NETWORK SECURITY

"General concepts"

Corso di Laurea Magistrale in Ingegneria Informatica

Prof. Simon Pietro Romano

spromano@unina.it

CREDITS

- Some of the figures in this presentation are taken from educational material created by William Stallings and made available to instructors on the Pearson publishing website
- The same applies to parts of the slide content
- Another source of inspiration for this lecture is the course material for Network Security taught at Columbia University by Prof. Bellovin

"It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him; not to presume that he will not attack, but rather to make one's self invincible."

- The Art of War, Sun Tzu

OBJECTIVES

- Security Triad:
  - Confidentiality, Integrity, Availability
- Requirements to be ensured in two distinct domains:
  - on network connections ('on-the-wire')
  - in end-systems
- Strategies differ significantly in the two mentioned domains

HOST/NETWORK DICHOTOMY

- Hosts are typically (or can be) well controlled
  - well-established authentication and authorization models
  - a clear concept of 'privileged state'
- None of this holds true when examining the network!

NETWORKS AND "ANARCHY"

- Anyone can connect to the network
- Connectivity can be 'controlled' at most in very restricted contexts subject to appropriate regulation
- Different operating systems have very different concepts of ownership, such as:
  - user identifiers
  - user privileges
- There is therefore no shared definition of what a 'privilege' is in a network of heterogeneous computers

WHY DOES EVERYTHING BECOME MORE COMPLICATED WITH NETWORKS?

- "Because networks, by their nature, always interconnect!"
  - [Citation] *Bellovin's Laws of Networking*...
- Because networks typically interconnect at the frontier ('edge') rather than in the central parts ('core'):
  - it is practically impossible to think of centralized mechanisms for controlling (and enforcing) security policies

"BENIGN" FAILURES

- The vast majority of computer network failures are benign in nature:
  - data corruption in transit
  - timeouts
  - end-systems being offline
  - reachability issues (routing)
- Any network program must take these types of failures into account
- General rule:

"Anything that can happen by mistake can certainly happen on purpose!"

COMPUTER SECURITY vs NETWORK SECURITY

- Computer Security:
  - a generic term used to refer to the set of tools designed to protect data and block hackers
- Network Security:
  - a specific term used to indicate all actions that can be taken to deter, prevent, and correct security breaches involving the transmission of information between distributed entities

FURTHER DEFINITIONS*

- Vulnerability:
  - an error or imperfection in the design, implementation, or operational procedures of a system
- Attack:
  - a way of exploiting one or more vulnerabilities in a system
- Threat:
  - an adversary who is motivated and capable of exploiting a vulnerability in a system

*"Trust in Cyberspace", Fred B. Schneider [Editor]

VULNERABILITY

- The technical failure of a system
- The central topic of any security course
- Question:

"If we removed all vulnerabilities, would threats still exist?"

VULNERABILITIES: HOST AND NETWORK

- In a network, there are:
  - hosts or end-systems:
    - clients and servers
    - peer entities in a peer-to-peer (P2P) network
  - the network itself, meaning the connections:
    - wired
    - wireless
- We must protect both hosts and the network itself
  - different vulnerabilities
  - different techniques

HOST VULNERABILITIES

- In this course, the host is of interest as a network node
- Objective:
  - Prevent an attacker from penetrating a network node (typically by exploiting a flawed application)
- If the flawed application is used solely to compromise the host's security:
  - security problem related to the Operating System and the application
- If the application can be modified to perform unwanted actions on the network:
  - network security problem
- The boundary between these two categories mentioned above is VERY blurred...

NETWORK VULNERABILITIES

- What can a potential attacker do?
- Where is the attacker located (physically)?
- What are we intending to protect?
  - the network is actually a complex set of interoperating protocol layers

VULNERABILITIES IN A "LAYERED" WORLD

- Every layer has its weaknesses:
  - Link Layer:
    - e.g.: ARP spoofing
  - Network Layer:
    - e.g.: IP ‘address forgery’
  - Transport Layer:
    - e.g.: TCP sequence number guessing
  - Application Layer:
    - e.g.: worms sent via e-mail

ARP SPOOFING

- Translation of IP addresses into local network addresses

```
spromano$ tcpdump -ennqti en1 \( arp  \)
listening on en1, link-type EN10MB (Ethernet), capture size 65535 bytes
ARP, length 42: Request who-has 192.168.178.20 tell 192.168.178.1, length 28
ARP, length 42: Reply 192.168.178.20 is-at 00:23:12:0f:82:de, length 28
```

- And if we replied instead of someone else?
  - the first reply 'usually' wins...

