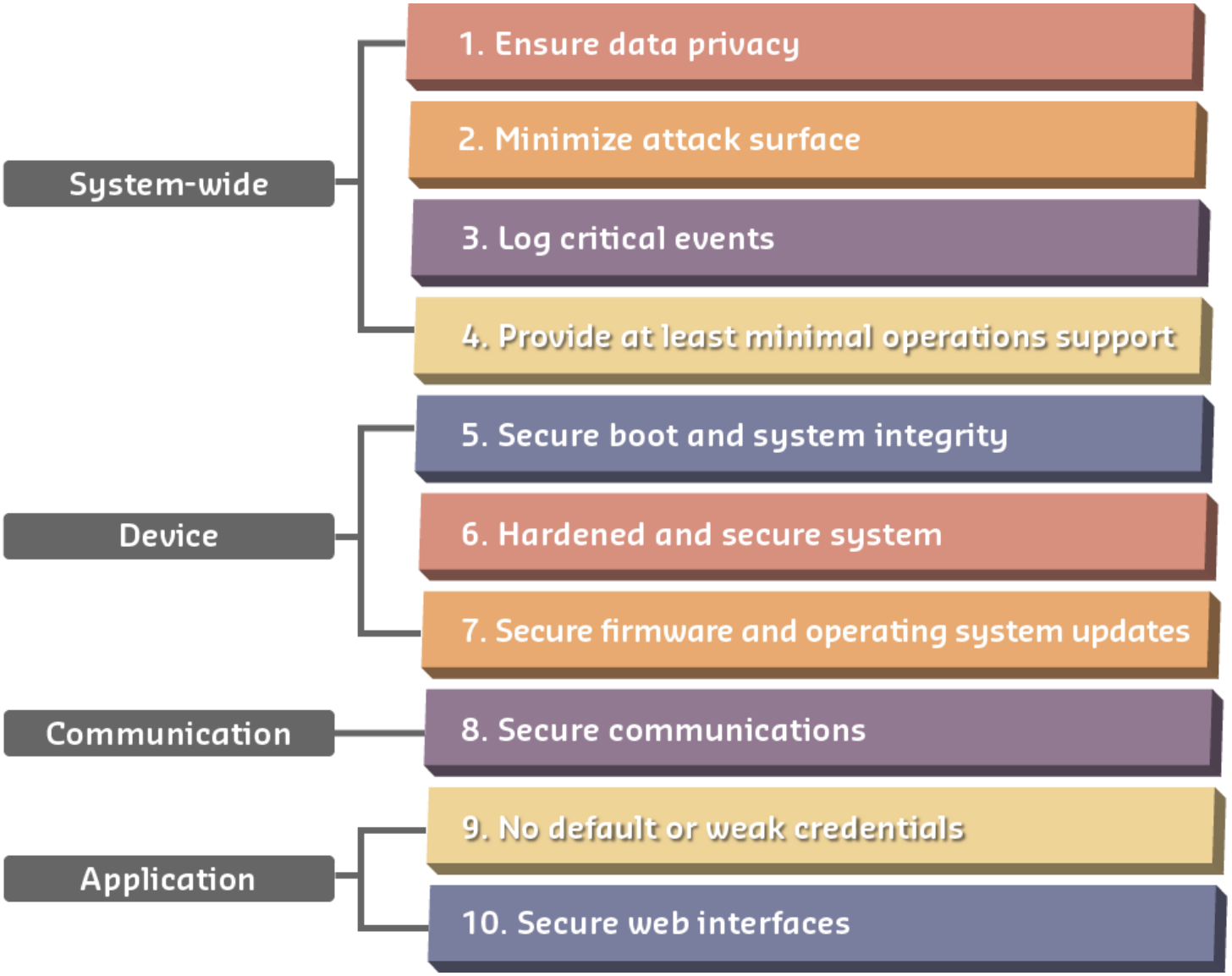
- **Assets:** Objects, data, people
- **Vulnerability:** Weakness of an asset
- **Threat:** loss of security due to vulnerability
- **Attack:** threat occurrence

- **Risk estimation** is the process of identifying vulnerabilities and threats and their impact and probability of occurring an attack.

