Software Security

Prof.ssa Mila Dalla Preda

AA 2023/2024

Orario

- Mercoledì 12:30 - 14:30 (2 ore) aula T.03
- Giovedì 13:30 - 16:30 (iniziamo alle 14:00, ok? 2 o 3 ore) aula T.03
- Date Laboratorio:
  - Giovedì 2 Novembre
  - Giovedì 16 o 23 Novembre
  - Mercoledì 20 e Giovedì 21 Dicembre

Recupero Lezioni

- Sulla pagina moodle del corso verranno caricate le registrazioni delle lezioni dello scorso anno
- Per qualsiasi necessità particolare contattatemi via mail

Exam

- Progetto/approfondimento individuale o di gruppo (max 3 persone). Il tema del progetto/approfondimento può essere proposto dagli stessi studenti al docente. I risultati del progetto/approfondimento dovranno essere scritti in una relazione che verrà poi discussa e presentata oralmente al docente su appuntamento e poi verbalizzata nella prima sessione utile. La presentazione avrà la durata di 15 minuti (preferibilmente supportata da slides)
- Alla presentazione del progetto seguiranno domande orali sui temi trattati nel corso
- Office: Ca' Vignal 2, 1st floor, room 72
- Please contact me by email: mila.dallapreda@univr.it

Material

- Slides available on the course webpage
- Surreptitious Software, C. Collberg and J. Nagra, Addison Wesley, 2009.
- M. Bishop. Introduction to Computer Security. Addison-Wesley. 2004
- W. Stallings and L. Brown. Computer Security: Principles and Practice. Pearson International Edition. 2008
- D. Gollmann. Computer Security (Second Edition). John Wiley & Sons, Ltd. 2006

Software security (~24h)

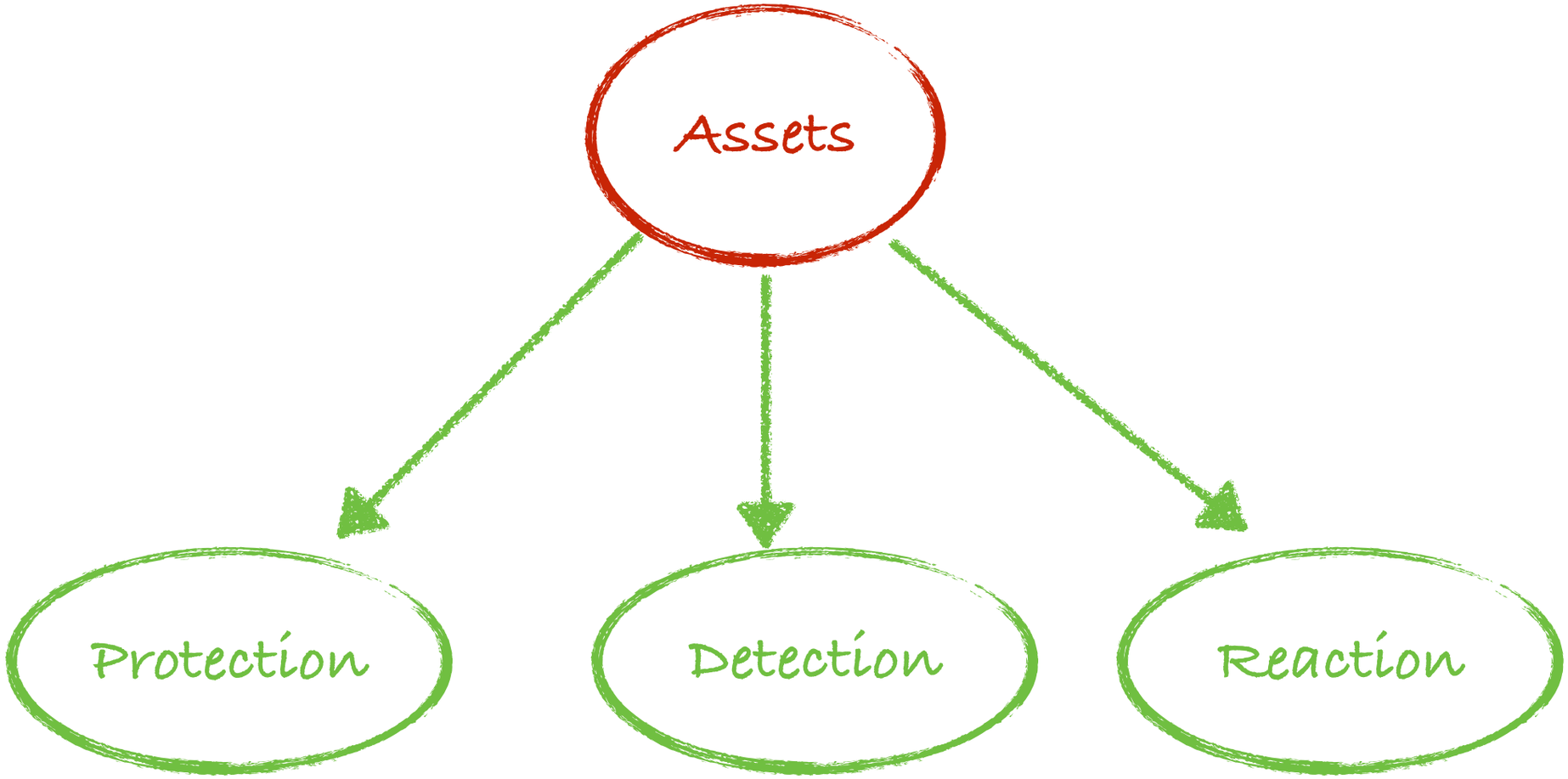
- Introduction
- Computer security technology and principles
  - Access control
  - Authentication
- Software vulnerabilities & Lab activities
  - background su assembly x86 e ELF
  - tools per analisi di binari: gdb, ghidra
  - ripasso python 3 e libreria pwntools
  - reverse engineering e patching di binari
  - buffer overflow attacks
  - stack canaries, format string vulnerabilities

Software Protection (~24h)

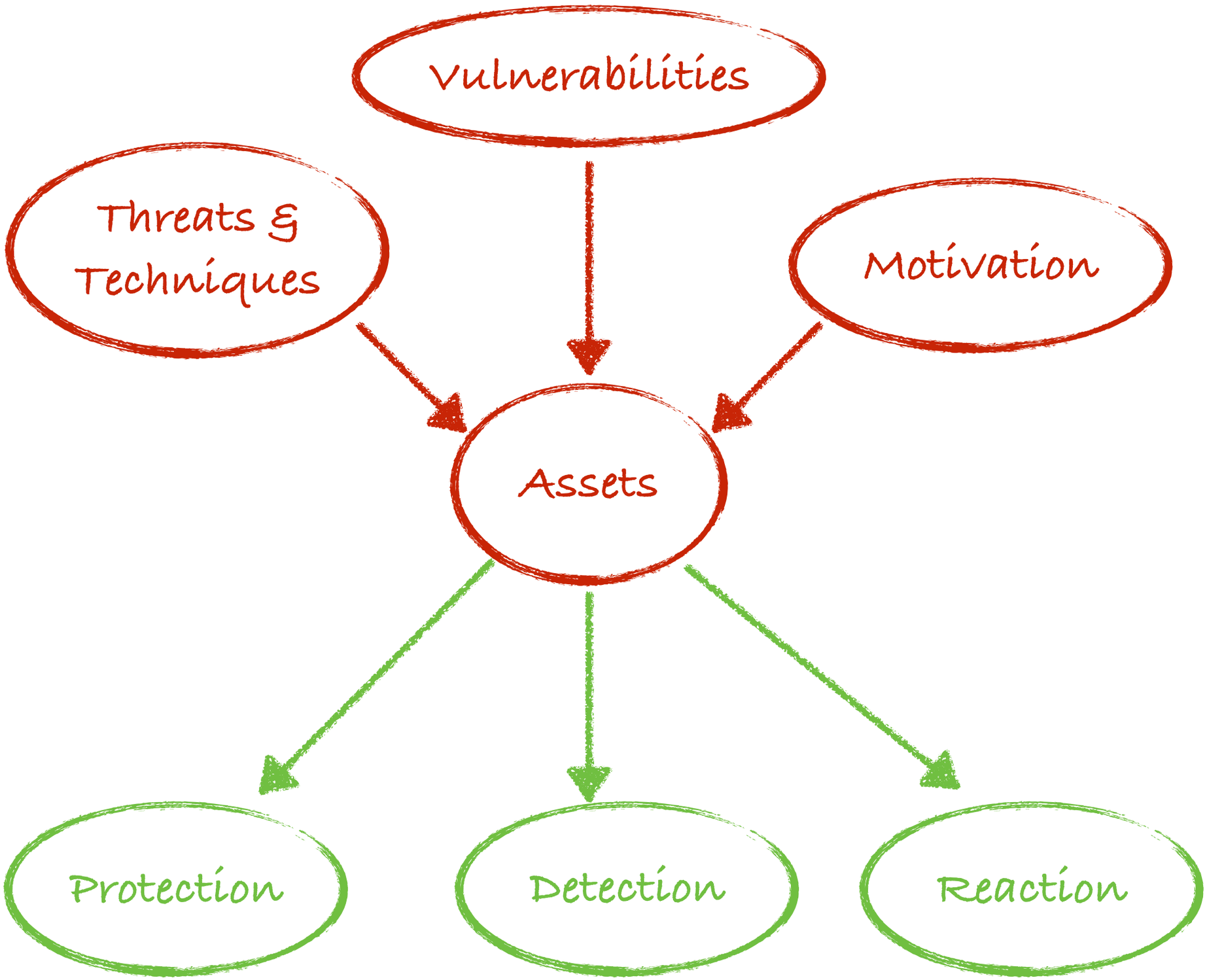
- Introduction
- Code Obfuscation Techniques
- Impossibility result
- Semantics based attacks and defenses & malware detection
- Tampering and Anti-tampering
- Watermarking
- Similarity analysis
- Open Challenges

System Security

What is Security?



What is Computer Security?



Computer Security

Security practitioners know that *security is a people problem*
that cannot be solved by technology alone

Dieter Gollmann - Computer Security

How is information/software security different?

- The Information/software can be stolen – but you still have it.
- Confidential information or proprietary software may be copied and sold – but the theft might not be detected.
- The criminal may be on the other side of the world.

Computer security deals with the prevention and detection of *unauthorised actions* by users of a computer system.

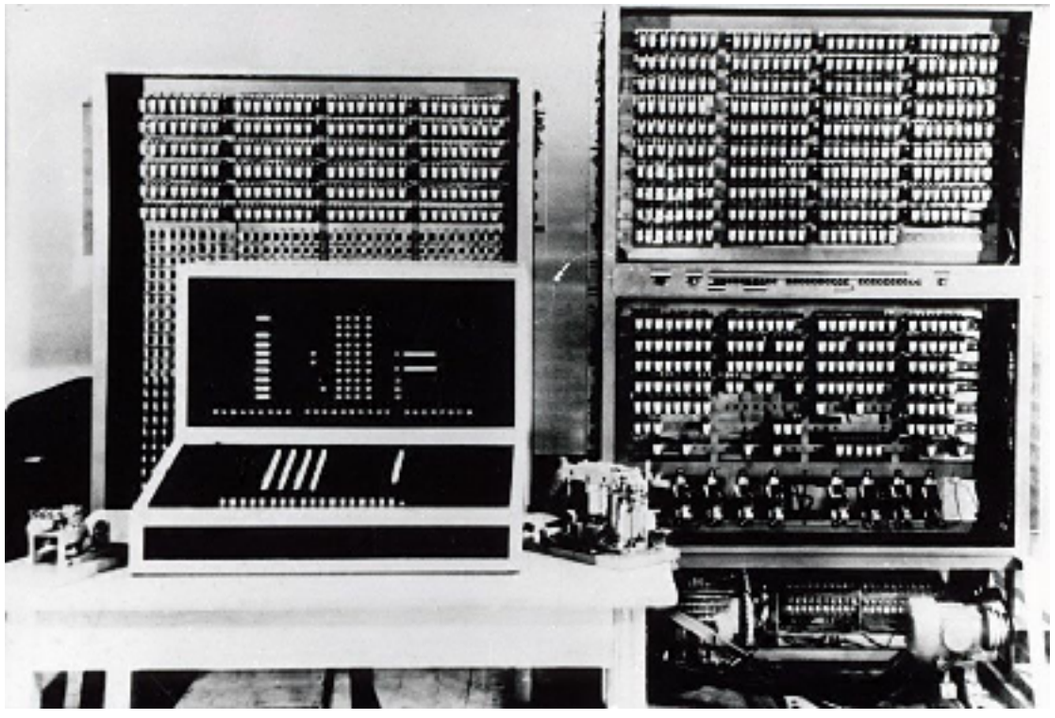
Security

Protection of computer systems from the theft or damage to their hardware, software or information, as less as disruption or misdirection of the services they provide (M. Gasser 1998)

The origins of Computer Security

* As cybersecurity and technology have evolved, so have criminals who seek to exploit weaknesses in the system for personal gain

* New security challenges arise when new or old technologies are put to new use



- The first computer was built in 1940s
- Carrying out cyberattacks was tricky. Access to the giant electronic machines was limited and they were isolated
- In1949 John von Neumann speculated that computer programs could reproduce.