3-WAY HANDSHAKE IN TCP

$C \rightarrow S : SYN(ISN_C)$

$S \rightarrow C : SYN(ISN_S), ACK(ISN_C)$

$C \rightarrow S : ACK(ISN_S)$

$C \rightarrow S : data$

- In some (obsolete) versions of TCP, the Initial Sequence Number (ISN) is incremented by a constant value 'k' after each connection and every 500 milliseconds...

“SEQUENCE NUMBER GUESSING” ATTACK

- X starts a legitimate connection with S to learn the value of ISN_S :

$$X \rightarrow S : SYN(ISN_X)$$

$$S \rightarrow X : SYN(ISN_S), ACK(ISN_X)$$

- X pretends to be T:

$$X \rightarrow S : SYN(ISN_X), SRC = T$$

$$S \rightarrow T : SYN(ISN_S + k), ACK(ISN_X)$$

$$X \rightarrow S : ACK(ISN_S + k), SRC = T,$$

$$X \rightarrow S : SRC = T, \text{‘attack data’}$$

SEQUENCE NUMBER GUESSING: PROBLEMS

- T sees the 'SYN+ACK' segment sent by S:
  - according to the specification, it will respond with a 'RESET' (RST) segment
- X must prevent this from happening
  - Possible solutions:
    - impersonate a non-active host ('dead host')
    - launch a parallel Denial of Service (DoS) attack towards T to prevent it from sending the RST segment
- However:
  - very often, firewalls do not forward packets associated with connections they have not initiated
    - in this case, host T will never see the SYN+ACK segment and, consequently, will not send the RST segment!
  - …the so-called 'side-effects' of security mechanisms

THE HUMAN FACTOR!

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed, but they are sufficiently pervasive that we must design our protocols around their limitations."

Kaufman et al.

THREATS

- Different adversaries have different characteristics and skills
- A novice hacker will never be able to breach a modern cryptographic algorithm
- An experienced hacker, on the other hand, is capable of exploiting the so-called '3 Bs':
  - 'Burglary':
    - breaking and entering (into a home, but also into a network resource...)
  - 'Bribery':
    - Corruption
  - 'Blackmail':
    - Extortion

    https://hbr.org/2009/10/when-hackers-turn-to-blackmail-2
- Any secure system project heavily depends on understanding the enemy!

THREATS AND HACKER TYPES

- Hackers for fun (joy hackers)
  - some are simple 'skiddies'...
  - ...while others are very skilled
- Keep in mind:
  - scripts are often very sophisticated (and can cause a lot of damage)
  - hackers are more likely to share their tools than so-called 'good guys'

ARE JOY HACKERS A PROBLEM?

- They have fun...
- ...but:
  - we have to rebuild successfully attacked nodes
  - we make a fool of ourselves when the news gets out!
  - we risk losing our job if our role in the company is that of a system administrator ☹

HACKING AND COLD, HARD CASH

- Hackers are often also spammers and phishers
- The main motivation for a hacker today is money
- The possibility of profiting from hacking activities has:
  - attracted talented individuals to this new arena
  - stimulated the development of highly sophisticated attack techniques
    - most viruses and worms produced lately are designed to turn victims' computers into members of so-called 'botnets'
  - this has significantly reduced cases of pure vandalism in favor of situations of organized cybercrime

INDUSTRIAL ESPIONAGE

- A minimal percentage of attacks are actually detected
- Very often, the goal of professional attackers is to:
  - penetrate an organization's system
  - assume a profile as 'normal' as possible once inside
  - gather, transmit, and process information about the organization
- In this case, we're talking about 'Advanced Persistent Threats' (APTs)

PROFESSIONAL HACKERS

- More often than one might imagine, they use non-technical tools:
  - social engineering
  - bribery
  - wiretapping
- The professionals:
  - know what they are doing
  - know what they want

AND WHAT IF THE PROBLEM LIES WITHIN?

- The problem of 'insiders' (people within the organization):
  - they know your assets
  - they know your weaknesses
  - they are 'behind' the corporate firewall
  - sometimes, they turn against you
    - what happens if the system administrator switches sides?

