Introduction

CSE 565: Fall 2024
Computer Security

Xiangyu Guo (xiangyug@buffalo.edu)

University at Buffalo

Overview

- Syllabus overview
  - Logistics
  - Teaching team
  - Course policy: academic integrity, grading
  - Recommend resources
  - Tentative schedule
- Course overview
  - Goal
  - What is Computer Security
  - A realworld example

Syllabus overview

Logistics

- Course homepage:
  - https://www.buffalo.edu/~xiangyug/teaching/cse565-fall24/index.html
- Piazza: primary channel for any course-related Q&As
  - Sec B: https://piazza.com/buffalo/fall2024/cse565b
  - Sec C: https://piazza.com/buffalo/fall2024/cse565c
- UB Learns (a.k.a. Brightspace):
  - Lecture recordings
  - homework submission & checking grades

Logistics

- Materials (syllabus, announcements, homework, labs): will be posted both on course homepage & Piazza
- Q&As: handled by Piazza only
  - Post in the right category
  - Mark a questions as “Resolved” when it is resolved
- Do **NOT** send emails for course-related issues, unless emergency (or Piazza is down).

Teaching team

Instructor

- Dr. Xiangyu Guo
- Email: xiangyug@buffalo.edu
- Office: Davis Hall 318
- Homepage: https://www.buffalo.edu/~xiangyug/
- Office hours: Tue & Thu, 11:00 am - 12:00 pm
  - Both in-person at Davis 318 & virtual at https://buffalo.zoom.us/j/92961665527?pwd=2vmKd5ZXebEA7EK2hKGoiQqK6HQc7M.1

Teaching team

TA / Graders

- TAs (OH on course page)
  - Gaoxiang Liu (gliu25@buffalo.edu)
  - Jiawei Guo (jiaweigu@buffalo.edu)
  - Yu Nong (yunong@buffalo.edu)
  - Isabelle Ondracek (ikondrac@buffalo.edu)
- Graders
  - Not finalized yet
  - No OH but will answer grading-related questions on Piazza

Academic Integrity

- To understand your responsibilities as a student read: UB Student Code of Conduct

- Plagiarism or any form of cheating in homework, or exams is subject to serious academic penalty

- LLMs (ChatGPT, Claude.ai, Mistral AI, etc) prohibited unless explicitly allowed.

- Any violation of the academic integrity policy will result in a 0 on the homework or exam, and even an **F** on the final grade. And, the violation will be reported to the Dean's office

Grading Policy

- Components
  - Assignment (4): 20%
  - Projects (4): 30%
  - (In-class) Midterm Exam (1): 20%
  - Final Exam (1): 30%
- Homework/Projects should be done **individually**. The exam will contain several questions *derived* from the assignments/projects
- Homeworks will be submitted via UBlearns; they must be typed (diagrams can be hand-drawn) and normally would need to be submitted as a **PDF**

Grades cutoffs

- Tentative and subject to change and curving:
  - A: >= 90
  - A-: 85 ~ 89
  - B-, B, B+ : 70 ~ 74, 75 ~ 79, 80 ~ 84
  - C-, C, C+: 50 ~ 59, 60 ~ 64, 65 ~ 69
  - D: 40 ~ 50
  - F: < 40

Late Policy

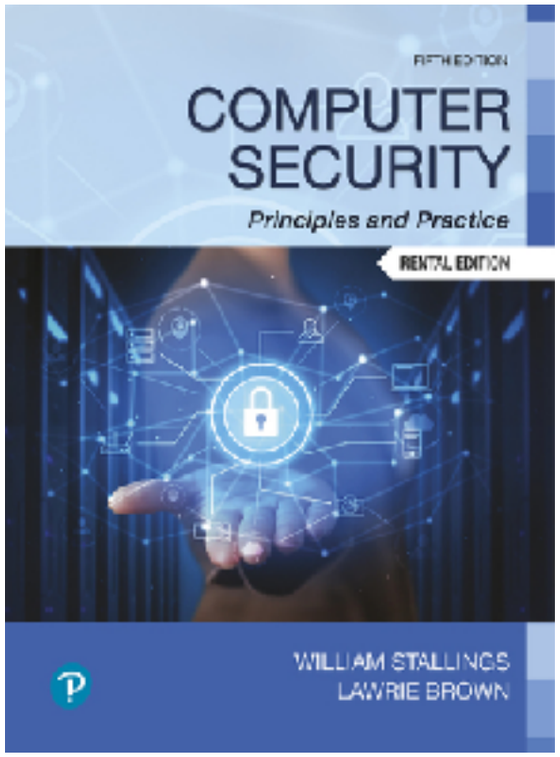
- All assignments are due on the day and time posted.
- You can submit an assignment up to **3 days** late with **daily penalty of 20%, 40%, 60%** out of total points. Latest submission (3 days late) will receive at most 40% of max points even if it's all correct; 0 points if more than 3 days late
- The workload is heavy, you should start the assignments early! Excuses that you did not have enough time for an assignment will not be considered.
- Extreme circumstances will be considered at the discretion of the instructor, contact the instructor via e-mails if you think these apply to you.

Regrading policy

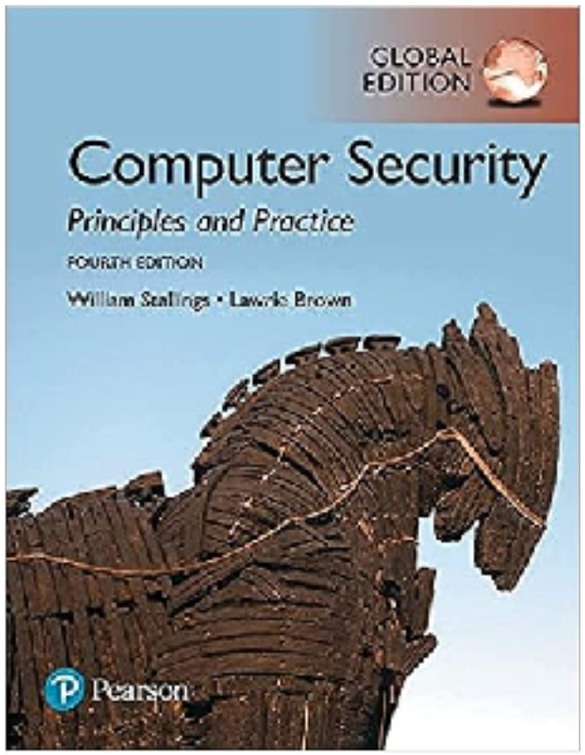
- Submit the regrading request on Piazza.
- Submit **within two weeks** of releasing the graded material to the class.
- The request needs to be in writing clearly describing the error in grading

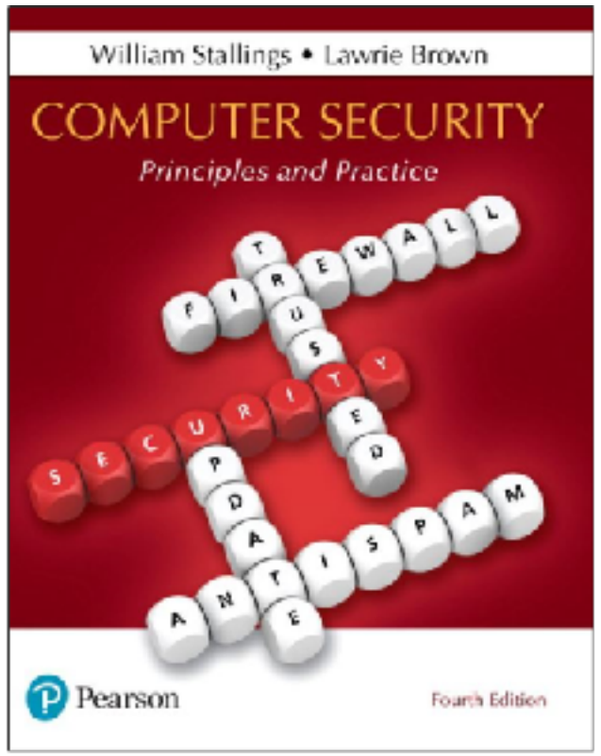
Recommend readings

- William Stallings and Lawrie Brown, *Computer Security: Principles and Practice*, **5th edition, Pearson, 2024** or **4th edition, Pearson, 2017**