1950s: The phone phreaks

- ✓ The technological and subcultural roots of cyberattacks as much related to early telephones as they are to computers.
- ✓ In the late 1950s, *phone phreaking* emerged.
  - ✓ hijack the protocols that allowed telecoms engineers to work on the network remotely to make free calls and avoid long-distance tolls.
  - ✓ eventually died out in the 1980s.

1970s: Computer security is born

- ✓ The existence of *multi-user systems* led to the need of protection mechanism for the systems from its users and for users from each others (protection rings)
- ✓ In 1971 Bob Thomas created a computer program called Creeper that could move across ARPANET's network, leaving a breadcrumb trail wherever it went.
- ✓ Ray Tomlinson wrote the program Reaper, which chased and deleted Creeper.

```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19    3 JOBS
LOAD AV    3.87    2.95    2.14
JOB  TTY   USER        SUBSYS
1    DET   SYSTEM      NETSER
2    DET   SYSTEM      TIPSER
3    12    RT          EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

https://corewar.co.uk/creeper.htm

* The early 70's witnessed a marked increase in discussions around computer security.

1970s: Computer security is born

ESD-TR-73-51, Vol. II

COMPUTER SECURITY TECHNOLOGY PLANNING STUDY

James P. Anderson

October 1972

In recent years the Air Force has become increasingly aware of the problem of computer security. This problem has intruded on virtually any aspect of USAF operations and administration. The problem arises from a combination of factors that includes: greater reliance on the computer as a data-processing and decision-making tool in sensitive functional areas; the need to realize economies by consolidating ADP [automated data processing] resources thereby integrating or co-locating previously separate data-processing operations; the emergence of complex resource sharing computer systems providing users with capabilities for sharing data and processes with other users; the extension of resource sharing concepts to networks of computers; and the slowly growing recognition of security inadequacies of currently available computer systems.

Computing Surveys, Vol. 8, No. 4, December 1976

Operating System Structures to Support Security and Reliable Software

THEODORE A. LINDEN

Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234

INTRODUCTION

For the year 1974, one source has identified 339 cases of computer-related crime.[1] The *average* loss in the 339 incidents was $544,000. This average is not distorted by a few exceptional cases; the median loss was very close to the average. Most of the incidents involved simple fraud by an employee who had access to computerized financial records. In 85 percent of the cases, management did not report the incident to the police—often because publicity about it would have been embarrassing.

The fraud is usually possible because of some oversight in an applications system. A simple oversight, for example, may allow a clerk to feed data to an accounts payable system in such a way that no one notices when checks are diverted to a dummy corporation.

If the amount of computer-related fraud is to be controlled, then it is necessary to automate the concepts of segregated duties, independent checking, and accountability for actions that are typical in manual ac-

[1] This information is based on conversations with Robert Courtney. Courtney reports that details on these cases are in his possession, but that they cannot be made public. The work of Parker [PARK 75] based on public reports, supports a similar conclusion about the average loss in computer-related crime.

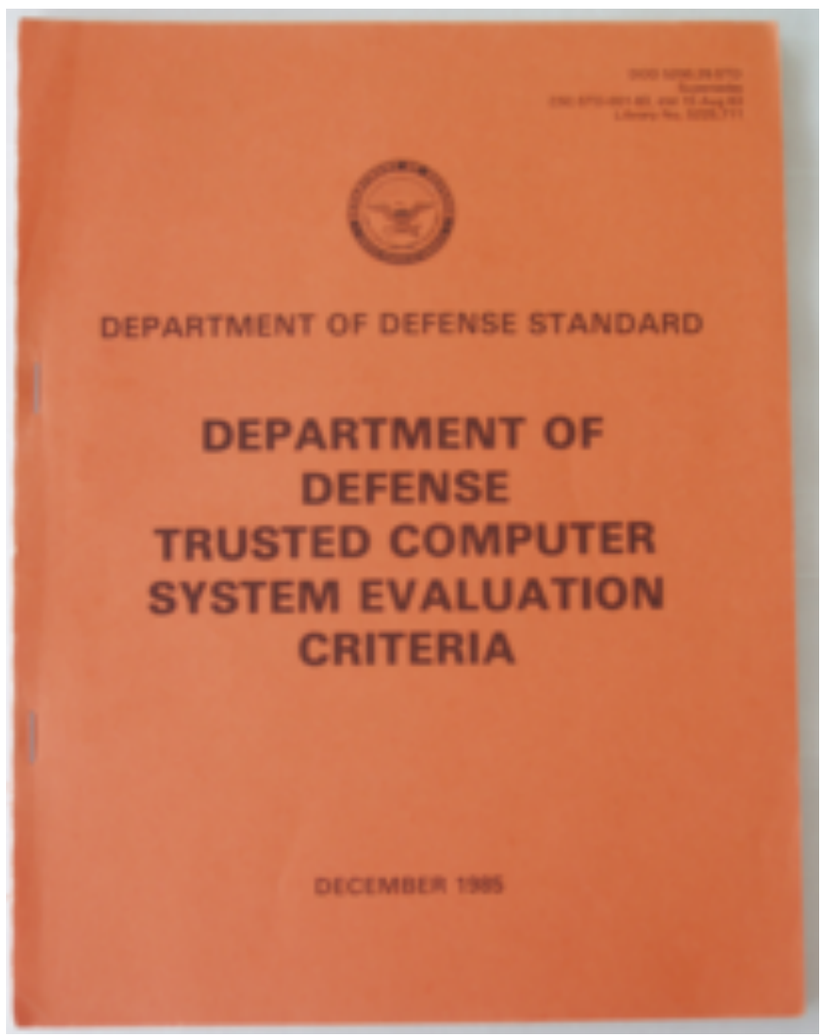
1970s: Mainframe

- The fast evolution of the storage technologies led to the processing of huge amounts of data
- There are two relevant application fields
  - ✓ The Defense recognized the utility of exploiting computers, but *classified information* have to be treated in a *secure* mode
    - ◇ Study of a formal model for multilevel policies
    - ◇ The computer architectures started to be designed including security mechanisms
  - ✓ Processing of "*unclassified but sensitive data*"
    - ◇ Multi-user security
    - ◇ Encryption
    - ◇ New security problems in statistical databases

1980s - PC

* Graphical interfaces and mouses made input/output procedures more *user-friendly*
  - ✓ The pc was a single user machine for the processing of documents with sensitive, rarely classified, information
  - ✓ New problems of *information flow and noninterference models* that access control models are unable to catch in multi-users systems
  - ✓ New *commercial policies* to model

✓ The Orange Book 1985 describes the security design of a computer that can be trusted to handle both unclassified and classified information, known as a multilevel secure or trusted computer.



1990s - Internet

- Internet was opened for commercial use (1992)
  - ✓ HTTP and HTML protocols provided the bases for more interesting applications than email or remote procedure call
  - ✓ The World Wide Web and the introduction of graphical browsers provided new possibilities to users
- Initially, *internet security* as communication security (cryptography): this protects data in transit while the Internet creates a network of computers and that poses new challenges:
  - ◇ The pc owner cannot check who sends input to the pc
  - ◇ The pc owner cannot check which input are sent to the pc