ELSEVIER

Computers & Security

Volume 133, October 2023, 103410

Including insider threats into risk management through Bayesian threat graph networks

Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano

Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2023.103410

Get rights and content

Abstract

Cybersecurity incidents do represent a serious danger for companies. In fact, the number of cyber crimes is exponentially growing in a scenario where the global COVID-19 pandemic determined several conditions that have negatively affected companies' cyber-security posture. The adoption of risk management processes can help reduce security threats and mitigate both financial and reputation losses. In computer systems, it is crucial to relate security risks to the system infrastructure. Bayesian attack graph models can help reach such a goal. The approach is very effective as it allows to define the attack paths an attacker would perform against a specific network infrastructure. In this way, it is possible to construct a truthful representation of a company's security risks that cannot be obtained with other approaches. Still, Bayesian risk management approaches are usually based on advanced threats. Namely, those threats relate to vulnerabilities that

AND THE SPIES?

- Some governments might be interested in uncovering the secrets of a specific technology...
- ...and they are willing to pay handsomely to obtain them
- Cyber spies are typically highly professionalized and well-paid
- ...and they often compete with each other to gain new market shares!
- Ever heard of the Italians from 'Hacking Team'?

https://www.repubblica.it/tecnologia/sicurezza/2015/07/06/news/hackerato_hacking_team-118452298/

A LOOK AT THE STANDARDS

OSI SECURITY ARCHITECTURE

- "Security attack":
  - any action that compromises the security of information held by an organization
- "Security mechanism":
  - a process (or a device that incorporates such a process) designed to detect, prevent, or recover from an attack
- "Security service":
  - a processing or communication service that enhances the security of an organization's information processing and transfer
  - designed to respond to security attacks
  - based on one or more 'security mechanisms'

MORE ON THREATS AND ATTACKS [RFC4949]

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

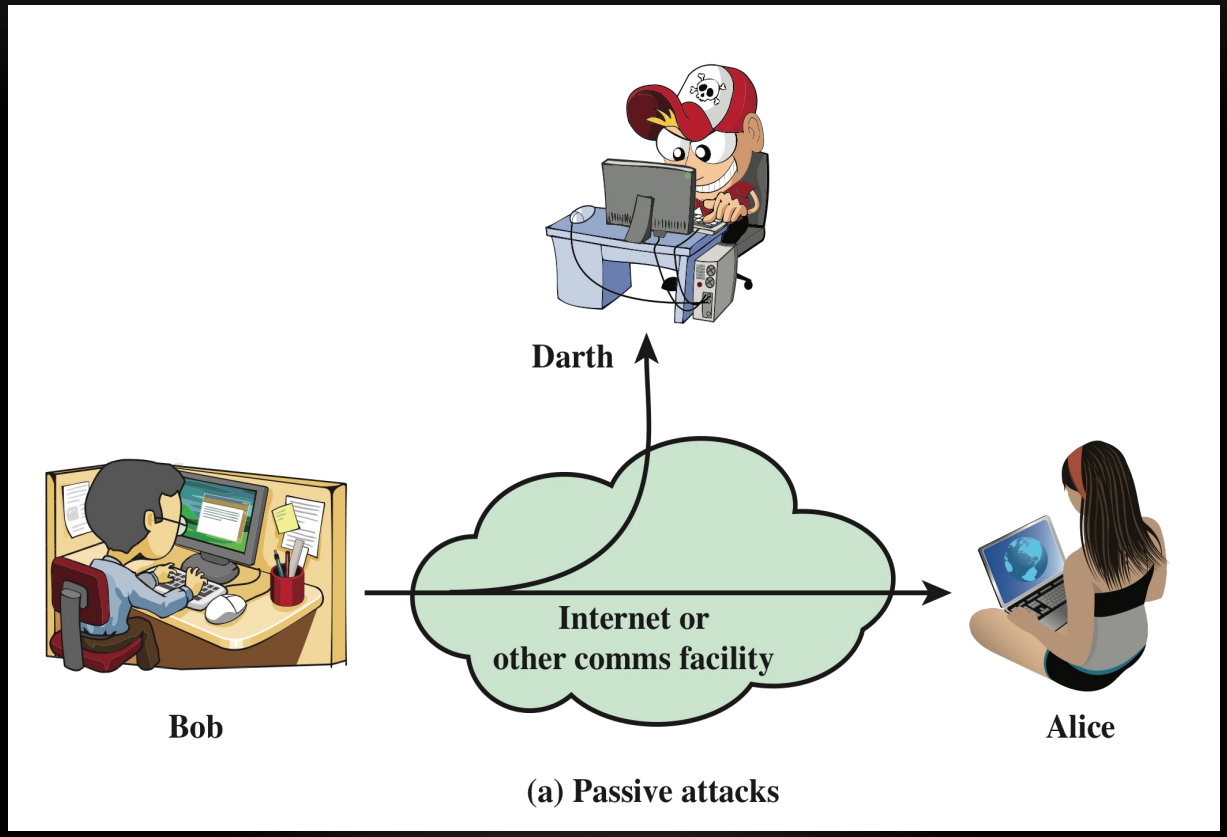
Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