5th ed

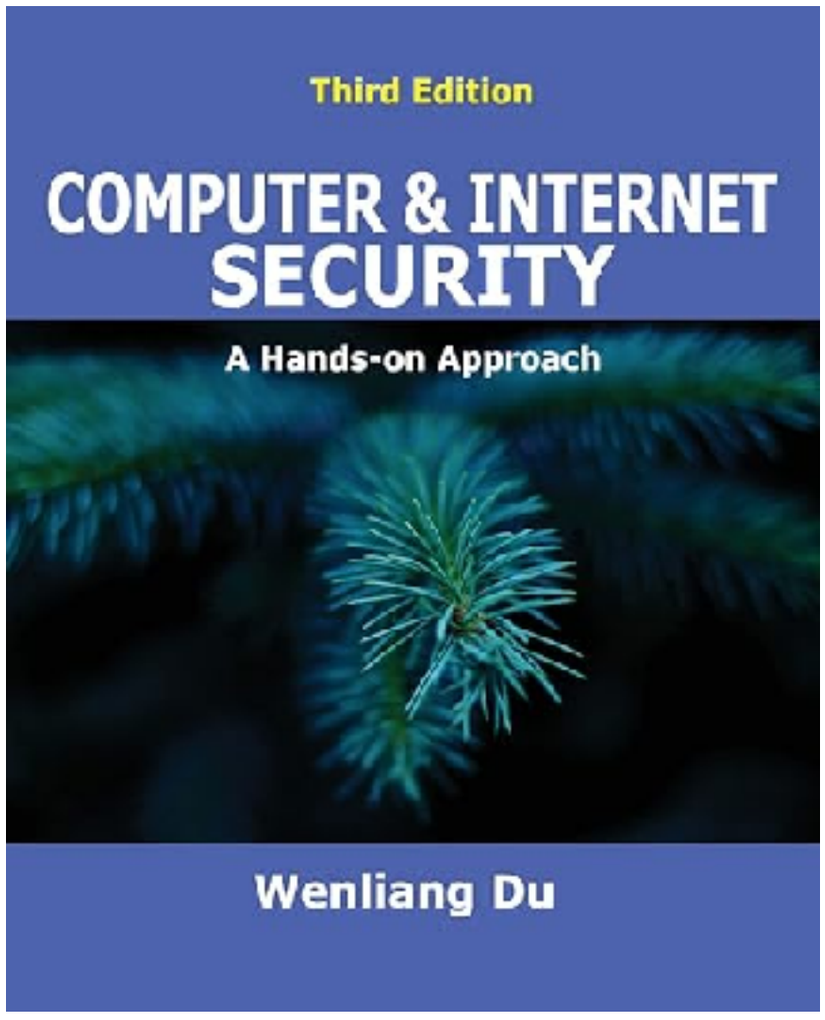




4th ed

Recommend readings

- Wenliang Du, *Computer & Internet Security: A Hands-on Approach,* 3rd Edition, 2022



Additional resources

- Michael T. Goodrich and Roberto Tamassia, *Introduction to Computer Security*, Addison-Wesley, 2011

- Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World*

- Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd Edition, 2020

- Niels Ferguson and Bruce Schneier, *Cryptography Engineering: Design Principles and Practical Applications*.

Practicing playground

- Pico CTF: CTF for beginners. Good for learn all the basics.
- pwn.college: Educational CTF platform maintained by ASU security team. Good for beginners.
- pwnable.kr: A collection of fun challenges.
- cryptopals: Learning cryptography by implementing classical algorithms and attacks
- wargame-nexus: List of CTF playgrounds maintained by Yan Shoshitaishvili

Tentative Schedule

https://www.buffalo.edu/~xiangyug/teaching/cse565-fall24/schedule.html

Date	Topic	Note	HW Release (00:00 EST time)	HW Deadline (24:00 EST time)
Tue 08/27	Overview I: Course Syllabus & Policy			
Thu 08/29	Overview II: Course Overview			
Tue 09/03	Cryptography I: Overview; Algorithm analysis & discrete probability recap			
Thu 09/05	Cryptography II: Symmetric Encryption: Block Ciphers			
Tue 09/10	Cryptography III: Message Integrity; Hash Functions.		Assignment 1 release; Lab 1 Release	
Thu 09/12	Cryptography IV: Public Key algorithms; Digital signature.			
Tue 09/17	Access Control I: Authentication			
Thu 09/19	Access Control II: Authorization			
Tue 09/24	Access Control III: Authorization continued.			Assignment 1 Due; Lab 1 Due
Thu 09/26	Network Security I: Network Basics; ARP protocol.			
Tue 10/01	Network Security II: TCP/IP Basics;		Assignment 2 Release; Lab 2 Release	
Thu 10/03	Network Security III: Attacks on TCP			
Tue 10/08	Network Security IV: Attacks on DNS			
Thu 10/10	Midterm Review			
Tue 10/15	Fall break; No class.			Assignment 2 Due; Lab 2 Due
Thu 10/17	(In Class) Midterm Exam			
Tue 10/22	Web Security I: Basics for web server & SQL		Assignment 3 Release;	
Thu 10/24	Web Security II: SQL injection		Lab 3 Release	
Tue 10/29	Web Security III: Cross-Site Scripting (XSS) Attack; Cross-Site Request Forgery (CSRF) Attack			
Thu 10/31	Software Security I: Assembly basics			
Tue 11/05	Software Security II: Buffer Overflow			Assignment 3 Due;
Thu 11/07	Software Security III: Buffer Overflow Defense			Lab 3 Due.
Tue 11/12	Software Security IV: Shellcode		Assignment 4 Release; Lab 4 Release	
Thu 11/14	System Security I: OS Security overview			
Tue 11/19	System Security II: Micro-architecture Basics			
Thu 11/21	System Security III: Meltdown & Spectre Attack			
Tue 11/26	AI Security I: Differential Privacy			Assignment 4 Due; Lab 4 Due
Thu 11/28	Thanksgiving; No class.			
Tue 12/03	AI Security II: Adversarial Attack on ML models.			
Thu 12/05	Review			
Tue 12/17	Final Exam	Time: **8:00-11:00 AM**. Location: Section B - **Knox 20**; Section C - **Knox 21**		

Course overview

Course goal

- Objectives: developing a solid understanding of **fundamental principles** of the **security** field and building knowledge of tools and mechanisms to safeguard a wide range of software and computing systems.
- Topics:
  - Cryptographic background and tools;
  - Access control; authentication;
  - Network security: protocols (TCP/IP, DNS, SSL/TLS etc), attacks (spoofing/sniffing, MITM, etc), and countermeasures;
  - Web security: SQL injection, XSS/XSRF attack;
  - Software security: buffer overflow, shellcode, ROP;
  - System & Hardware security: micro-arch attack
  - Emerging field: ML Security, Privacy;
  - Legal and ethical aspects (cybercrime, intellectual property)

Positioning

- The syllabus is mostly the same as *CSE565 - Section A* offered by Prof Hongxin Hu

- The assignments/labs will be different.

- Acknowledgement:

  - The course materials are heavily based on Prof Hongxin Hu & Prof Ziming Zhao's past offering of CSE565

Positioning

Roadmap

Security research: Ready to read/understand state-of-the-art security papers/systems.