OWASP top 10 Vulnerabilities

Category	IoT Security Consideration	Recommendations
I1: Insecure Web Interface	•Ensure that any web interface coding is written to prevent the use of weak passwords …	When building a web interface consider implementing lessons learned from web application security. Employ a framework that utilizes security …
I2: Insufficient Authentication/Authorization	•Ensure that applications are written to require strong passwords where authentication is needed …	Refer to the OWASP Authentication Cheat Sheet
I3: Insecure Network Services	•Ensure applications that use network services don't respond poorly to buffer overflow, fuzzing …	Try to utilize tested, proven, networking stacks and interfaces that handle exceptions gracefully...
I4: Lack of Transport Encryption	•Ensure all applications are written to make use of encrypted communication between devices…	Utilize encrypted protocols wherever possible to protect all data in transit…
I5: Privacy Concerns	•Ensure only the minimal amount of personal information is collected from consumers …	Data can present unintended privacy concerns when aggregated…
I6: Insecure Cloud Interface	•Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces) …	Cloud security presents unique security considerations, as well as countermeasures. Be sure to consult your cloud provider about options for security mechanisms…
I7: Insecure Mobile Interface	•Ensure that any mobile application coding is written to disallows weak passwords …	Mobile interfaces to IoT ecosystems require targeted security. Consult the OWASP Mobile …
I8: Insufficient Security Configurability	•Ensure applications are written to include password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication)…	Security can be a value proposition. Design should take into consideration a sliding scale of security requirements…
I9: Insecure Software/Firmware	•Ensure all applications are written to include update capability and can be updated quickly …	Many IoT deployments are either brownfield and/or have an extremely long deployment cycle...
I10: Poor Physical Security	•Ensure applications are written to utilize a minimal number of physical external ports (e.g. USB ports) on the device…	Plan on having IoT edge devices fall into malicious hands...

Requirements of security



Data Protection

- One of the most valuable assets is data
- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers

- An effective information security program is essential to the protection of the integrity and value of the organization's data

- Organizations must have secure infrastructure services based on the size and scope of the enterprise
- Additional security services may have to be provided

Threats

- A threat is an object, person, or other entity that represents a constant danger to an asset

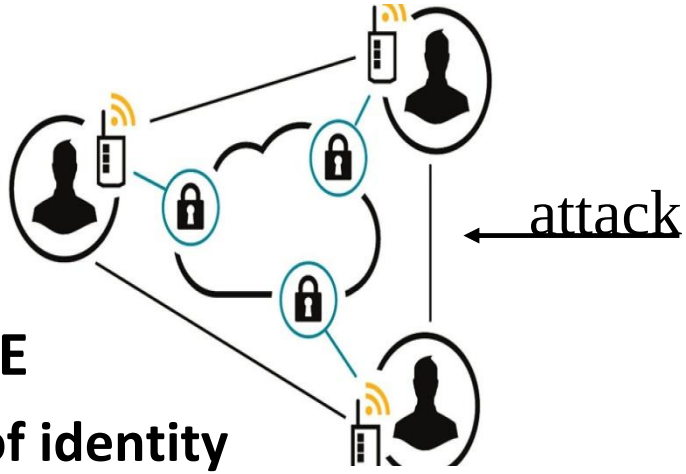
- Management must be informed of the various kinds of threats facing the organization

- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls

Threat Modeling

Threat Modeling

- **Theoretical use cases considered to identify potential threats.**

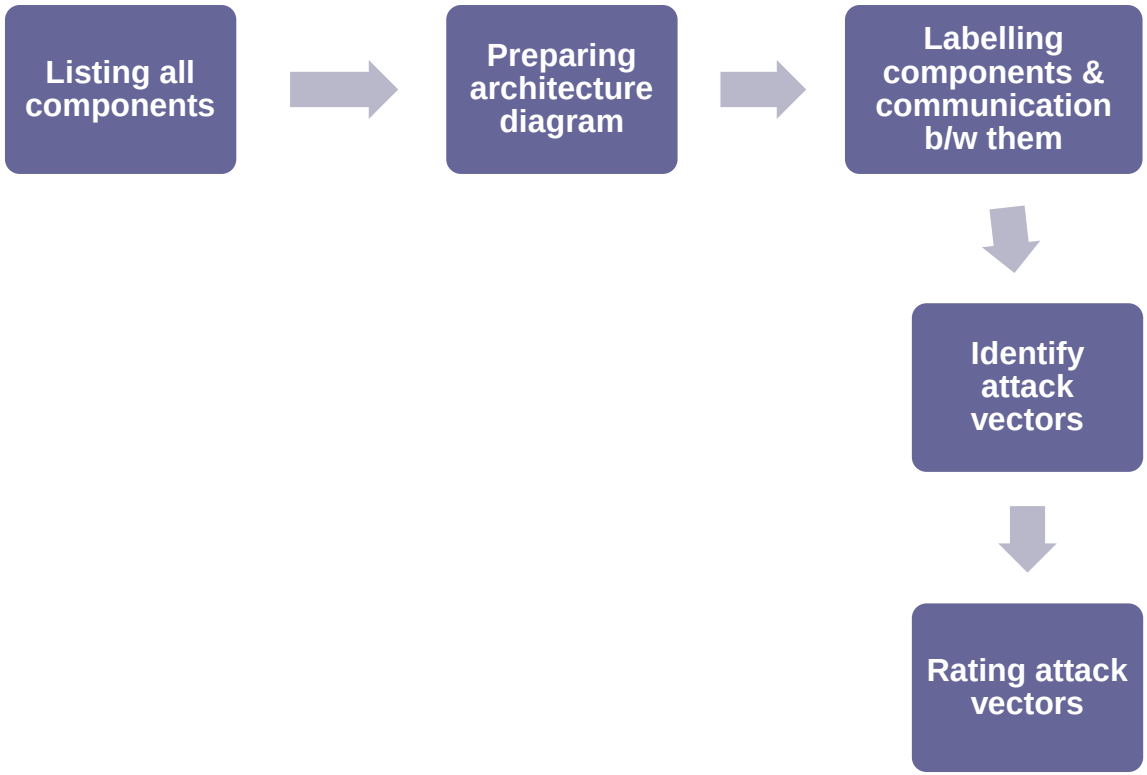


- **Microsoft STRIDE**
  - **S: Spoofing of identity**
  - **T: Tampering with data**
  - **R: Repudiation**
  - **I: Information disclosure**
  - **D: Denial of service**
  - **E: Elevation of privilege**
- **Requires realization of Assets and Vulnerabilities**

Attack Surface Mapping

- Attack surfaces are different points that an unauthorized user can employ to compromise a system/ network/ solution.
- Each attack surface has its associated risk, likelihood and impact.
- Source of input maybe HW, SW/FW, Communication
- Mapping out all entry points an attacker can abuse in IoT device.
- Involves creating an architecture diagram
  - Tests performed based on priority
  - Priority = ease of exploitation * impact of exploitation

Attack Surface Mapping Process



Threats to Information Security

TABLE 2-1 Threats to Information Security[4]

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Attacks

- An attack is the deliberate act that exploits vulnerability
- It is accomplished by a threat-agent to damage or steal an organization's information or physical asset
  - A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective
  - An exploit is a technique to compromise a system
  - An attack is then the use of an exploit to achieve the compromise of a controlled system

Some classes of attacks

- **phishing (~ fishing):**
- **“dear Internet banking user, please fill in the attached module and return it to us ASAP according to the privacy law 675 …”**

- **psychological pressure:**
- **“help me, otherwise I’ll be in troubles …”**
- **“do it, or I’ll report it to your boss …”**
- **showing acquaintance with the company’s procedures, habits and personnel helps in gaining trust and make the target lower his defenses**

- **Back Doors**
  - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource
- **Password Crack**
  - Attempting to reverse calculate a password
  - **Brute Force**
  - The application of computing and network resources to try every possible combination of options of a password
  - **Dictionary**
  - The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses

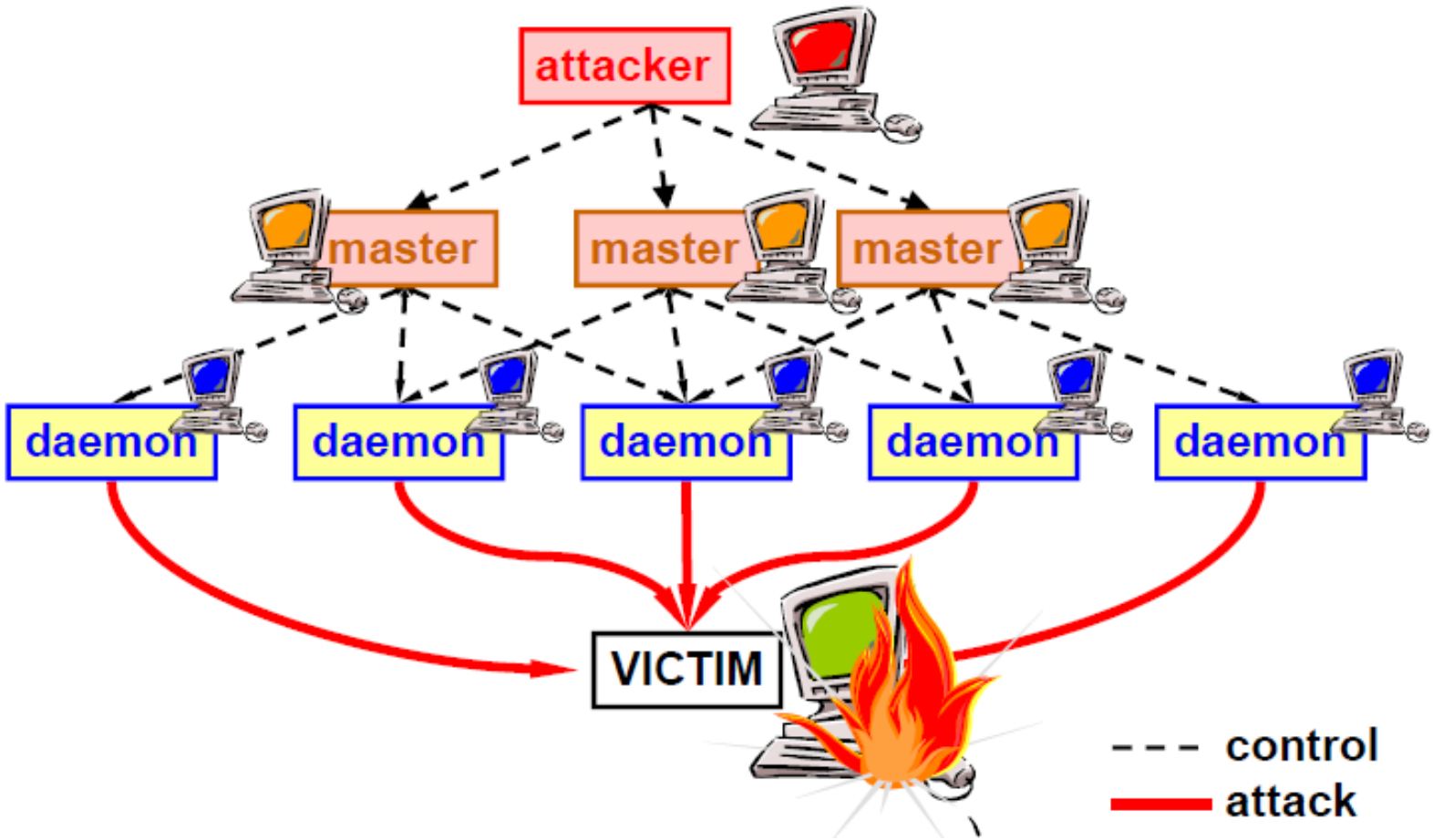
Some classes of attacks

- **IP spoofing / shadow server**
  - someone takes the place of a (legitimate) host
- **Packet sniffing**
  - passwords and/or sensitive data are read by (unauthorized) third parties
- **Connection hijacking / data spoofing**
  - data inserted / modified during their transmission
- **Denial-of-service (distributed DoS)**
  - the functionality of a service is limited or disrupted (e.g. ping bombing)