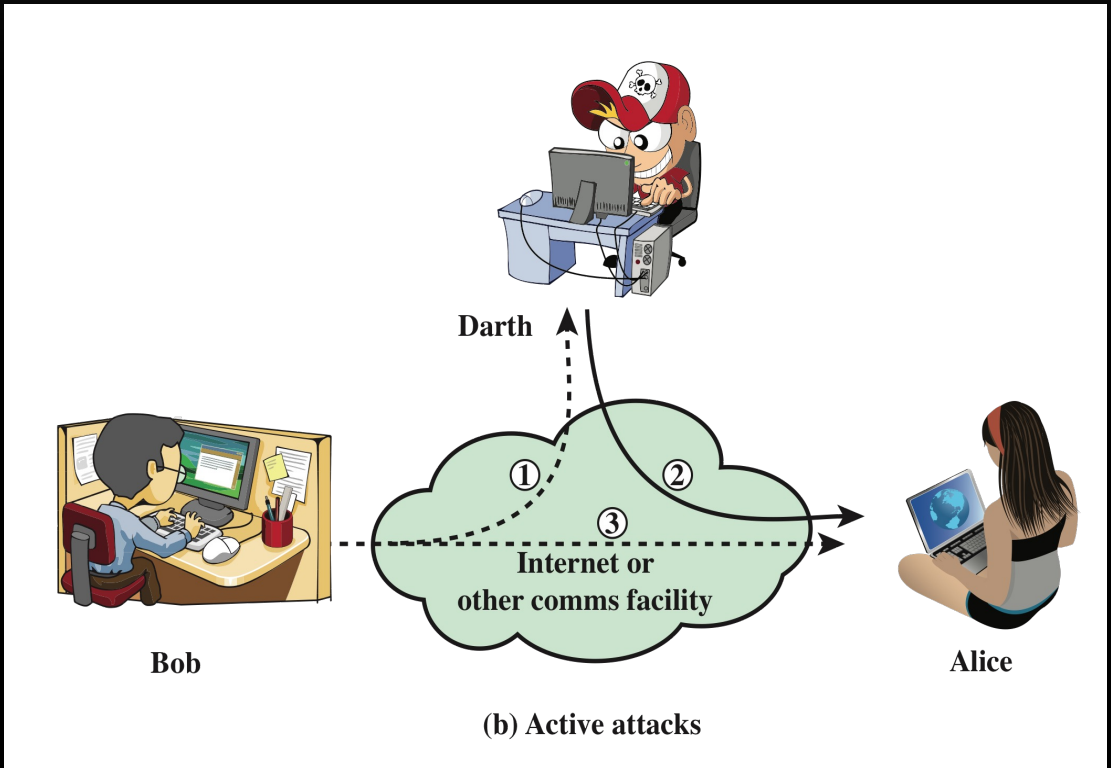
ATTACKS [RFC4949]

- "Passive attack":
  - an attempt to learn or make use of information from the target system(s)
  - has no obvious impact on the system's resources
- "Active attack":
  - an attempt to alter the system's resources or interfere with its normal operation

PASSIVE ATTACKS [Stallings]



ACTIVE ATTACKS [Stallings]



CHARACTERISTICS OF PASSIVE ATTACKS

- Typically used for:
  - eavesdropping
  - monitoring
- Main objective:
  - obtain useful information contained in transmitted data
- Classic types of attacks:
  - access to message content
  - traffic analysis

CHARACTERISTICS OF ACTIVE ATTACKS

- They involve modifying (at least partially) the flow of data or creating 'fake' data streams
- Difficult to prevent due to the enormous variety of potential vulnerabilities at the physical, software, or network level
- Defense strategies in these cases aim to:
  - detect the attack
  - restore the system from any damage or slowdown caused by it

ACTIVE ATTACKS: TYPES

SECURITY SERVICES

- According to the X.800* standard :

"A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers"

- According to RFC 4949:

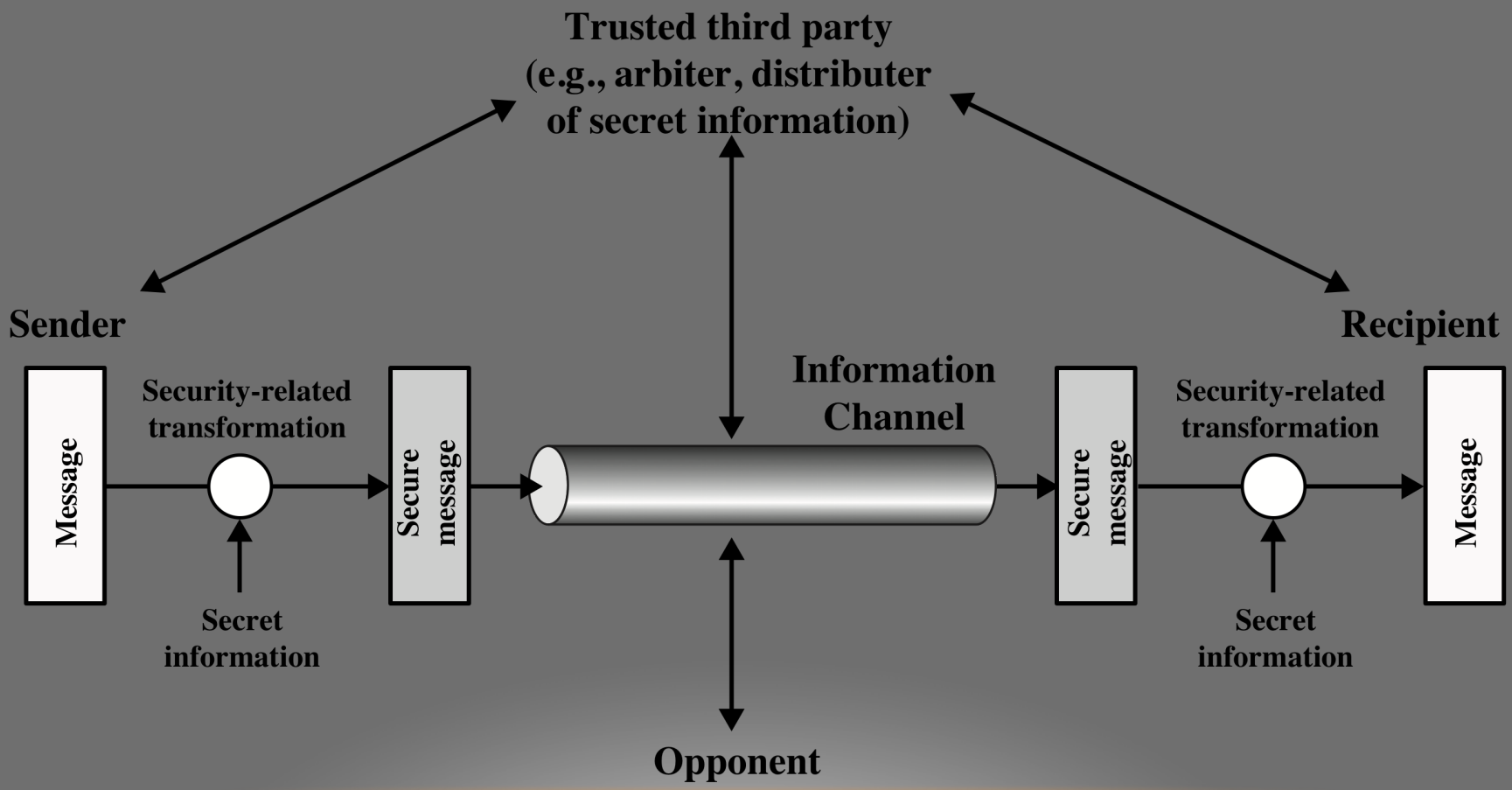
"A processing or communication service provided by a system to give a specific kind of protection to system resources"

*X.800 : Security architecture for Open Systems Interconnection for CCITT applications