IEEE S&P (Oakland), USENIX Security, ACM CCS, NDSS, CRYPTO, Euro S&P, etc

Web Security

Network Security

CSE410/510 Software Security

System Security

Cryptography

CSE365 Intro to Computer Security

This Course

CSE220 System Programming

CSE421 Operating System

Compiler

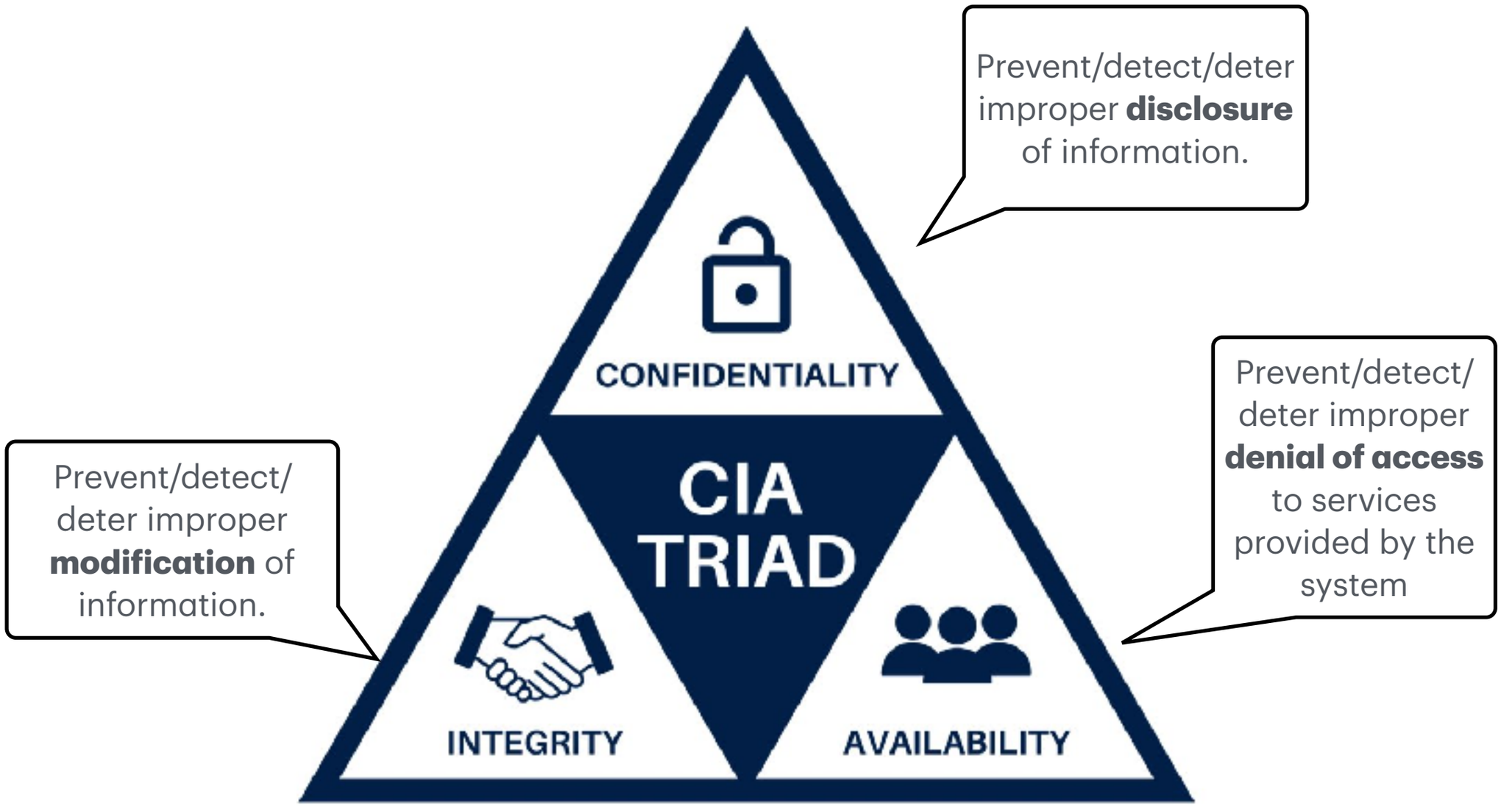
CSE 331/431/531 Algorithm

What is Computer Security?

The NIST Internal/Interagency Report NISTIR 7298 (Glossary of Key Information Security Terms , May 2013) Defines the Term Computer Security as Follows:

*"Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated."*

Security Objective: The CIA Triad



Confidentiality

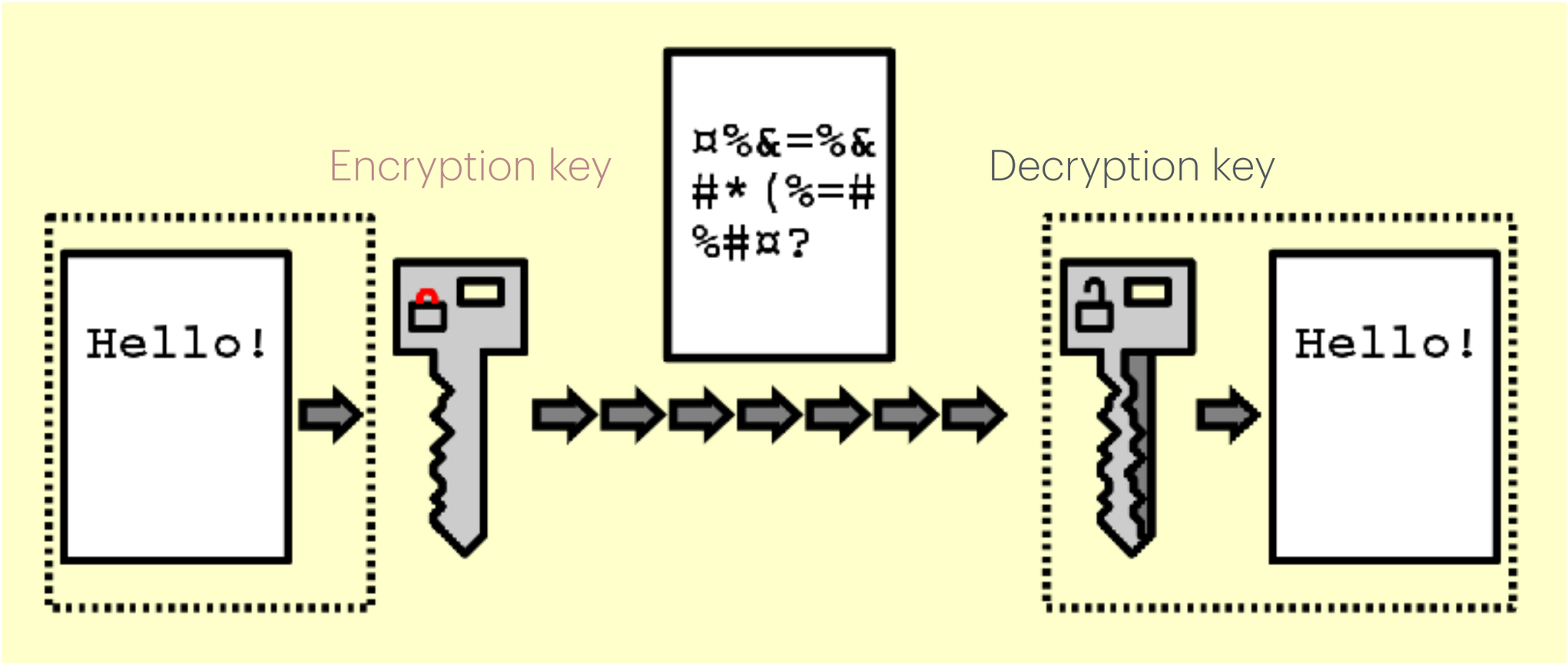
- **C**onfidentiality involves the *protection of data*, providing access for those who are *allowed* to see it while *disallowing* others from learning anything about its content.

  - data confidentiality: sensitive information is available to authorized parties only

  - privacy: individuals can control what information about them can be collected and stored and to whom it is made available

Tools for Confidentiality

- **Encryption:** the transformation of information using a *secret*, called an *encryption key*, so that the transformed information can only be read using another secret, called the *decryption key*



Tools for Confidentiality

Authorization (*Access control*) : rules and policies that limit access to confidential information to those people and/or systems with a "need to know."

- This "need to know" may be determined by identity, such as a person's name or a computer's serial number, or by a role that a person has, such as being a manager or a computer security specialist.

- The determination if a person or system is allowed access to resources, based on an **access control policy**.

    - Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources.

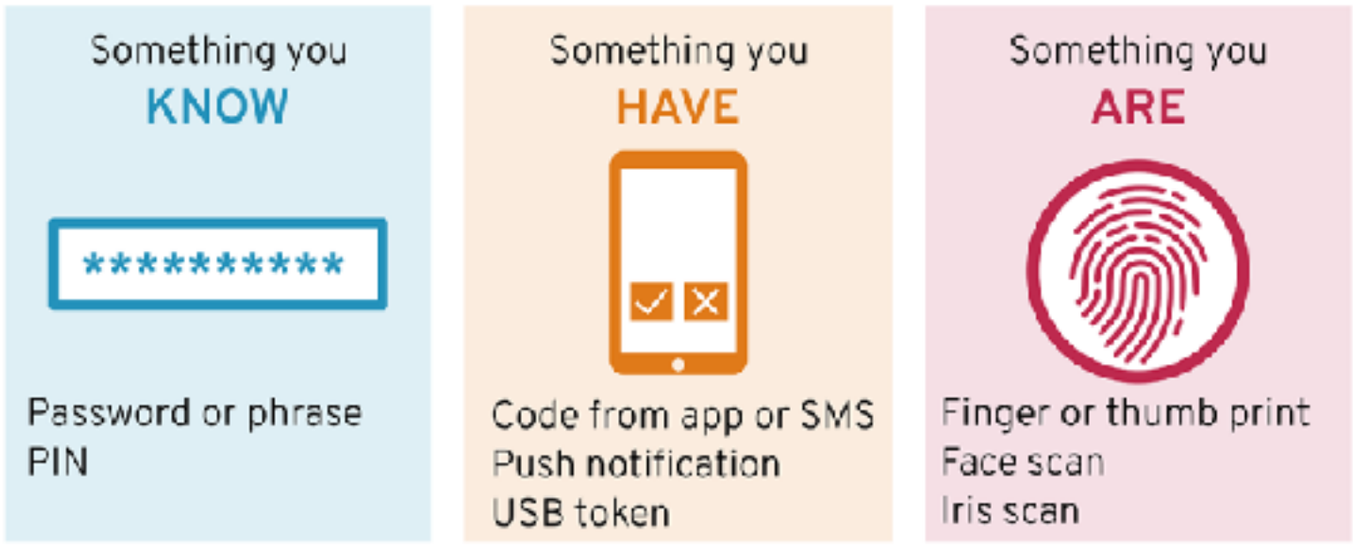
Tools for Confidentiality

- **Authentication**: the determination of the identity or role that someone has. This determination can be done in a number of different ways, but it is usually based on a *combination* of