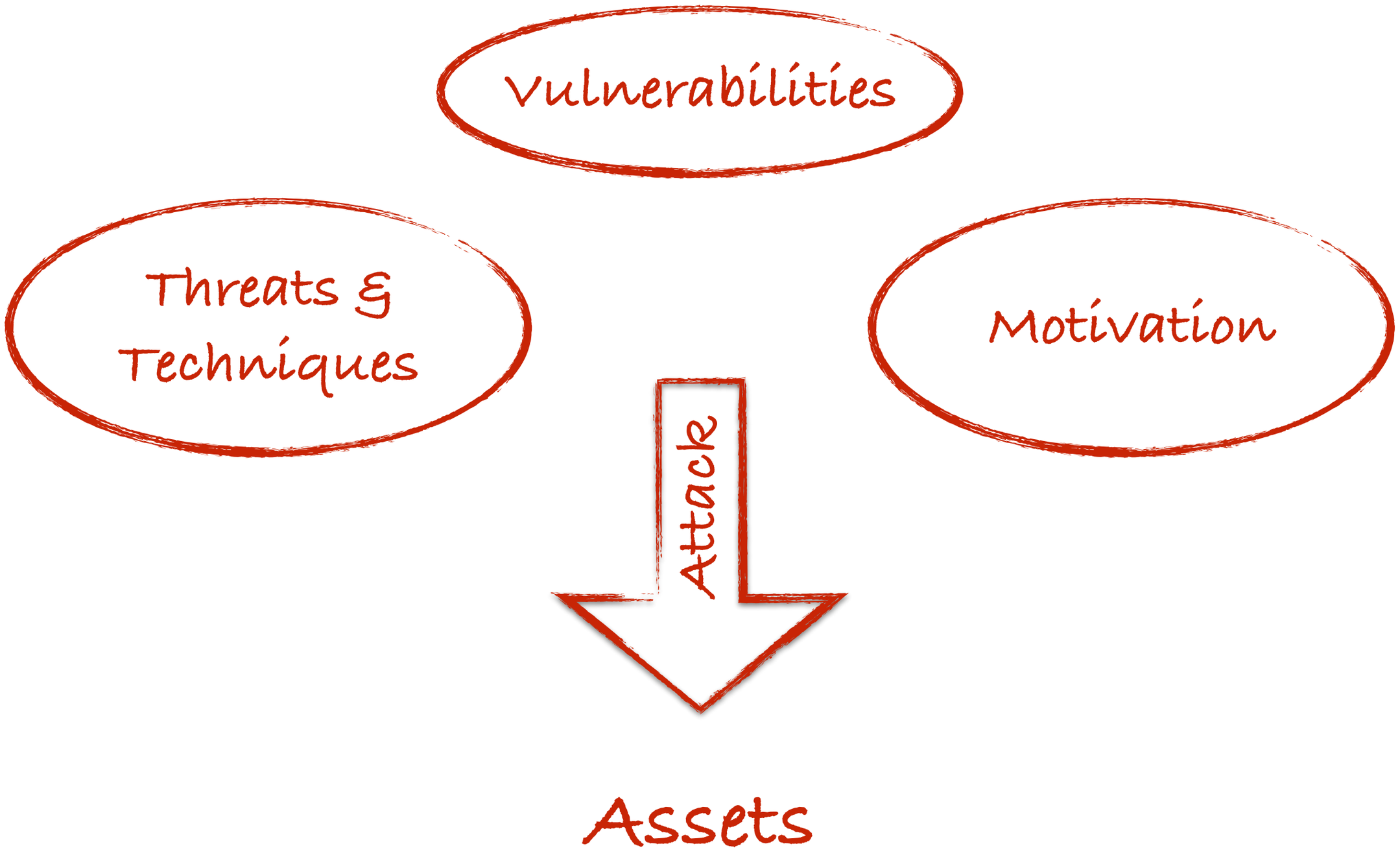
1990s - Internet

* New graphical technologies transformed PCs in platforms for home entertainment (e.g. videogame) and this lead to the problem of *intellectual property protection*
* Internet becomes an attractive way for providing these kind of services
  - ✓ New problems of *copyright protection*
  - ✓ New *Digital Rights Management (DRM)* problems made access control inadequate for protecting information
  - ✓ New SW and HW solutions for *code protection*
* Availability was a critical security problem
  - ✓ Due to Internet the *Denial of Service (DoS) attack* became a reality
  - ✓ To improve protection were introduced *firewall* and *Intrusion Detection Systems (IDS)*

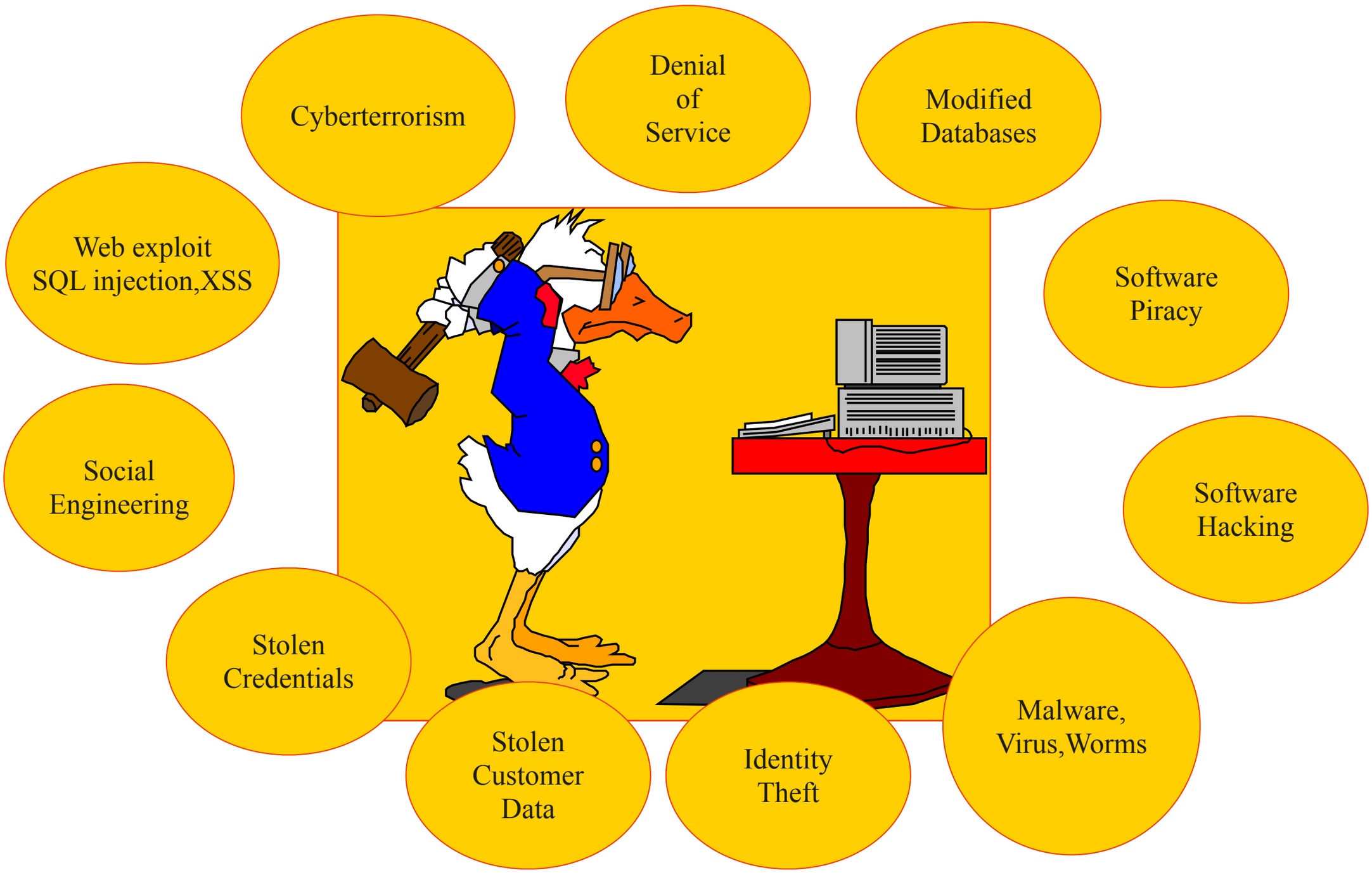
2000s - Web

- Web = Technology + Users
  - ✓ Users = services providers and consumers
  - ✓ After the 90's the big challenge was the increase of users
- Service providers had direct access to consumers without middlemen
  - ◇ Flight companies, eBay, Amazon, …
- Many commercial applications
- The application SW providing the service became the main attack target (SQL injection, XSS attacks)
  - ◇ The first attackers were young people challenging security protection systems
  - ◇ Now attackers are criminals with precise tasks aiming at gaining some economic advantage

Security


Vulnerabilities
Threats & Techniques
Motivation
Attack
Assets

Security Threats



* To decide whether a computer system is *secure*, you must first decide what *secure* means to you, then identify the threats you care about

Security Management

Security is about the protection of assets

- Protecting the assets of an organization is the responsibility of management
- Security measures often restrict members of the organization in their working patterns and there may be a potential temptation to flout security rules.
- Not every member has to become a security expert, but all members need to know
  - why security is important for themselves and for the organization,
  - what is expected of each member, and
  - which good practices they should follow.
- Security **awareness** (security training)
- *Security policy* – a statement that defines the security objectives of an organization; it has to state what needs to be protected; it may also indicate how this is to be done.

Asset

Security is about the protection of assets

* We have to know the *assets* and their *values*
  - ✓ hardware: laptops, servers routers, mobile phones, smart cards…
  - ✓ software: applications, OS, DB management systems, source code…
  - ✓ data and information: essential data for running and planning your business, design documents, digital content, data about costumers, …
  - ✓ reputation

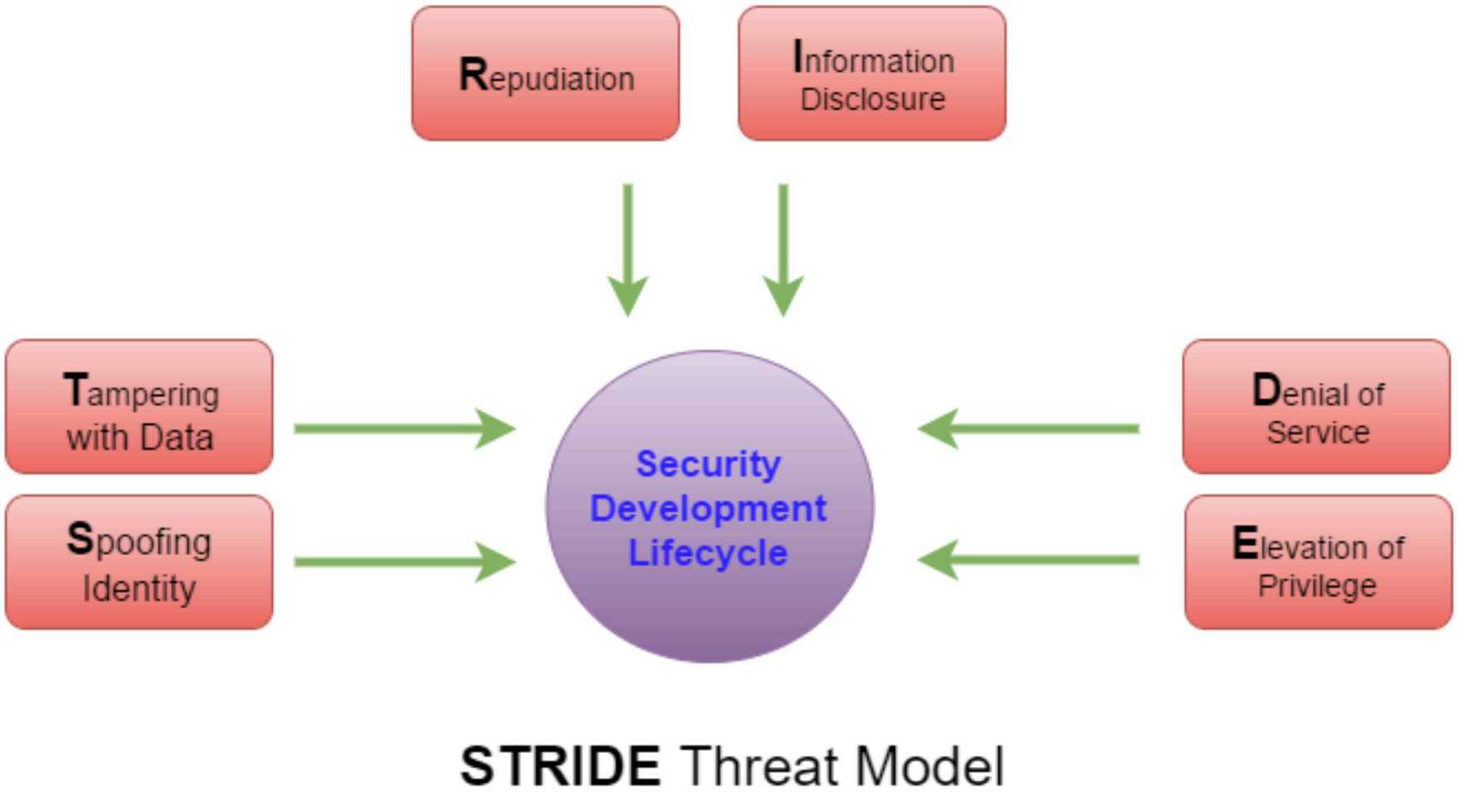
Temporality Principle

* Data value: Hard to measure since each datum has to be considered and interpreted in the right context, also because this value may change in the course of time

Temporality: the elements of an IT system have to be protected only until they have a value, and relatively to their value

Threat

A threat is an undesirable negative impact on an asset



STRIDE Threat Model

TYPES OF SPOOFING ATTACKS

Caller ID

Website spoofing

Email spoofing

IP spoofing

Text message spoofing

DNS spoofing

ARP spoofing

GPS spoofing

Extension spoofing

Man-in-the-middle spoofing

Tampering with Data

CYBERSECURITY LATEST NEWS

Attacks Involving Data Tampering are Difficult to Identify

by Madhurjya Chowdhury / August 29, 2022

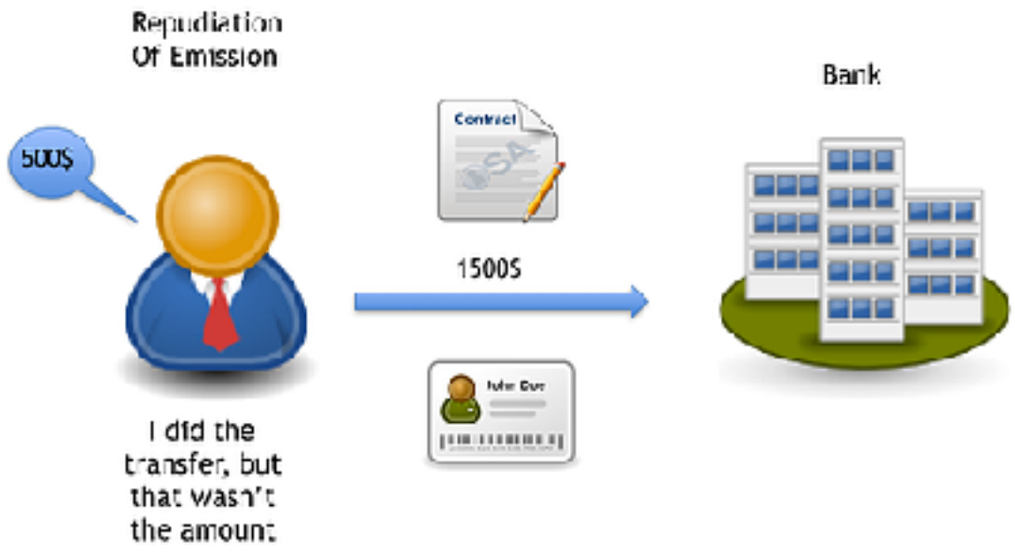
> *"What happens when you can't trust your own data? This is a nightmare scenario."*

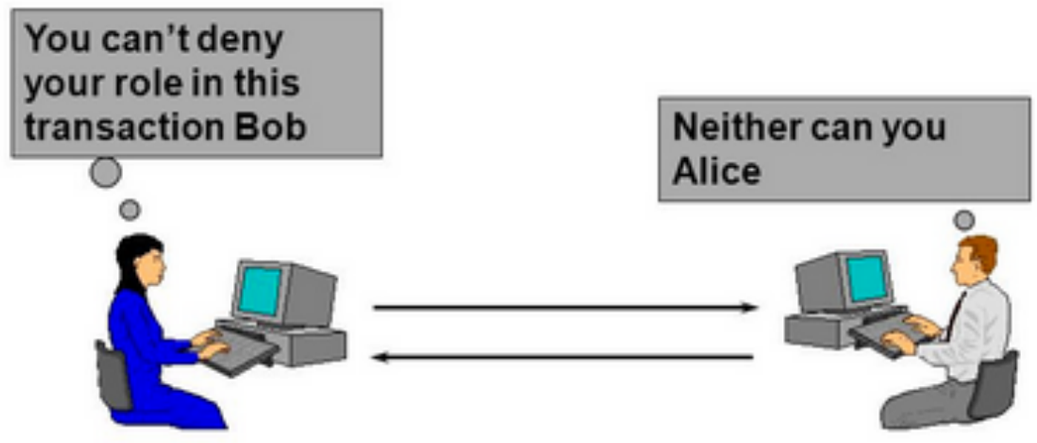
Florida Water Treatment Plant Hit With Cyber Attack

Steve Kardon

February 9, 2021

Repudiation





Non-repudiation

Information Disclosure

Data Breaches That Have Happened in 2022 So Far

Apple, Meta, Twitter, and Samsung have all disclosed cybersecurity attacks this year. We track the latest data breaches.

Aaron Drapkin | September 22nd 2022 - 3:55 am

https://tech.co/news/data-breaches-2022-so-far

IBM Report: Consumers Pay the Price as Data Breach Costs Reach All-Time High

60% of breached businesses raised product prices post-breach; vast majority of critical infrastructure lagging in zero trust adoption; $550,000 in extra costs for insufficiently staffed businesses

Jul 27, 2022

CAMBRIDGE, Mass., July 27, 2022 /PRNewswire/ -- IBM (NYSE: IBM) Security today released the annual Cost of a Data Breach Report,[1] revealing costlier and higher-impact data breaches than ever before, with the global average cost of a data breach reaching an all-time high of $4.35 million for studied organizations. With breach costs increasing nearly 13% over the last two years of the report, the findings suggest these incidents may also be contributing to rising costs of goods and services. In fact, 60% of studied organizations raised their product or services prices due to the breach, when the cost of goods is already soaring worldwide amid inflation and supply chain issues.

https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High

Denial of Service

Record DDoS Attack with 25.3 Billion Requests Abused HTTP/2 Multiplexing

September 21, 2022 Ravie Lakshmanan

Cybersecurity company Imperva has disclosed that it mitigated a distributed denial-of-service (DDoS) attack with a total of over 25.3 billion requests on June 27, 2022. The "strong attack," which targeted an unnamed Chinese telecommunications company, is said to have lasted for four hours and peaked at 3.9 million requests per second (RPS).