Distributed Denial of Service

- **Software for DoS installed on many nodes (named daemon, zombie or malbot) to create a Botnet**
- **Daemons remotely controlled by a master (often via encrypted channels) and have auto-updating feature**
- **Effect of the base DoS attack multiplied by the number of daemons**

Distributed Denial of Service



Basic problems

- Networks are insecure: (most) communications are made in clear
- LANs operate in broadcast

- Geographical connections are NOT made through end-to-end dedicated lines but:
  - through shared lines
  - through third-party routers
  - weak user authentication (normally password-based)

- There is no server authentication
- Software contains many bugs!

Basic Problems

- low problem understanding (awareness)
- mistakes of human beings (especially when overloaded, stressed, …)
- human beings have a natural tendency to trust
- complex interfaces / architectures can mislead the user and originate erroneous behaviors
- performance decrease due to the application of security
- ask for the (involuntary) user's participation to the attack action
- usually naive users are targeted (e.g. "do change immediately your password with the following one, because your PC is under attack") ...
- but experienced users are targeted too (e.g. by copying an authentic mail but changing its attachment or URL)

Roots of Insecurity

- "Defensive strategies are reactionary"
- "Thousands - perhaps millions - of system with weak security are connected to the Internet"
- "The explosion in use of the Internet is straining our scarse technical talent. The average level of system administrators has decreased dramatically in the last 5 years"
- "Increasingly complex software is being written by programmers who have no training in writing secure code"
- "Attacks and attack tools transcend geography and national boundaries"
- "The difficulty of criminal investigation of cybercrime coupled with the complexity of international law means that prosecution of computer crime is unlikely"

ICT security

- **ICT (Information and Communication Technologies)** refers to technologies that provide access to information through telecommunications.
- **ICT security** is the set of products, services, organization rules and individual behaviors that protect the ICT system of a company.

- **Three main components of any system are:**
  - **Hardware**
  - **OS and applications**
  - **Communication**

  - **Cloud - (Optional)**

Security Design Principles

Principal of ….

- **Least Privilege**
- **Separation of privilege**
- **Fail-safe defaults**
- **Complete mediation**
- **Economy of mechanism**
- **Least Common Mechanism**
- **Psychological acceptability**

Principle of least privilege

- Provide bare minimum privileges to a program or user to function properly
- Temporary elevation should be relinquished immediately
- Granularity of privileges

Advantage

- Abuse of privileges is restricted
- Damage caused by the compromised user or application is reduced

Separation of Privilege

- Access should not be granted based on single condition
- Multiple conditions should be required to achieve access to restricted resources

Examples:

- Two persons to sign checks
- Password login + OTC to perform financial transactions

Fail-safe defaults

- The default configuration of a system should have a conservative approach…
  - Default access to an object is none
  - Explicit access to an object should be given

Examples

- Access Control Lists
- Firewall rules

Complete mediation

- Instead of one time check, every access to a resource must be checked for compliance with a protection scheme
- restricts the caching of information
- Security vs performance issue

- Whenever a subject attempts to read an object, the operating system should mediate the action. First, it determines if the subject can read the object. If so, it provides the resources for the read to occur. If the subject tries to read the object again, the system should again check that the subject can still read the object. Most systems would not make the second check. They would cache the results of the first check, and base the second access upon the cached results.
  - UNIX file descriptor
  - DNS cache poisoning

Principle of economy of mechanism

- **Simplicity in design and implementation of security measures**

- **A simple secure framework provides…**
  - **Fewer errors**
  - **Development, testing and verification of security measures is easy**
  - **Less assumptions**

Least common mechanism

- In shared systems with multiple users, mechanisms allowing resources to be shared by more than one user should be minimized
- Separate channel for users
- Separation of network resources

Principle of psychological acceptability

- **Security mechanism should not make the resources difficult to access**
- **User interface should be well designed and intuitive**
- **Security related setting should consider the expectation of ordinary users**