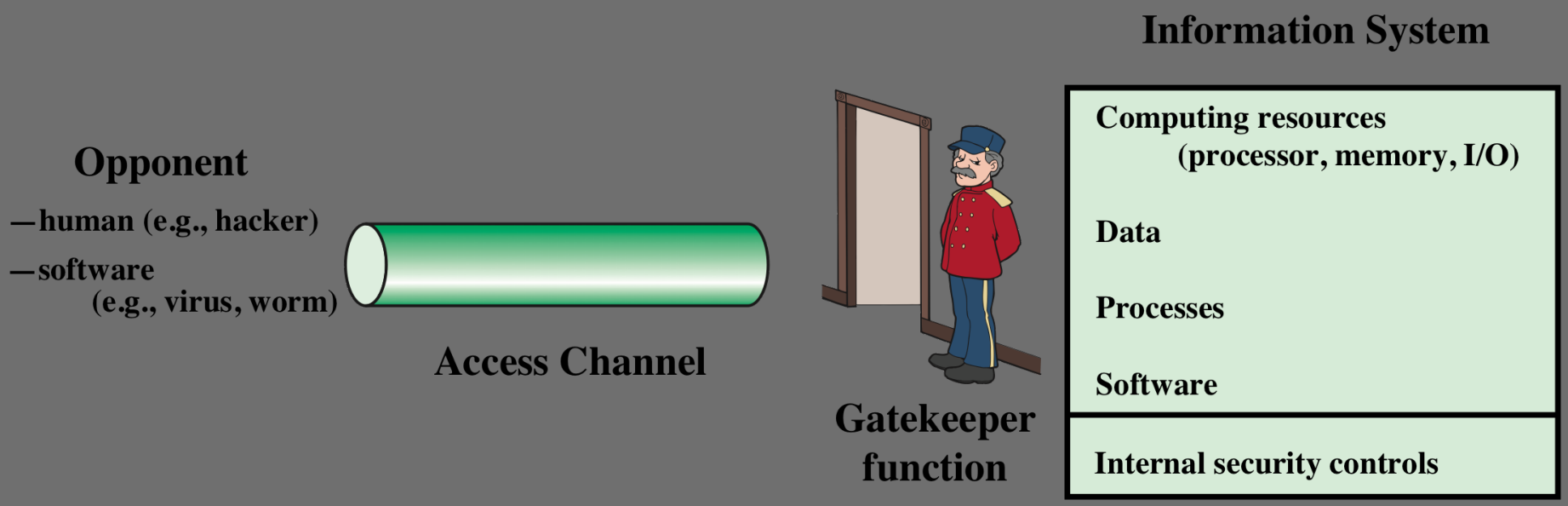
X.800 SERVICE CATEGORIES

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation

A MODEL FOR NETWORK SECURITY

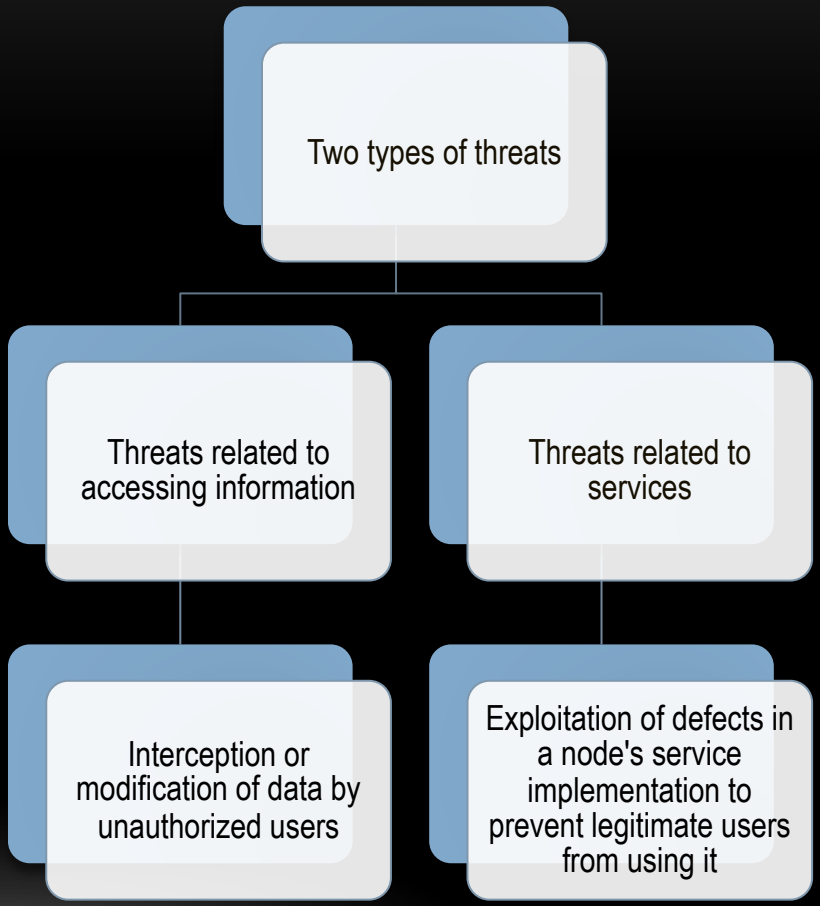


A SECURITY MODEL FOR NETWORK ACCESS



UNAUTHORIZED ACCESS

- Introduction, within a node, of mechanisms capable of exploiting vulnerabilities in the system and that can affect both application programs and utility programs