Malicious DDoS Attacks Jump By 203% in First Half of 2022

By George Winslow published August 25, 2022

Russian invasion of Ukraine dramatically boosted cyber attacks and shifted the threat landscape, according to Radware

Elevation of Privileges

Security Update Guide

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the inform

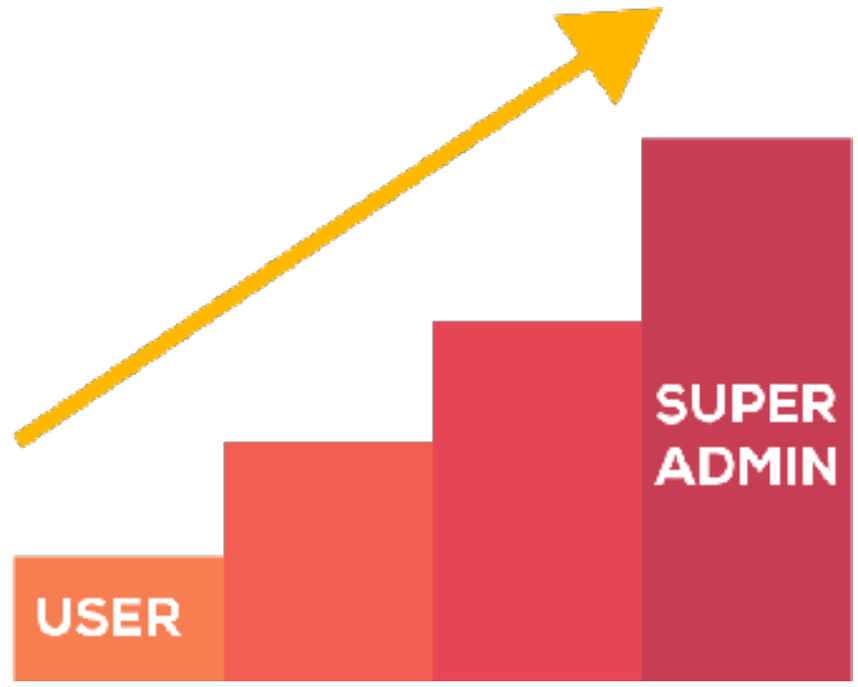
All Deployments Vulnerabilities

Aug 16, 2022 - Sep 27, 2022

ELEVATION OF PRIVI... No grouping

Release Date	Last Updated	CVE Number	CVE Title	Tag
Sep 13, 2022	-	CVE-2022-38030	Visual Studio Code Elevation of Privilege Vulnerability	Visual Studio Code
Sep 13, 2022	-	CVE-2022-38037	Azure Guest Configuration and Azure Arc-enabled servers Elevation of	Azure Arc
Sep 13, 2022	-	CVE-2022-38033	Windows Print Spooler Elevation of Privilege Vulnerability	Windows Print Spooler Components
Sep 13, 2022	-	CVE-2022-37959	Windows Common Log File System Driver Elevation of Privilege Vulner	Windows Common Log File System Driver
Sep 13, 2022	-	CVE-2022-37954	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel
Sep 13, 2022	-	CVE-2022-37957	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel
Sep 13, 2022	-	CVE-2022-37956	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel
Sep 13, 2022	Sep 20, 2022	CVE-2022-37955	Windows Group Policy Elevation of Privilege Vulnerability	Windows Group Policy
Sep 13, 2022	-	CVE-2022-37954	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Microsoft Graphics Component
Sep 13, 2022	-	CVE-2022-35678	Microsoft Defender for Endpoint for Mac Elevation of Privilege Vulner	Windows Defender
Aug 9, 2022	Aug 19, 2022	CVE-2022-35620	Windows Bluetooth Driver Elevation of Privilege Vulnerability	Microsoft Bluetooth Driver
Sep 13, 2022	-	CVE-2022-35838	Windows Common Log File System Driver Elevation of Privilege Vulner	Windows Common Log File System Driver
Aug 9, 2022	Sep 20, 2022	CVE-2022-35751	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel
Aug 9, 2022	Aug 19, 2022	CVE-2022-35751	Windows Hyper-V Elevation of Privilege Vulnerability	Role: Windows Hyper-V

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the ongoing effort to help you manage security risks and help keep your systems protected.



Tampering with Code

Modify code behaviour

Software Piracy

Bypass licence check

Vulnerabilities

Vulnerabilities are weaknesses of a system that could be accidentally or intentionally exploited to damage assets

- ✓ accounts with default password not changed
- ✓ programs with unnecessary privileges
- ✓ programs with known flows
- ✓ weak access control settings on resources
- ✓ weak firewall configurations that allow access to vulnerable services
- ✓ …

Vulnerabilities

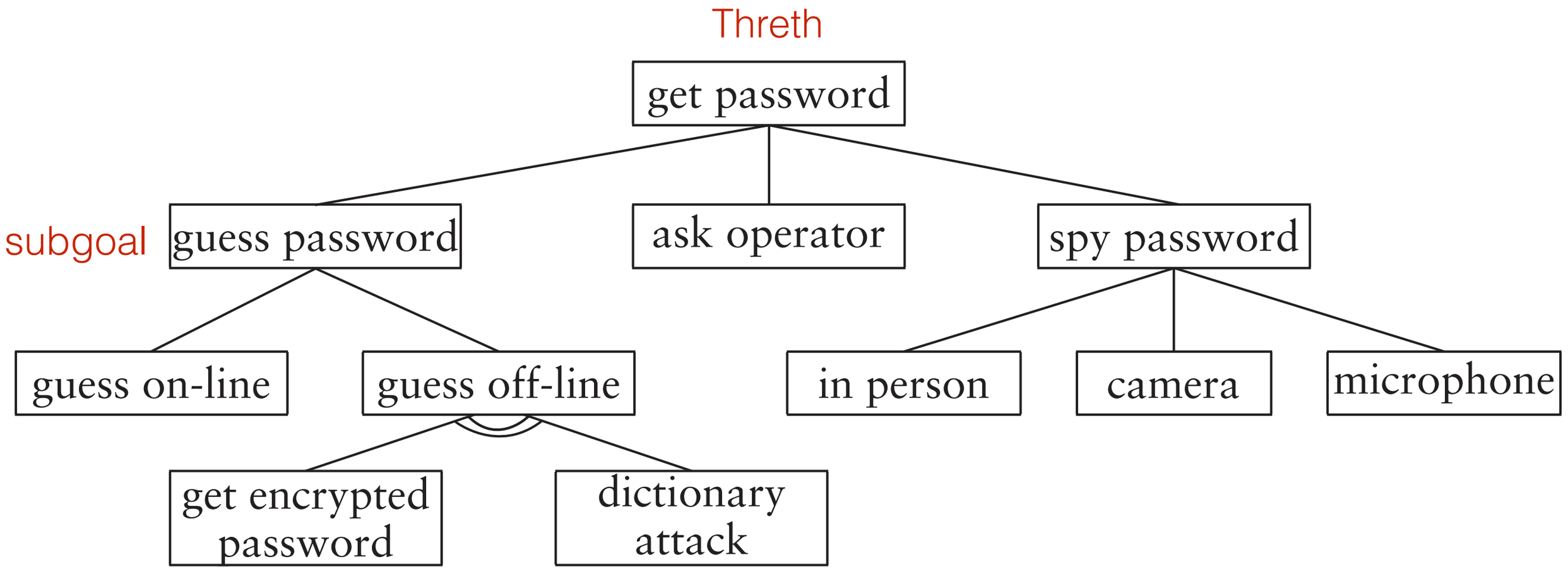
✓ *Vulnerability scanners* provide a systematic and automated way of identifying vulnerabilities. The dataset of known vulnerabilities has to be kept up to date. (SANS and computer emergency response teams CERTs@CMU)

✓ *Risk analysis* has to measure the criticality of vulnerabilities. The criticality of a vulnerability depends on the attacks that might exploit it. A vulnerability that allows an attacker to completely impersonate a user is more critical than a vulnerability where the user can only be impersonated in the context of a single specific service.

Attacks

- ✓A threat materializes when an attack succeeds.
- ✓An attack is a sequence of steps.
- ✓To get a fuller picture of its potential impact, a forest of attack trees can be constructed.
  - ✓The root of an attack tree is a threat.
  - ✓The nodes in the tree are subgoals that must be achieved for the attack to succeed.
  - ✓There are AND nodes and OR nodes. To reach an AND node, all subgoals have to be achieved. To reach an OR node, it is enough if one subgoal is achieved.

Attacks


Threth
get password
subgoal
guess password
ask operator
spy password
guess on-line
guess off-line
in person
camera
microphone
get encrypted password
dictionary attack

Attacks

- ✓ The severity of an attack depends on the likelihood that it will be launched, that it will succeed and on the damage that it might do
- ✓ The **likelihood** depends on difficulty, motivation, existing countermeasures, etc.
- ✓ The DREAD methodology (from Microsoft) demonstrates how the severity of an attack can be measured in a systematic manner
  - ✓ *Damage potential*: relates to the values of the assets being affected
  - ✓ *Reproducibility:* attacks that are easy to reproduce are more likely to be launched from the environment than attacks that only work in specific circumstances
  - ✓ *Exploitability:* captures the effort, expertise, and resources required to launch an attack.
  - ✓ *Affected users:* the number of assets affected contributes to the damage potential
  - ✓ *Discoverability:* will the attack be detected? In the most damaging case, you will never know that your system has been compromised.

Risk Assessment

- Having measured the value of assets, the criticality of vulnerabilities, and the likelihood and impact of threats, you now face the tricky task of calculating your risks.

$$Risk = Assets \times Threats \times Vulnerabilities$$

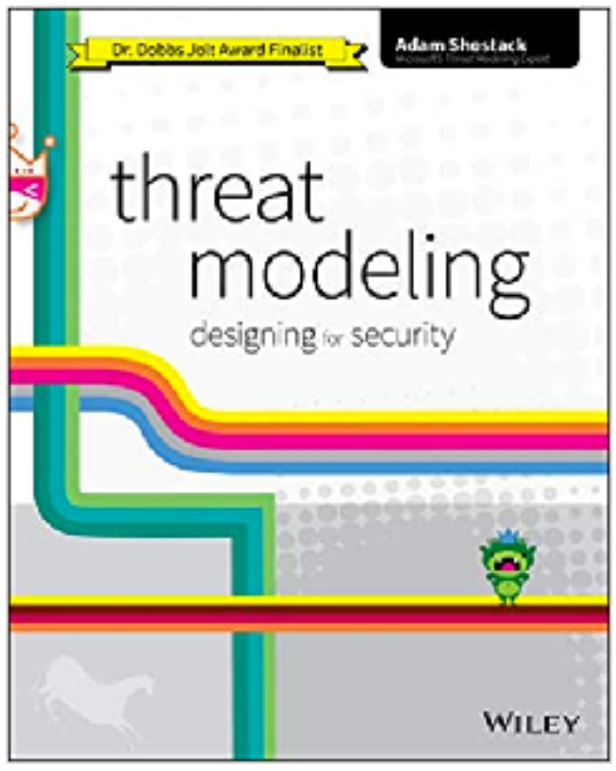
- Quantitative assessment: Not always useful, usually very complex;
- Qualitative assessment:
  - ✓ Value of assets: very important, important or not important