  - Something you *know* (like a password),

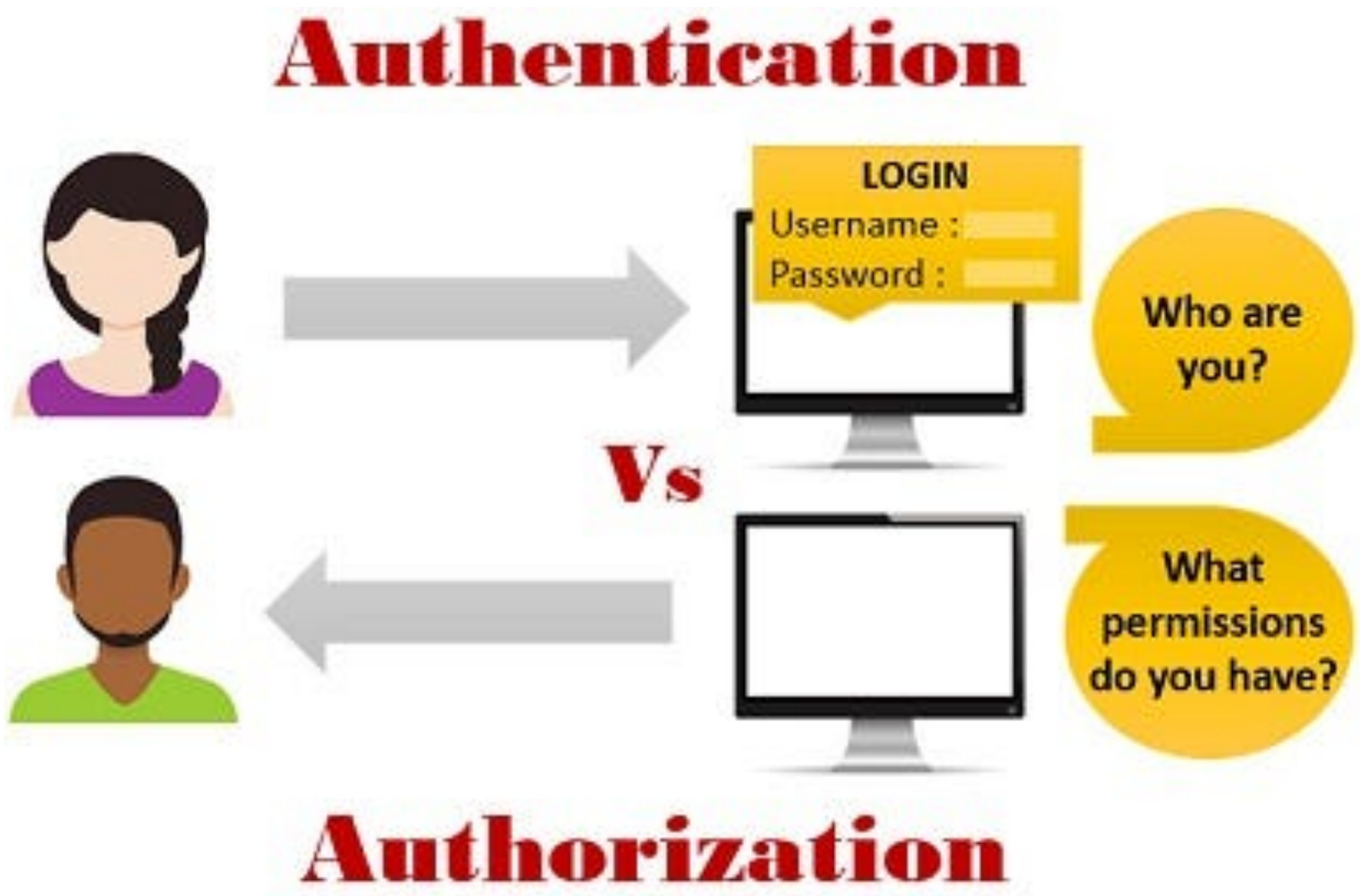
  - Something you *have* (like a smart card or a cellphone),

  - Something you *are* (like a human with a fingerprint).



Tools for Confidentiality

Authentication vs Authorization



Examples

Attack on *confidentiality*

- **Eavesdropping**: the interception of information intended for someone else during its transmission over a communication channel.
    - Example: **packet sniffers**

Integrity

- Integrity: Prevent/detect/deter improper modification of information
- Data integrity : Assures that information and programs are *changed* only in a specified and authorized manner.
- System integrity : Assures that a system performs its *intended function* in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

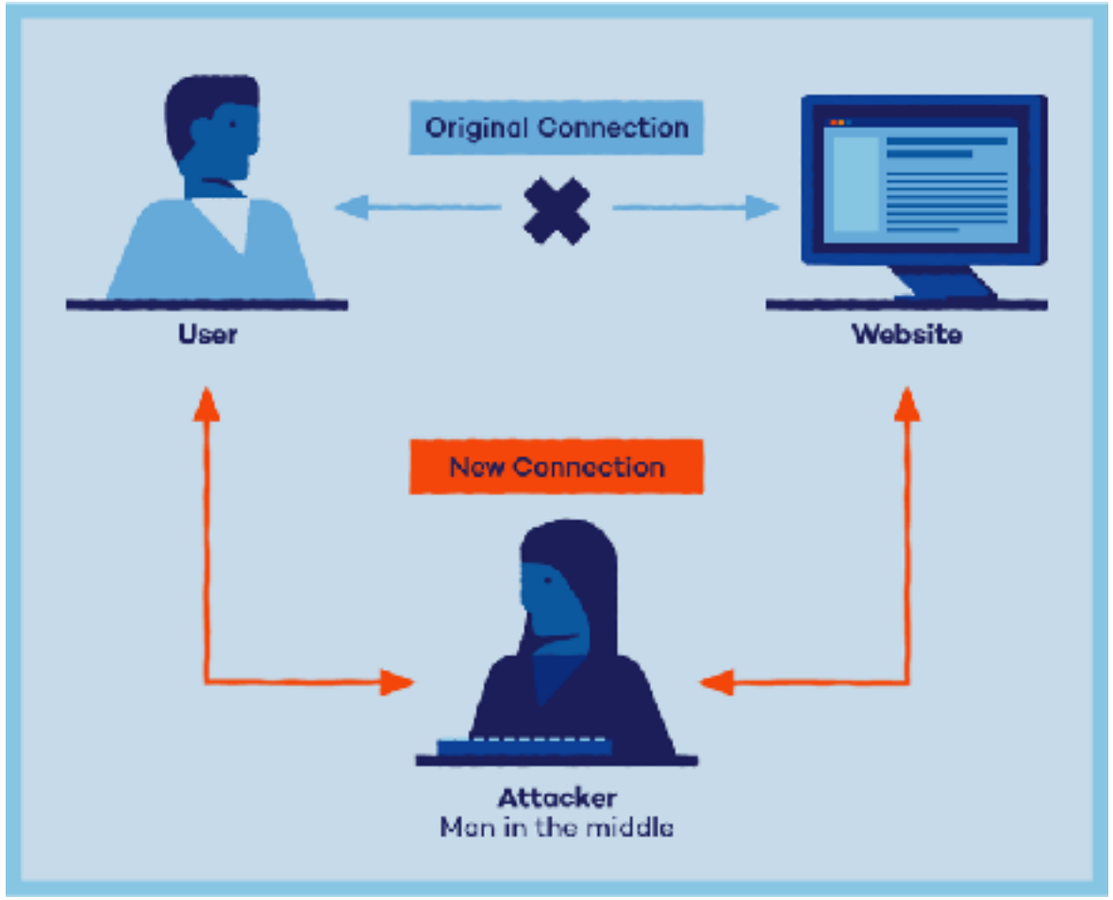
Tools for Integrity

- **Backup**: Periodic archiving of data. (e.g, iCloud)
- **Checksums**: the computation of a function that maps the contents of a file to a numerical value (a.k.a., *hash*).
  - Depends on the *entire contents* of a file
  - Sensitive to *a small change* in the input file: even flipping a single bit is highly likely to result in a different checksum.
- **Data correcting codes**: methods for storing data in such a way that small changes can be easily detected and automatically corrected

Examples

Attack on *data integrity*

- **Alteration**: unauthorized modification of information.
  - Example: the **man-in-the-middle attack**, where a network stream is intercepted, modified, and retransmitted.