STANDARDS AND ORGANIZATIONS

NIST

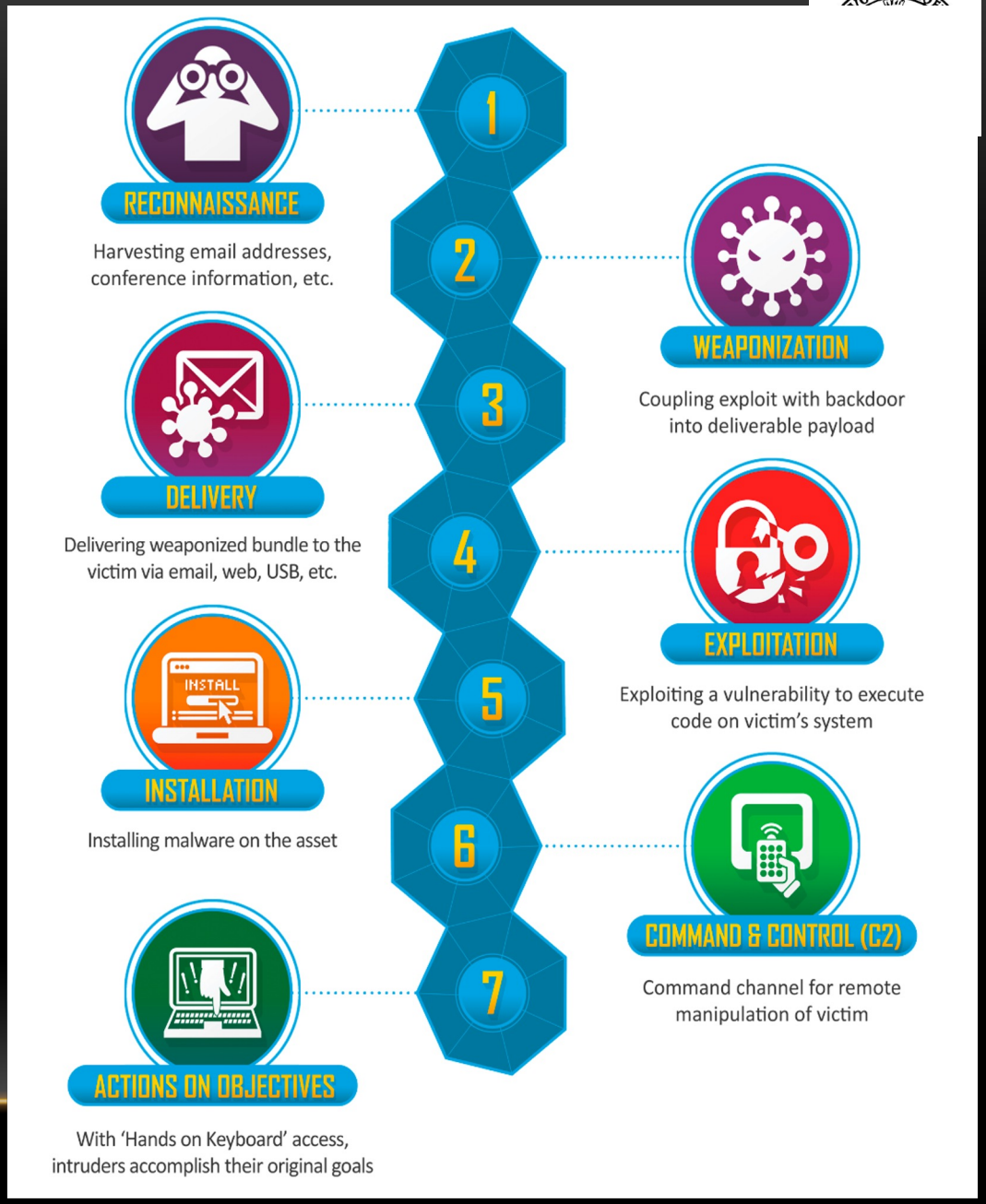
- National Institute of Standards and Technology
- The federal American agency responsible for measurement science, standards, and technologies related to the use by the United States government, as well as promoting innovation in the private sector
- Documents issued by NIST have a global impact :
  - NIST Federal Information Processing Standards (FIPS)
  - Special Publications (SP)