  - ✓ Criticality of vulnerability: Immediate solution, in a limited time, to solve, to solve only if it is worthwhile;
  - ✓ Likelihodd of threat: very probable, probable, improbable, very improbable
- The range may be finer

Risk Mitigation

- The result of a risk analysis is a prioritized list of threats, together with recommended countermeasures to mitigate risk.
- Risk analysis tools usually come with a knowledge base of countermeasures for the threats they can identify.
- Conducting a risk analysis for a larger organization will take time and the world outside will keep changing. Full risk analysis is costly.
- For these reasons, organizations may opt for baseline protection as an alternative.
- Risk, threat, vulnerabilities, asset analysis is fundamental for identifying the right security countermeasures to use in an organisation

Adam Shostack

- Personal web page https://adam.shostack.org/
- Wrote an interesting book



- Interesting talk: **Threat Modeling Lessons from Star Wars**

https://youtu.be/nd02oPnMdR4

Protection Measures

* Prevention: taking measures that prevent your asset from being damaged

* Detection: taking measures that allow you to detect when an asset has been damaged, how it has been damaged and who has caused the damage

* Reaction: taking measures that allow you to recover your asset or to recover from a damage to your asset

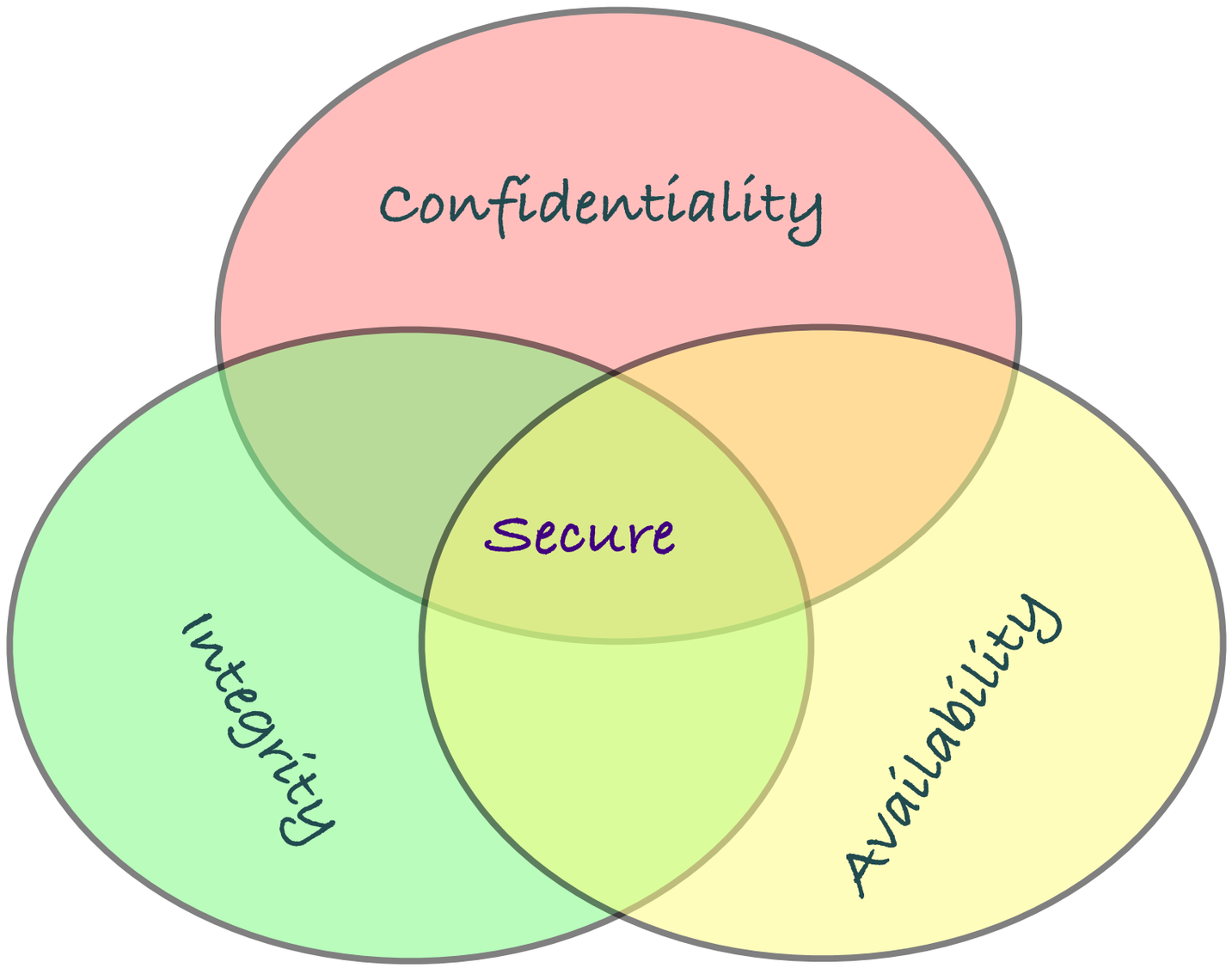
Secure system

* IT system: set of HW, SW, data, communication devices and people that a company uses for processing activities.

Security of an IT system:

Prevention and detection of non authorized actions performed by system users that have negative impact on the assets of the IT system

Security Targets



Confidentiality

- ✓ Historically, security is closely linked to *secrecy*. Security involved a few organisations dealing mainly with classified data.
- ✓ Unauthorised users should not learn sensitive information
- ✓ Confidentiality involves:
  - ✓ *privacy*: protection of personal data (individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed).
  - ✓ *secrecy*: protection of organizational data (private or confidential information is not made available or disclosed to unauthorised individuals.).

only authorized
users and systems
can access resources

Integrity

"Making sure that everything is as it is supposed to be."

- ✓ Integrity deals with the prevention of unauthorised writing (can be seen as the dual of confidentiality - similar mechanisms)
- ✓ *Data integrity*: Assures that information and programs are changed only in a specified and authorised manner.
- ✓ *System integrity*: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorised manipulation of the system.

Preventing unauthorized writing or modifications.

Availability

Assures that systems work promptly and service is not denied to authorized users.

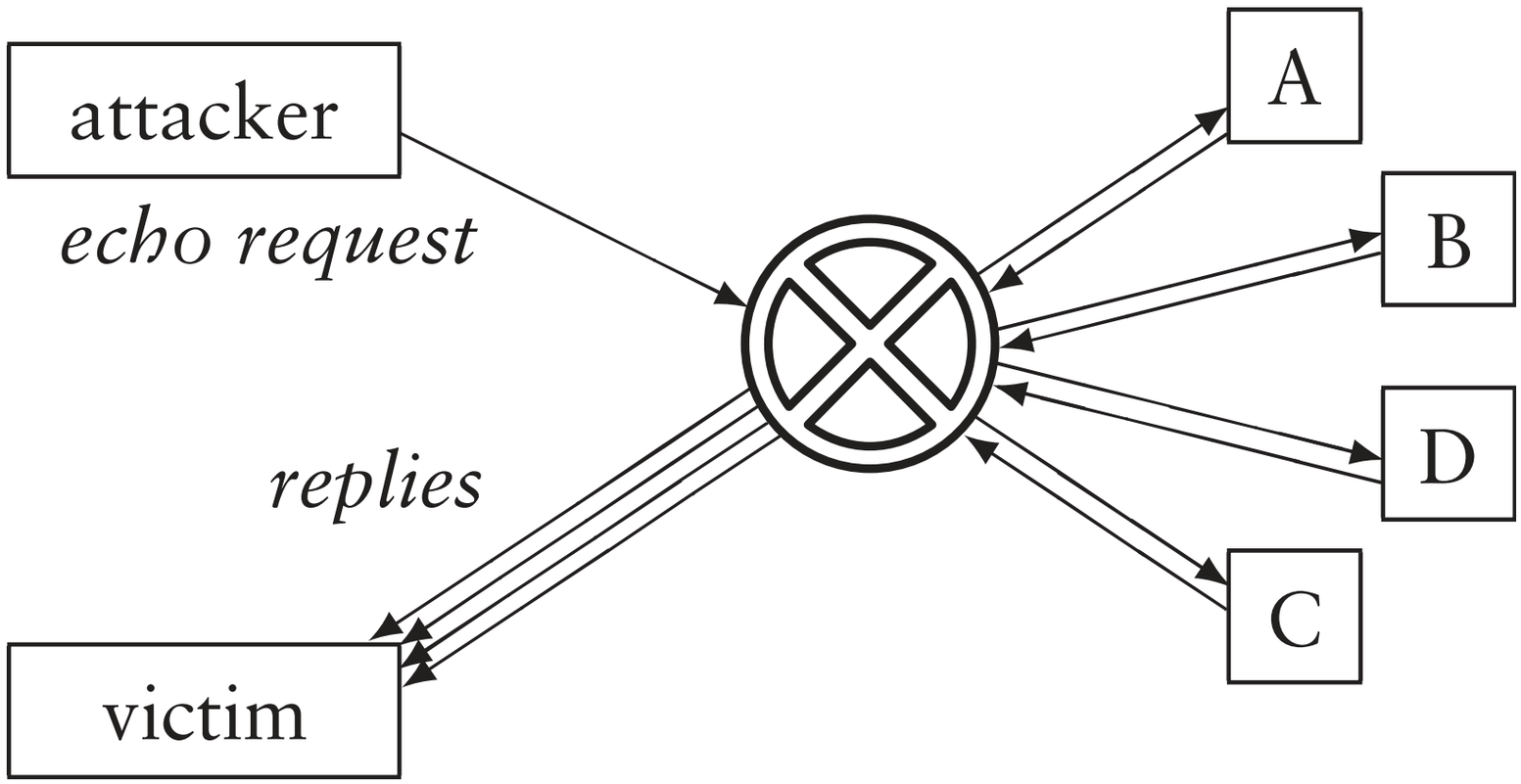
The services are always
- ✓usable
- ✓satisfy the service requirements
- ✓the job ends in an acceptable time

In the context of security, we want to ensure that a malicious attacker cannot prevent legitimate users from having reasonable access to their systems. That is, we want to *prevent denial of service.*

Services are accessible and useable (without delay) whenever needed by an authorized entity.

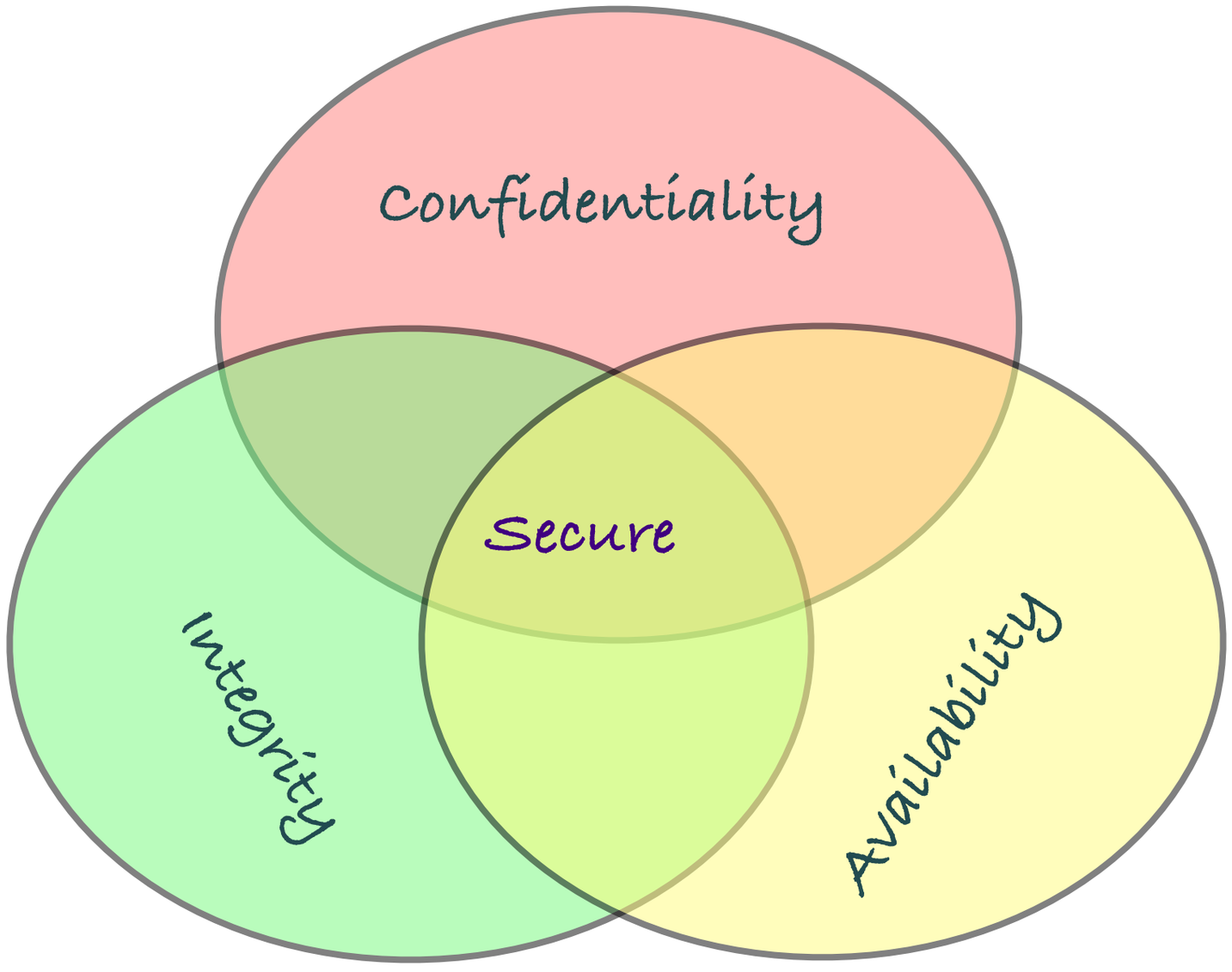
Availability

Denial of service: The prevention of authorised access to resources or the delaying of time-critical operations.



Smurf attack

Security Targets



Security: find the right balance among these objectives

Security Requirements

* Security so far deals with different aspects of **access control** and with the prevention of unwelcome events
* It is impossible to prevent all possible improper actions
* *Accountability:* The system is able to provide audit trails of all transactions. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. To this end the system has to:
  * Identify and authenticate users
  * Keep an audit trail of the security relevant events
  * *Responsibility*: Te log information has to be recorded securely in order to associate any potentially insecure action with the direct responsible

Security Requirements

- *Authenticity*:The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source

- *Non-repudiation:* Non-repudiation services provide unforgeable evidence that a specific action occurred.

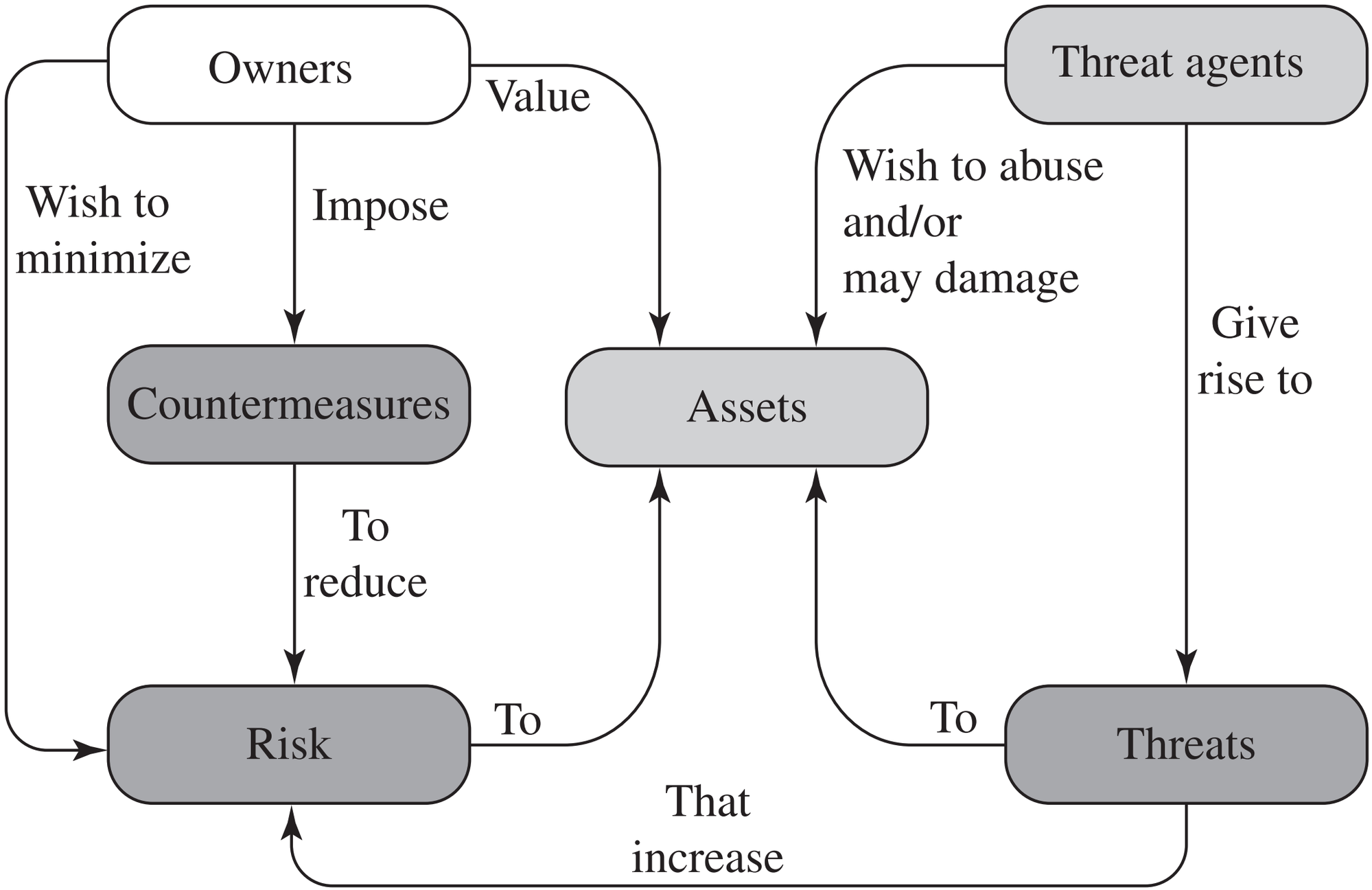
  - Relevant in communication security: non-repudiation of origin providing evidence about the sender of a document, and non-repudiation of delivery, providing evidence that a message was delivered to a specific recipient

  - Often achieved by digital signatures

Security Challenges

- ✓ Not easy: the requirements are straightforward but the mechanisms may be complex
- ✓ Consider *potential attacks* (often unexpected). "think like an arracker"
- ✓ Security mechanisms are complex and may appear counterintuitive
- ✓ Security mechanisms often involve many algorithms and *secret information* (encryption key)
- ✓ A battle between the *attacker* and the *administrator*
- ✓ Hard to see advantages without *fails*
- ✓ Security requires *continuous monitoring*
- ✓ Security often taken into account when the system is completed

Security Concepts



Threats: Unauthorised Disclosure

- **Unauthorised disclosure:** is a threat to confidentiality.