Availability

- **Availability:** Prevent/detect/deter improper *denial of access* to services provided by the system

- Tools:
  - Computational *redundancies*: computers and storage devices that serve as fallbacks/replicas in the case of failures

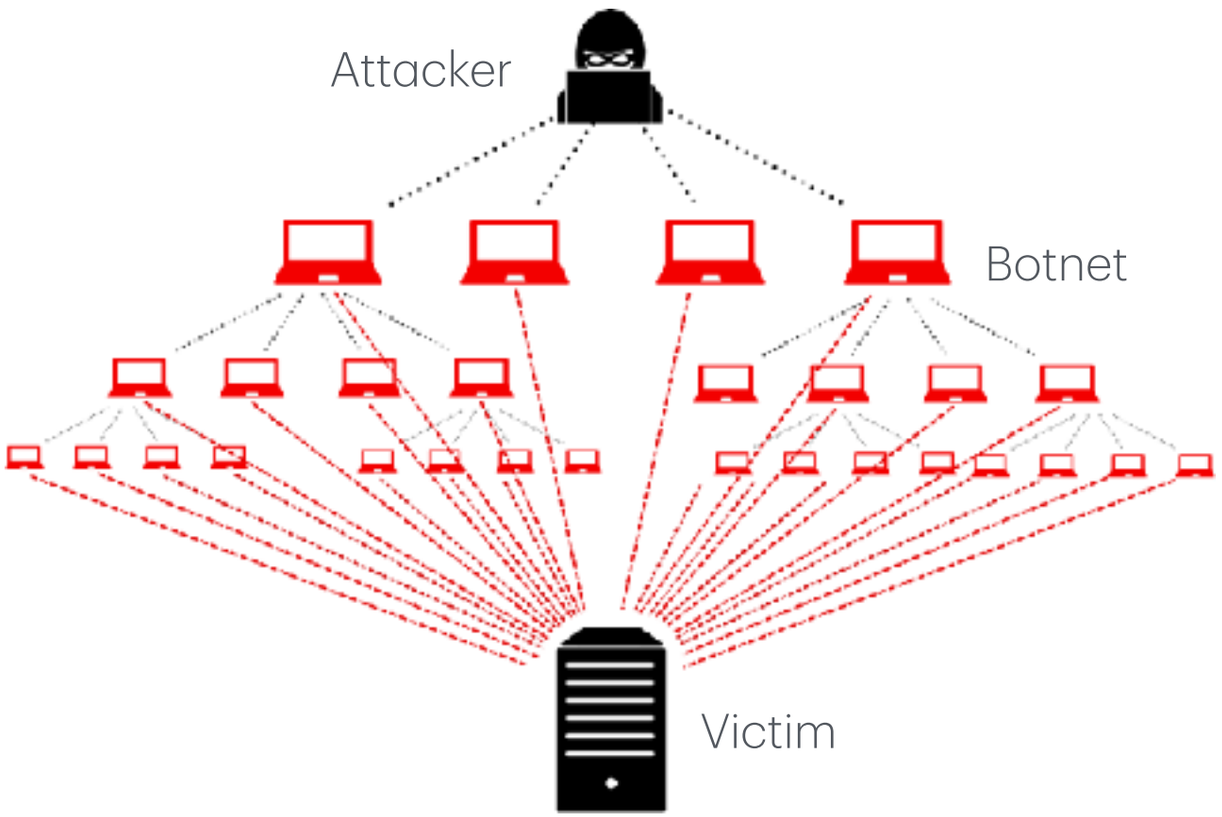
  - Physical protections: infrastructure meant to keep information available even in the event of physical challenges.

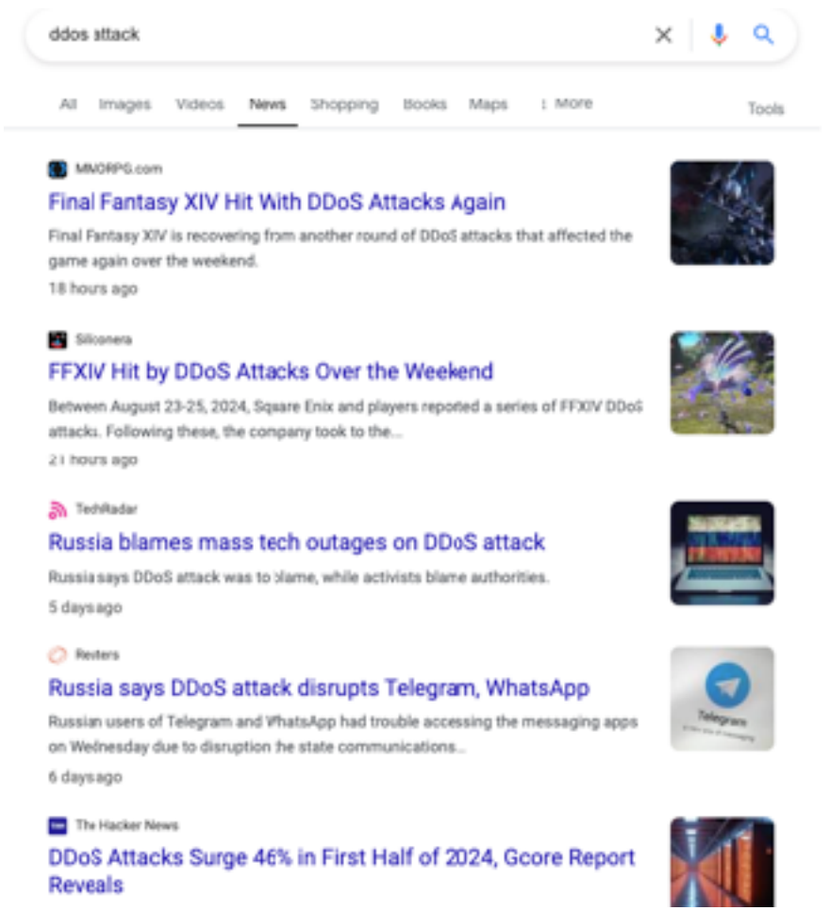
- This is also a central topic in distributed system design.

Example

Attack on *availability*

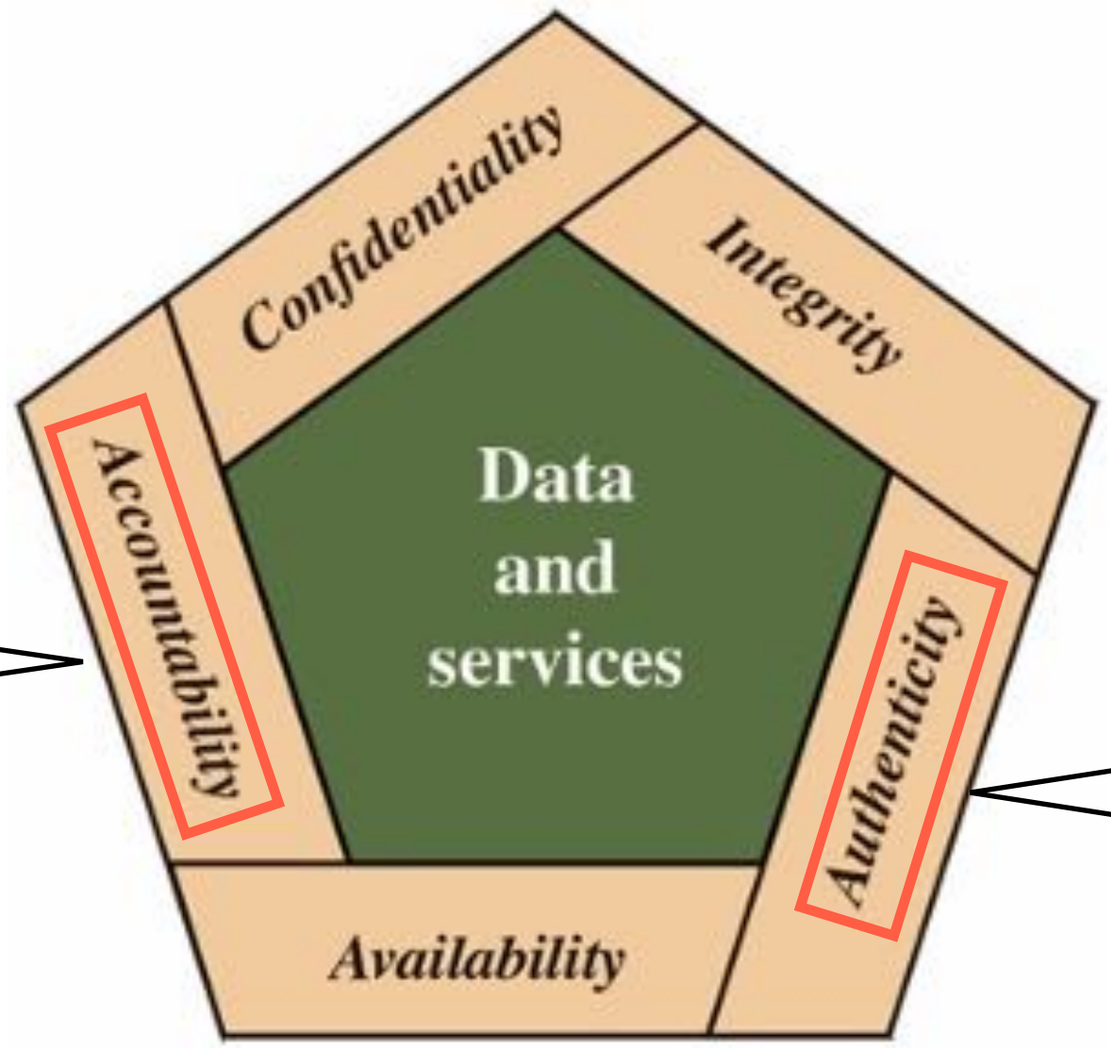
- **Denial-of-Service (DoS)**: the interruption or degradation of a data service or information access.
    - Example: Distributed DoS (DDoS), multiple compromised systems used to target a single system, server, or network, overwhelming it and causing it to become unavailable .