ISOC

- Internet Society
- A global society of professionals who participate, on an individual basis, in the definition, management, and evolution of the Internet
- The parent organization of groups that oversee standards for the infrastructure of the Internet, including the IETF (Internet Engineering Task Force) and the IAB (Internet Architecture Board)
- Internet standards (de facto) are published in the form of "Requests for Comments" (RFCs)

CYBER KILL CHAIN

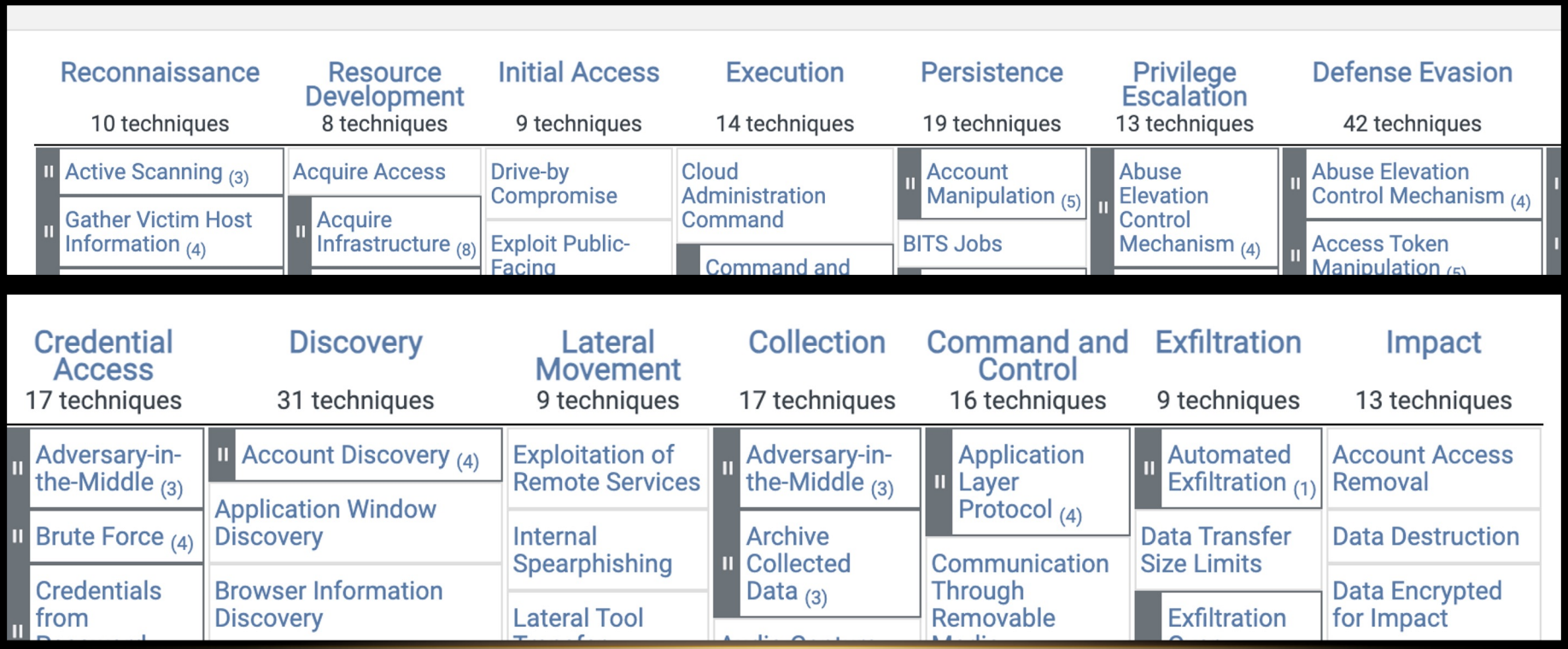
Conceptual model describing the stages of a cyber attack, from information gathering to achieving objectives, providing a detailed understanding of the attack process



MITRE ATT&CK

It catalogs the tactics and techniques used by attackers during a hacking operation, providing a detailed overview of the phases and objectives of a cyber attack

https://attack.mitre.org/



CYBER KILL CHAIN VS. MITRE ATT&CK

SIMULATED/EMULATED ENVIRONMENTS

There are many services, some free and others paid, that allow you to practice, including:

- Hack The Box (paid, but some rooms are free)
  - https://www.hackthebox.com/
- TryHackMe (paid, but some rooms are free)
  - https://tryhackme.com/
- PortSwigger Academy (free, but only for web vulnerabilities)
  - https://portswigger.net/web-security/all-topics

QUESTIONS?