  - **Exposure**: This can be deliberate, as when an insider intentionally releases sensitive information. It can also be the result of a human, hardware, or software error, which results in an entity gaining unauthorised knowledge of sensitive data.
  - **Interception**: An unauthorised entity directly accesses sensitive data traveling between authorised sources and destinations. On the internet, a determined attacker can gain access to e-mail traffic and other data transfer.
  - **Inference**: A threat action whereby an unauthorised entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications.
  - **Intrusion**: An unauthorised entity gains access to sensitive data by circumventing a system's security protections

Threats: Deception

- **Deception**: is a threat to either data integrity or system integrity. A circumstance or event that may result in an authorised entity receiving false data and believing it to be true.
  - **Masquerade**: An unauthorised entity gains access to a system or performs a malicious act by posing as an authorised entity.
  - **Falsification**: False data deceive an authorised entity.
  - **Repudiation**: An entity deceives another by falsely denying responsibility for an act.

Threats: Disruption

- **Disruption**: it is a threat to availability or system integrity. A circumstance or event that interrupts or prevents the correct operation of system services and functions.

- **Incapacitation:** Prevents or interrupts system operation by disabling a system component.

- **Corruption:** Undesirably alters system operation by adversely modifying system functions or data.

- **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.

Threats: Usurpation

* *usurpation*: is a threat to system integrity. The following types of attacks can result in this threat consequence: circumstance or event that interrupts or prevents the correct operation of system services and functions.

* *Misappropriation*: An entity assumes unauthorised logical or physical control of a system resource.

* *Misuse*: Causes a system component to perform a function or service that is detrimental to system security. or interrupts system operation by disabling a system component.

HW attacks

Avaliability
Equipment is stolen

Hardware

Confidentiality
An unencrypted CD-ROM or DVD is stolen.

Typically requires physical access

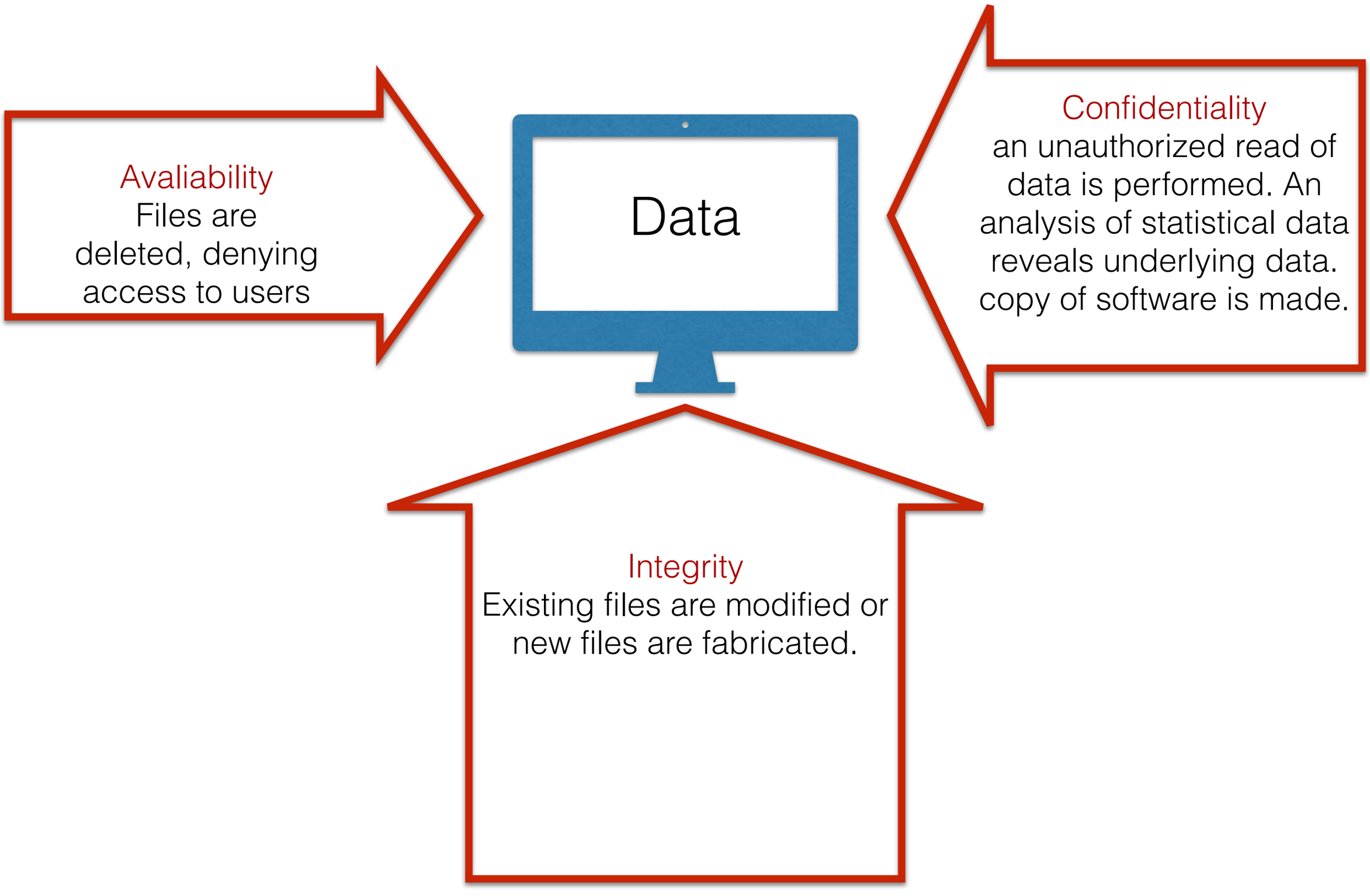
SW attacks

Avaliability
Programs are deleted, denying access to users.

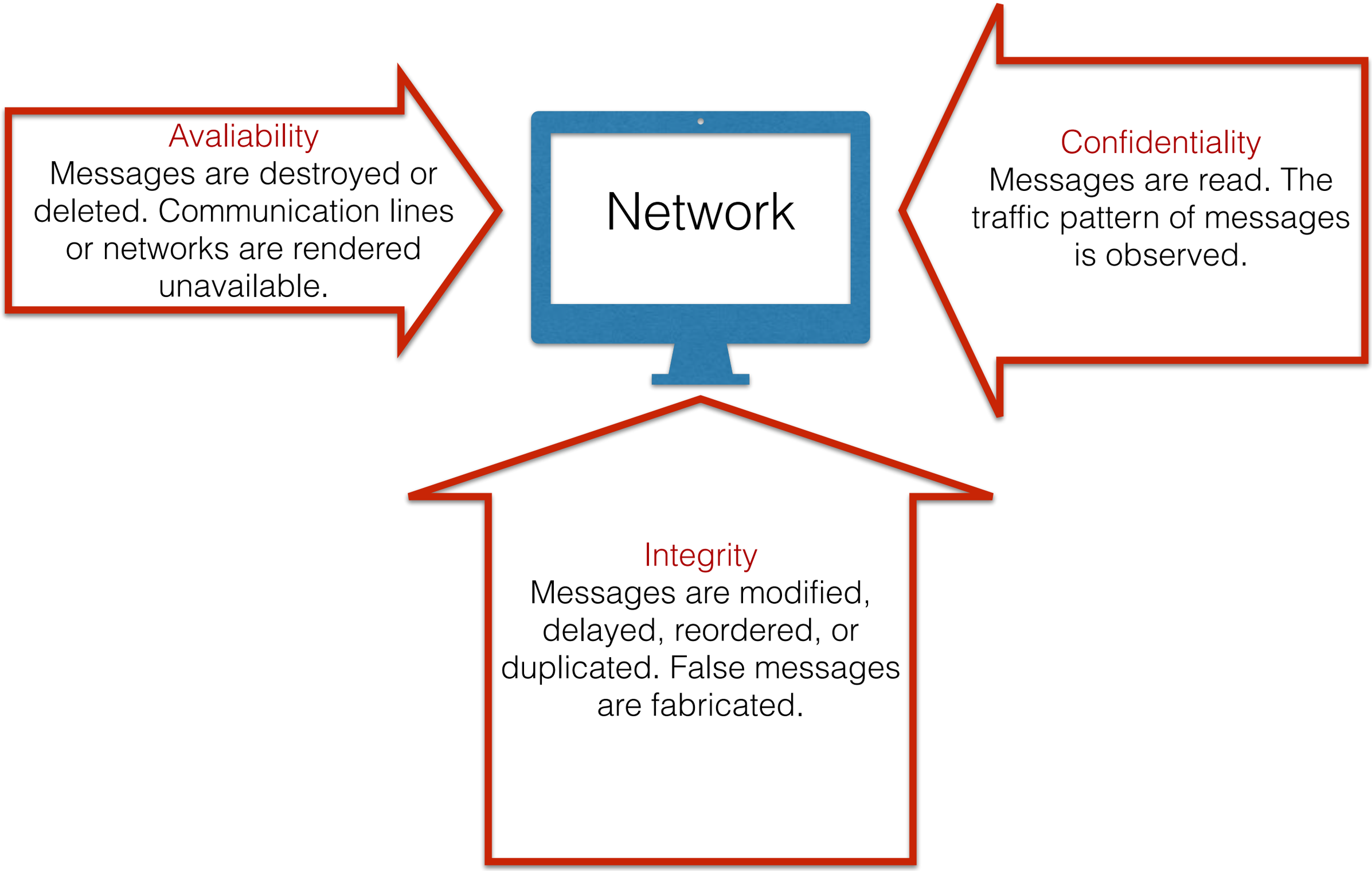
Confidentiality
An unauthorized copy of software is made.

Integrity
A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.

Data attacks



Communication attacks



Communication attacks

- Passive attacks: learn or make use of information from the system but does not affect system resources
  - The goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.
  - Passive attacks are very difficult to detect because they do not involve any alteration of the data. The emphasis is on prevention
- Active attacks: involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:
  - Replay, masquerade, modification of messages, and denial of service.
  - Easier to detect but more difficult to prevent

Easiest Breach Principle

Easiest breach: we have to take into account that an intruder may use any possible violation technique

- The security breach:
  - it is not performed in the most obvious way
  - it is not necessarily the one against which we have strongest protection techniques
  - it does not describe the behaviour that we think the intruder has
  - penetration test has to be repeated in time (especially when the system is modified)

IT security

it is a game whose rules are respected only by the defending team

Design Principles

- Despite years of research and development, it has not been possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions.

- In the absence of such foolproof techniques, it is useful to have a set of *widely agreed design principles* that can guide the development of protection mechanisms

Economy of Mechanism

> *Principle of Economy of Mechanism*
>
> The security mechanisms should be as simple and small as possible

* If a design and the implementation are simple, there are less possibilities to make errors
* The *testing* and *verification* processes are less complex
* With a *complex design*, there are many more opportunities for an adversary to discover *subtle weaknesses* to exploit that may be difficult to spot ahead of time.
* *Complex mechanism* are more likely to possess *exploitable flaws*. Simple mechanisms tend to have fewer exploitable flaws and require *less maintenance.*

Economy of Mechanism

> *Principle of Economy of Mechanism*
>
> The security mechanisms should be as simple and small as possible

* *Complex systems* make usually *assumptions* about the system in which they run
  - ✓ *if the assumptions are incorrect there can be security problems*
* Furthermore, updating or replacing a simple mechanism is a less intensive process. In practice, this is perhaps the most difficult principle to honor. There is a constant demand for new features in both hardware and software, complicating the security design task. The best that can be done is to keep this principle in mind during system design to try to eliminate unnecessary complexity.

Fail-Safe Defaults

> *Principle of Fail-Safe Defaults*
>
> Unless a subject is given explicit access to an object, it should be denied access to that object