Augmenting CIA Triad

Authenticity & Accountability

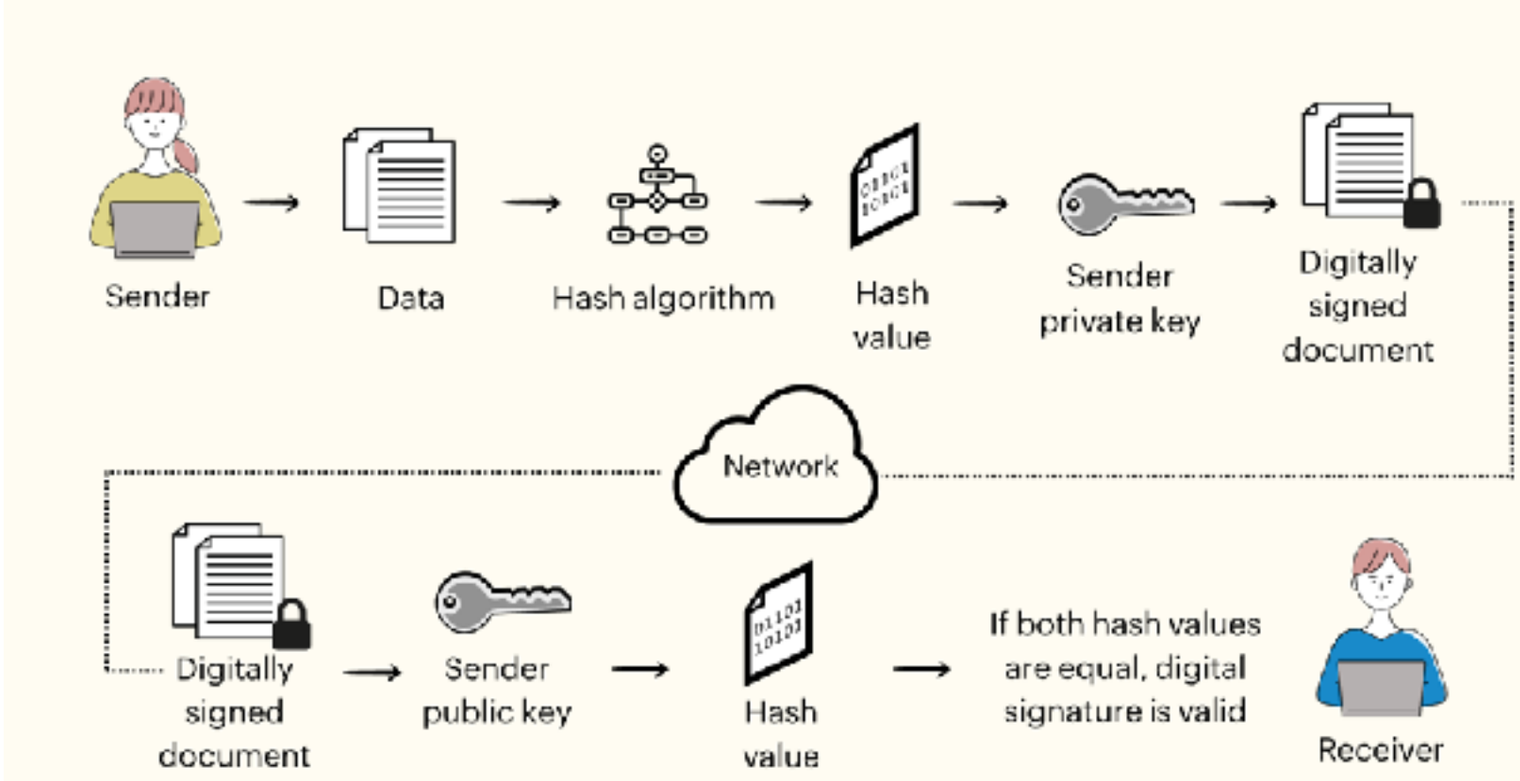


The assurance that every action can be attributed to the entity **responsible** for it.

The assurance that a message, transaction, or other exchange of information is from the **source** it claims to be from.

Tools for Authenticity

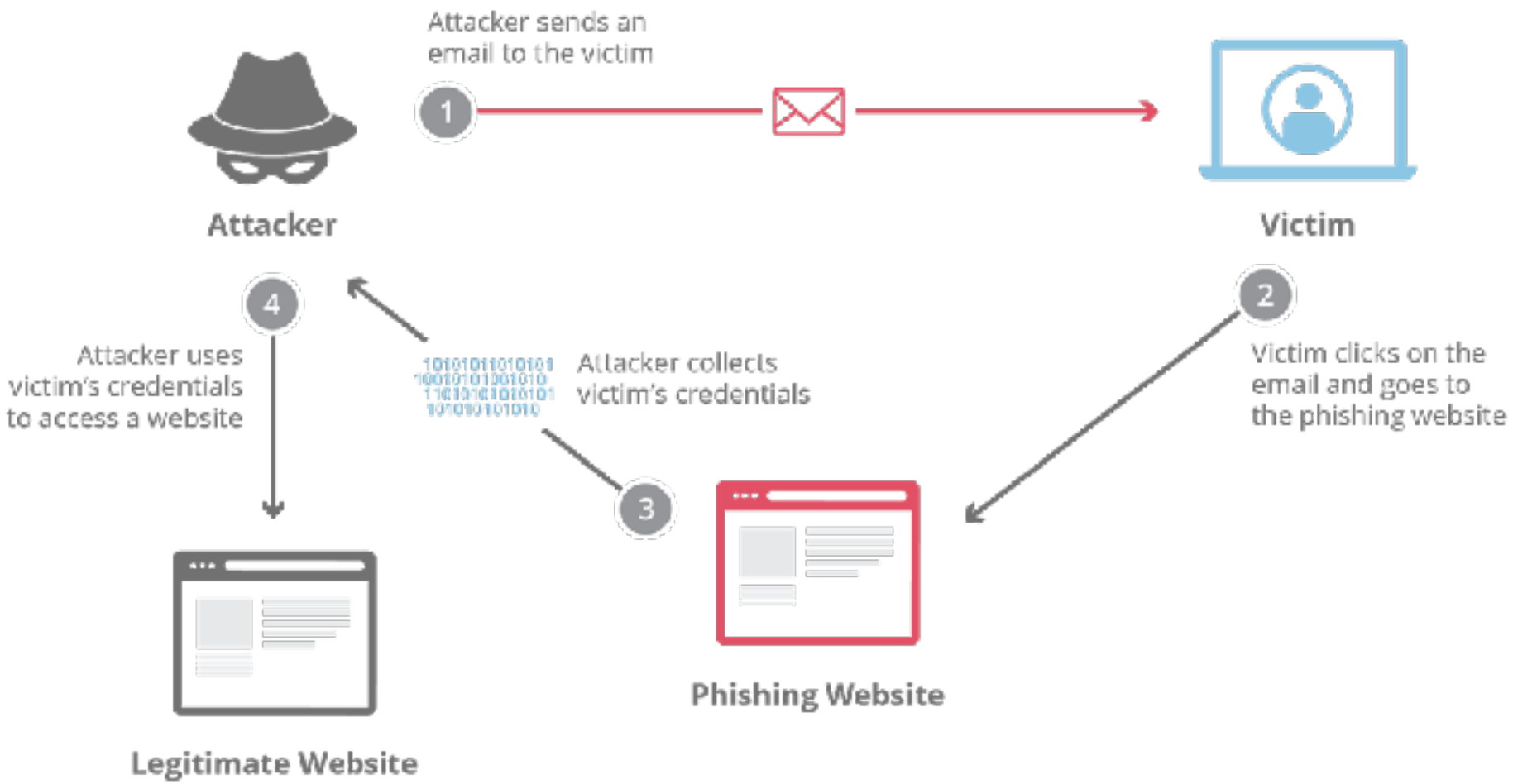
- **Digit signature**: cryptographic computations that allow a person or system to *commit* to the authenticity of their documents in a unique way that achieves **non-repudiation**, which is the property that authentic statements issued by some person or system cannot be denied.