- That is, the *default situation is lack of access*, and the protection scheme identifies conditions under which access is permitted.
- This approach exhibits a better failure mode than the alternative approach, where the default is to permit access.
- If a subject is unable to complete its task it has to delete all the modifications to the security state before terminating
  - ✓ In this way, even if the process fails the system is still safe

Complete Mediation

> *Principle of Complete Mediation*
>
> Requires to check all accesses to objects in order to ensure that they are allowed

- Whenever a subject attempts to read an object, the security system should mediate the action
  - ✓ it determines whether the subject has the right to access the object
  - ✓ If so, it provides the resources necessary
  - ✓ If the subject tries to access the object *again*, the system should check that the subject is still allowed to access the object
  - ✓ Most systems would not make the second check and cache the first result for successive access
- To fully implement complete mediation, every time a user reads a field or record in a file, or a data item in a database, the system must exercise access control. *This resource-intensive approach is rarely used.*

Open Design

Principle of Open Design

States that the security of a mechanism should not depend on the secrecy of its design or implementation

- Designers and implementers should not base their security mechanisms on the protection of the design and implementation details
- If the strength of a security system is based on the ignorance of the user, a learned user may defeat the system
- These details can be learned by reverse engineering or other means
- It is anyway true for cryptographic systems and software where the security is guaranteed by the secret key and not by the secrecy of the encoding algorithms
- The experience teaches that hiding the encoding algorithms adds very little to the security strength of the system

Separation of Duties

Principle of Separation of Duties

If two or more steps are necessary for performing a critical action, then there must be two different users that execute these actions.

- To move a product from the development phase to the production phase is a critical process
  - ✓ Suppose that a programmer made a wrong assumption in the development of the program
  - ✓ The following phase has also to verify the soundness of the program, with respect to the specifications
  - ✓ The mistake is easily detected if the *verifier* is different from the *developer*

Separation of Privileges

Principle of Separation of Privileges

A system should not grant permission based on a single condition

- Multiple privilege attributes are required to achieve access to a restricted resource
- Similar to the separation of duties
  - ✓A check with a value greater than $75.000 needs two signatures
  - ✓Systems and programs that grant access to resources should do it only when more than one condition is satisfied

Least Privilege

Principle of Least Privilege

A subject should be given only those privileges that it needs in order to complete its tasks.

- Every process and every user of the system should operate using the least set of privileges necessary to perform the task.
- If a subject *does not need* an access right, it should not have that right
- The *role* of the subject should control the right assignment
- The right should be *extendable on demand*
- Many systems have not the granularity of privileges and permissions required to apply this principle precisely
- This principle requires that processes should be confined to a protection domain as small as possible

Least Privilege

Principle of Least Privilege

A subject should be given only those privileges that it needs in order to complete its tasks.

* **Temporal aspect:** system programs or administrators who have special privileges should have those privileges only when necessary; when they are doing ordinary activities the privileges should be withdrawn. Leaving them in place just opens the door to accidents.

Least Common Mechanism

> *Principle of Least Common Mechanism*
>
> States that mechanisms used to access resources should not be shared

* The design should minimize the functions shared by different users, providing mutual security. This principle helps reduce the number of unintended communication paths and reduces the amount of hardware and software on which all users depend, thus making it easier to verify if there are any undesirable security implications.

* Sharing resources provides a channel along which information can be transmitted
  - ✓ This sharing should be minimized

* Confinement problem

Psychological Acceptability

Principle of Psychological Acceptability

Security mechanisms should not make te resource more difficult to access than if the security mechanisms were not present

- If security mechanisms hinder the usability or accessibility of resources, users may opt to turn off those mechanisms.
- To configurate and use a system should be as easy and as intuitive as possible
- The outputs should be clear, direct and useful
  - ✓ If a security SW is hard to configure, the administrators could make mistakes causing security problems
  - ✓ If a password is rejected, the program should clearly describe why the password was rejected, not only provide an error message

Psychological Acceptability

Principle of Psychological Acceptability