Example

Attack on *authenticity*

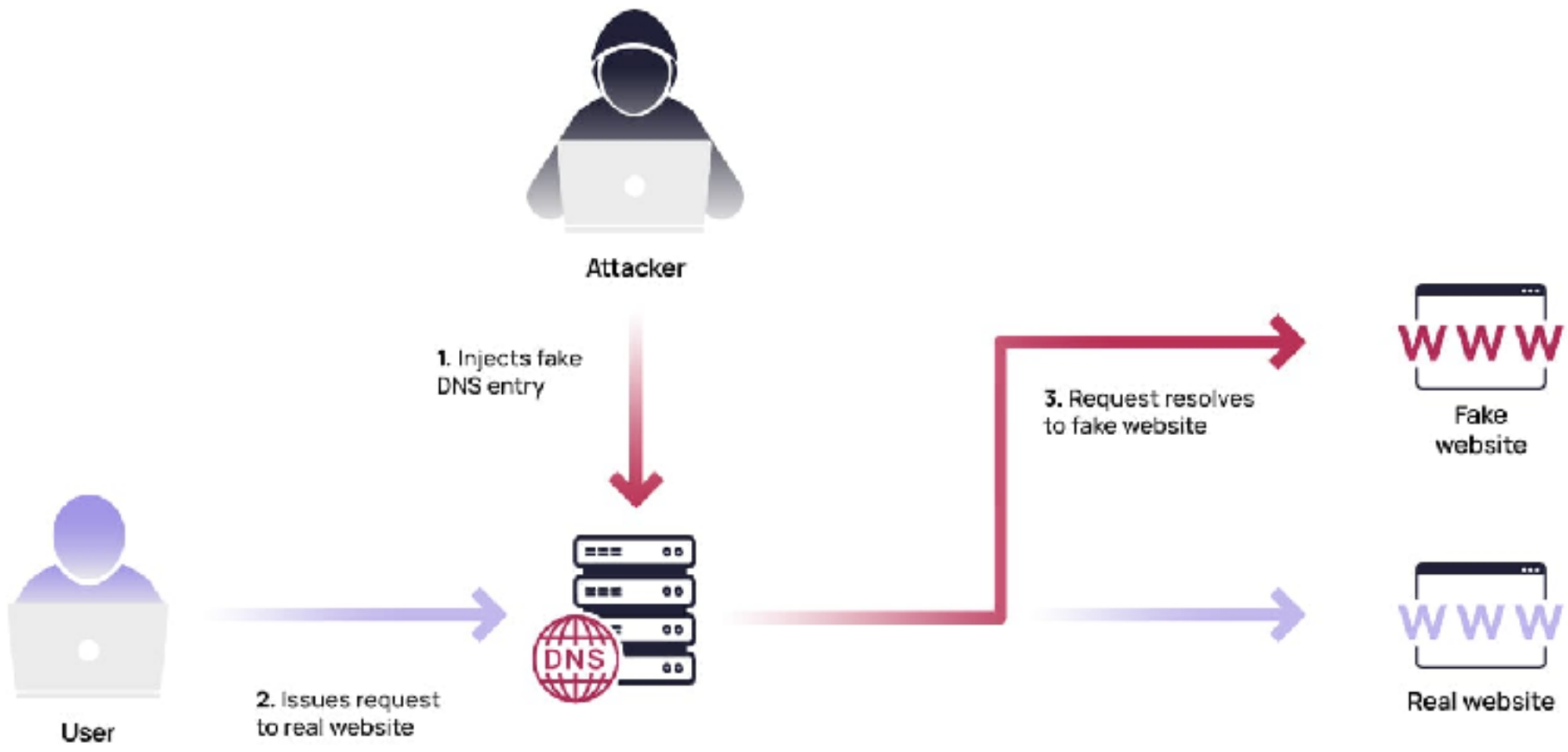
- **Phishing**: BankofAm**a**rica.com looks like BankofAm**e**rica.com



Example

Attack on *authenticity*

- **Spoofing:** Send a network packet with the wrong return IP address



Tools for Accountability

- Recall: Accountability is the assurance that every action can be attributed to the entity **responsible** for it.

- **Logging** and **Monitoring** Tools: record and monitor activities across systems, applications, and networks, creating a detailed audit trail.
  - Examples: Syslog, DataDog

- **Version Control Systems**: track changes in code, documents, and configurations, ensuring that all modifications are attributed to specific users.
  - Examples: Git, SVN, Mercurial

Example: Lifecycle of an access

Confidentiality + Accountability + Integrity

1. **Authentication**: Who goes there? (*Confidentiality)*

   - Restrictions on who (or what) can access system

2. **Authorization**: Are you allowed to do that? (*Confidentiality)*

   - Restrictions on actions of *authenticated* users

   - Authorization is a form of *access control*

3. **Accounting**: Every step leaves a trace. (*Accountability)*

   - Tracking and recording of users' activities within a system

4. **Auditing**: Every trace is examined. (*Integrity)*

   - Reviewing and verifying records to ensure compliance within a system.

Why is security so hard?

A chain is only as strong as its weakest link.

Why is security so hard?

- Identifying security requirements of a system is non-trivial
  - Must take into account services, environment, etc.
- Finding adequate (often complex) solutions is not easier
  - The decision must take into account known and unknown attacks and threats
  - Security mechanisms must be logically placed
- Securing a system is *not* a one-time task
  - The system must be constantly monitored in face of changing threats
  - Security mechanisms need to be re-evaluated

Why is security so hard?

- Managers do not perceive value in security investment (until a security failure occurs)
    - System administrators might not influence decisions or not make good decisions
- Users view security measures as an obstacle on the way of getting their work done
    - We would like security mechanisms to be as intuitive and robust as possible
- Adding security to an existing system might not be pretty
    - Ideally, security is an integral part of the design

Computer Security Terminology (1 of 3)

- **Adversary (threat agent)**
  - Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
- **Attack**
  - Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- **Countermeasure**
  - A device or technique that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Computer Security Terminology (1 of 3)

Type of Adversaries

- **Passive**: observes information without intervention
  - e.g., passively monitoring a communication link
- **Active**: changes system resources or affects their operation
  - e.g., changing messages, replaying old messages on the network, corrupting users, etc.
- **Insider**: is legitimately a part of the system with access to internal data or is inside the security perimeter. (e.g. *whistleblowers*)
- **Outsider**: is outside of the security perimeter or is not a legitimate user