Security mechanisms should not make te resource more difficult to access than if the security mechanisms were not present

- In addition to not being intrusive or burdensome, security procedures must *reflect the user's mental model of protection*. If the protection procedures do not make sense to the user or if the user must translate his image of protection into a substantially different protocol, the user is likely to *make errors*.

- This principle is interpreted to mean that the security mechanism may add some extra burden, but it must be both reasonable and minimal.

Isolation

Isolation

The easiest form of protection is isolation

- Limit the number of systems on which critical information is stored and *isolate them*, either physically or logically.
- *Physical isolation:* no physical connection exists between a public access information resources and a critical information.
- When implementing *logical isolation* solutions, layers of security services and mechanisms should be established between public systems and secure systems responsible for protecting critical resources.
- The processes and files of individual users should be isolated from one another except where it is explicitly desired.

Modularity

- Development of *security functions as separate, protected modules:*
- The design goal here is to *provide common security functions and services*, such as cryptographic functions, *as common modules*.
- For example, numerous protocols and applications make use of cryptographic functions. Rather than implementing such functions in each protocol or application, a more secure design is provided by developing a common cryptographic module that can be invoked by numerous protocols and applications. The design and implementation effort can then focus on the secure design and implementation of a single cryptographic module, including mechanisms to protect the module from tampering.

Layering

- Use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.
- By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected.
- Layering approach is often used to provide multiple barriers between an adversary and protected information or services. This technique is often referred to as *defense in depth.*

Computer Security Strategy

- A comprehensive security strategy involves three aspects:
  - Specification/*policy*: What is the security scheme supposed to do?
  - Implementation/*mechanisms*: How does it do it?
  - Correctness/*assurance*: Does it really work?

Security Policies

- A *security policy* is a formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
- In developing a security policy, a security manager needs to consider:
  - The value of the assets being protected
  - The vulnerabilities of the system
  - Potential threats and the likelihood of attacks
- And the following trade-offs:
  - *Ease of use versus security*: all security measures involve some penalty in the area of ease of use.
  - *Cost of security versus cost of failure and recovery*: In addition to ease of use and performance costs, there are direct monetary costs in implementing and maintaining security measures. All of these costs must be balanced against the cost of security failure and recovery if certain security measures are lacking.

Security Mechanisms

- *Prevention*: An ideal security scheme is one in which no attack is successful. Although this is not practical in all cases, there is a wide range of threats in which prevention is a reasonable goal.

- *Detection*: In a number of cases, absolute protection is not feasible, but it is practical to detect security attacks.

- *Response*: If security mechanisms detect an ongoing attack, such as a denial of service attack, the system may be able to respond in such a way as to halt the attack and prevent further damage.

- *Recovery*: An example of recovery is the use of backup systems, so that if data integrity is compromised, a prior, correct copy of the data can be reloaded.

Security Assurance

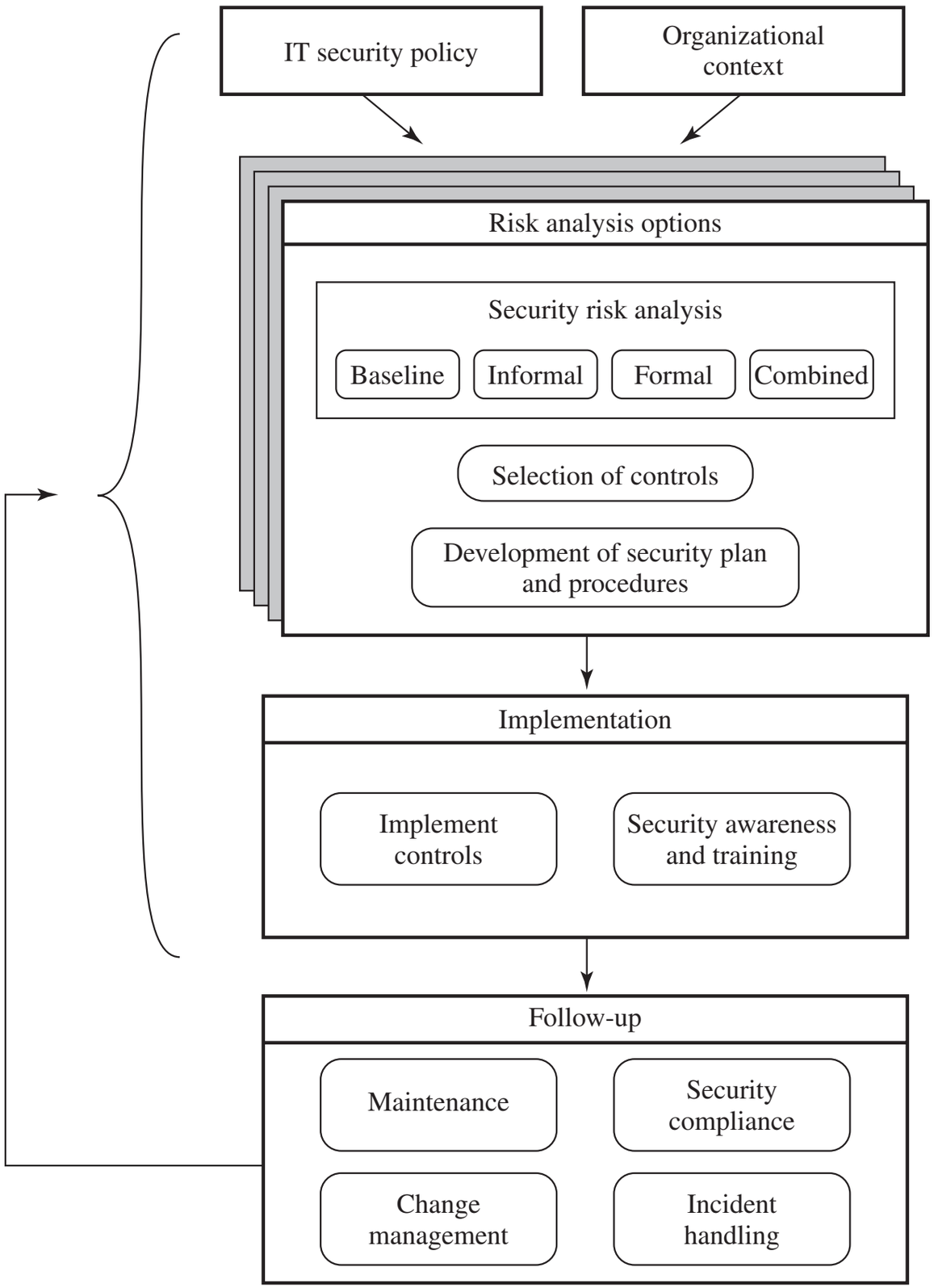
- Those who are "consumers" of computer security services and mechanisms (e.g., system managers, vendors, customers, and end users) desire a belief that the security measures in place work as intended

- *Assurance:* degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes.

  - Does the security system design meet its requirements?

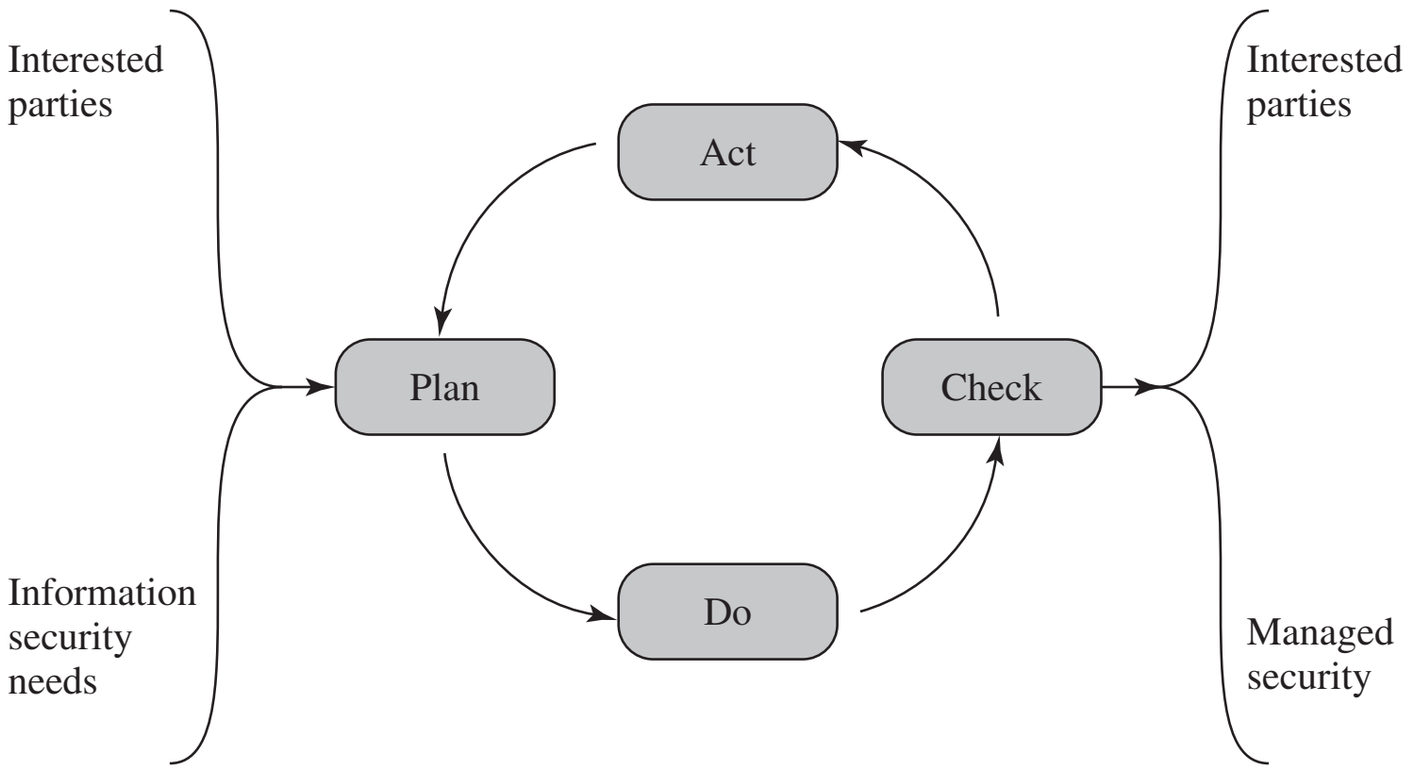
  - Does the security system implementation meet its specifications?

IT Security Management



- IT security management needs to be a key part of the overall management plan.
- IT security risk assessment process should be incorporated into the wider risk assessment of all the organization's assets and business processes.
- IT management is not something undertaken just once. Rather it is a *cyclic process* that must be repeated constantly in order to keep pace with the rapid changes in both IT technology and the risk environment.

Plan-Do-Check-Act



- The iterative nature of the IT security management leads to a model process that comprises the following steps:
  - ✓**Plan**: Establish security policy, objectives, processes and procedures; perform risk assessment; develop risk treatment plan with appropriate selection of controls or acceptance of risk.
  - ✓**Do**: Implement the risk treatment plan.
  - ✓**Check**: Monitor and maintain the risk treatment plan.
  - ✓**Act**: Maintain and improve the information security risk management process in response to incidents, review, or identified changes.