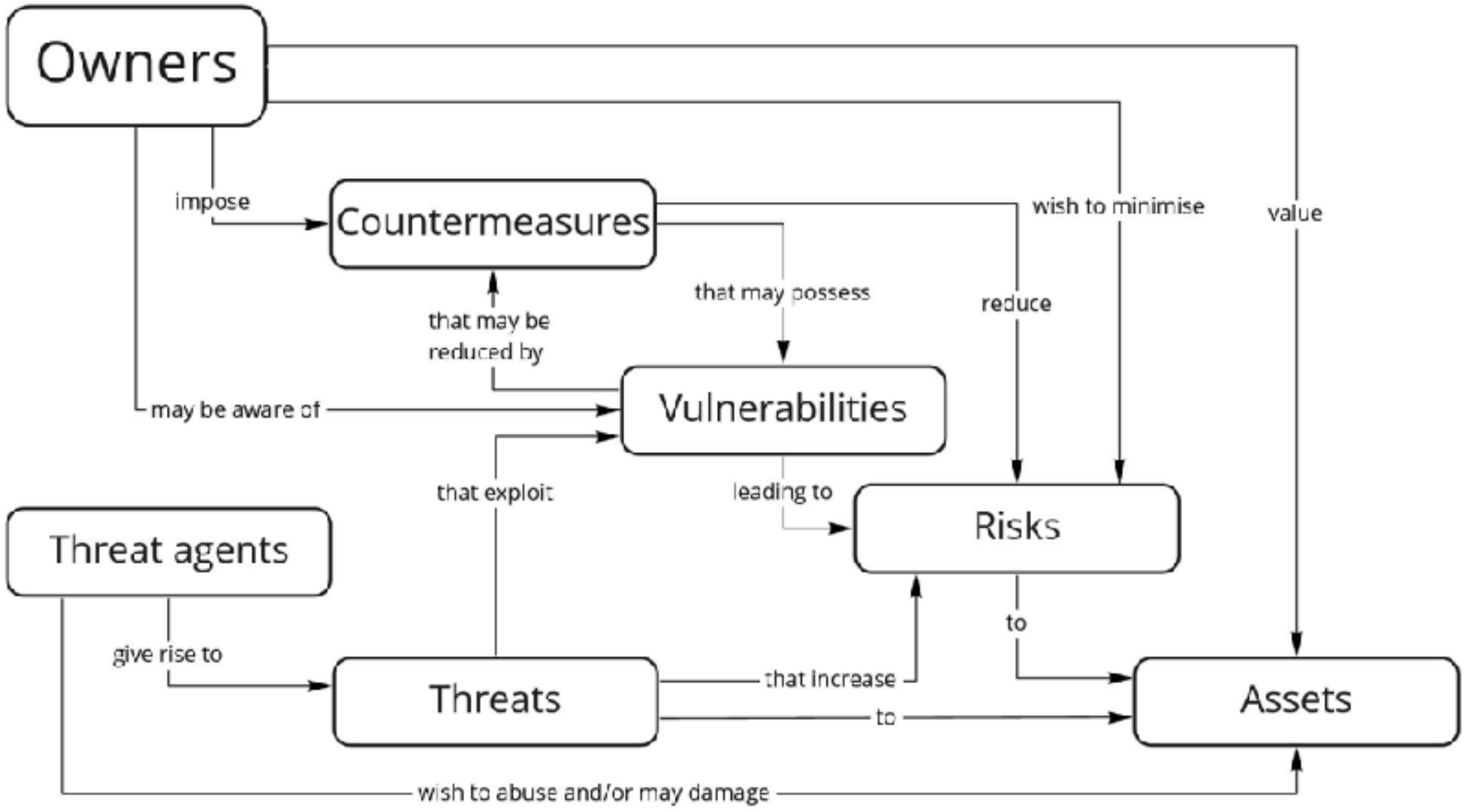
Computer Security Terminology (2 of 3)

- **Risk**
  - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.
- **Security Policy**
  - A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.
- **System Resource (Asset)**
  - A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Computer Security Terminology (3 of 3)

- **Threat**
  - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- **Vulnerability**
  - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a *threat* source.

Relations between the jargons



A taste of realworld hack

Hack the]HackingTeam[

- HackingTeam is a security technology company *that sold offensive intrusion and surveillance capabilities tools*.

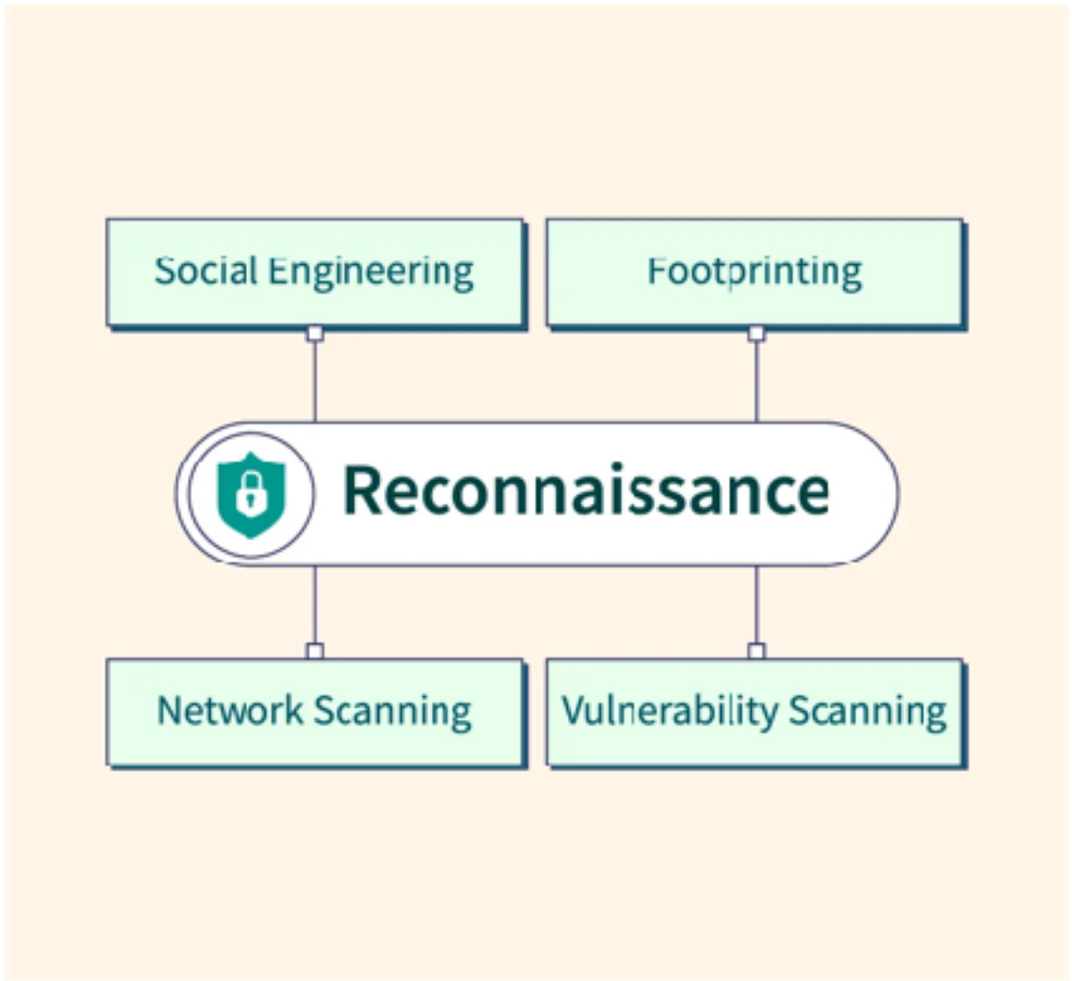
- Hacked brutally in Jul 2015: https://github.com/Alekseyyy/phineas-philes/blob/master/ht-english.txt

A taste of realworld hack

Hack the]HackingTeam[

Step 1: Reconnaissance

- HackingTeam is actually very careful.
- They did not expose much of an attack surface—"*only an up-to-date version of Joomla, a mail server, a couple routers, two VPN appliances, and a spam filtering appliance*."



A taste of realworld hack

Hack the]HackingTeam[

Step 2: Sneak in

- The hacker found and exploited a 0-day in the firmwares of an (unknown) embedded device:

- *"after two weeks of work reverse engineering, I got a remote root exploit."*

A taste of realworld hack

Hack the]HackingTeam[

Step 3: Watch and Listen

- Careful analysis and slow scan of the internal network
- Found an unsecured MongoDB server containing *audio recording* and *webcam images* from the physical security system.

A taste of realworld hack

Hack the]HackingTeam[

Step 4: Crossed Cables

- nmap found a vulnerable iSCSI device that stores backups of the company's Exchange server.
- Although too big to download, the hacker managed to mount the backups via port forwarding on the exploited embedded device (in Step 2).

A taste of realworld hack

Hack the]HackingTeam[

Step 5: Total compromise

- The hacker was able to dump an old BES admin password in the Windows registry hive from the backup. And this pwd is still valid!

The admin password dumped from the backup.

```
_SC_BlackBerry MDS Connection Service
0000   16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010   62 00 65 00 73 00 33 00 32 00 36 00 37 00 38 00   b.e.s.3.2.6.7.8.
0020   21 00 21 00 21 00 00 00 00 00 00 00 00 00 00 00   !.!.!...........
```

A taste of realworld hack

Hack the]HackingTeam[

Step 5: Total compromise

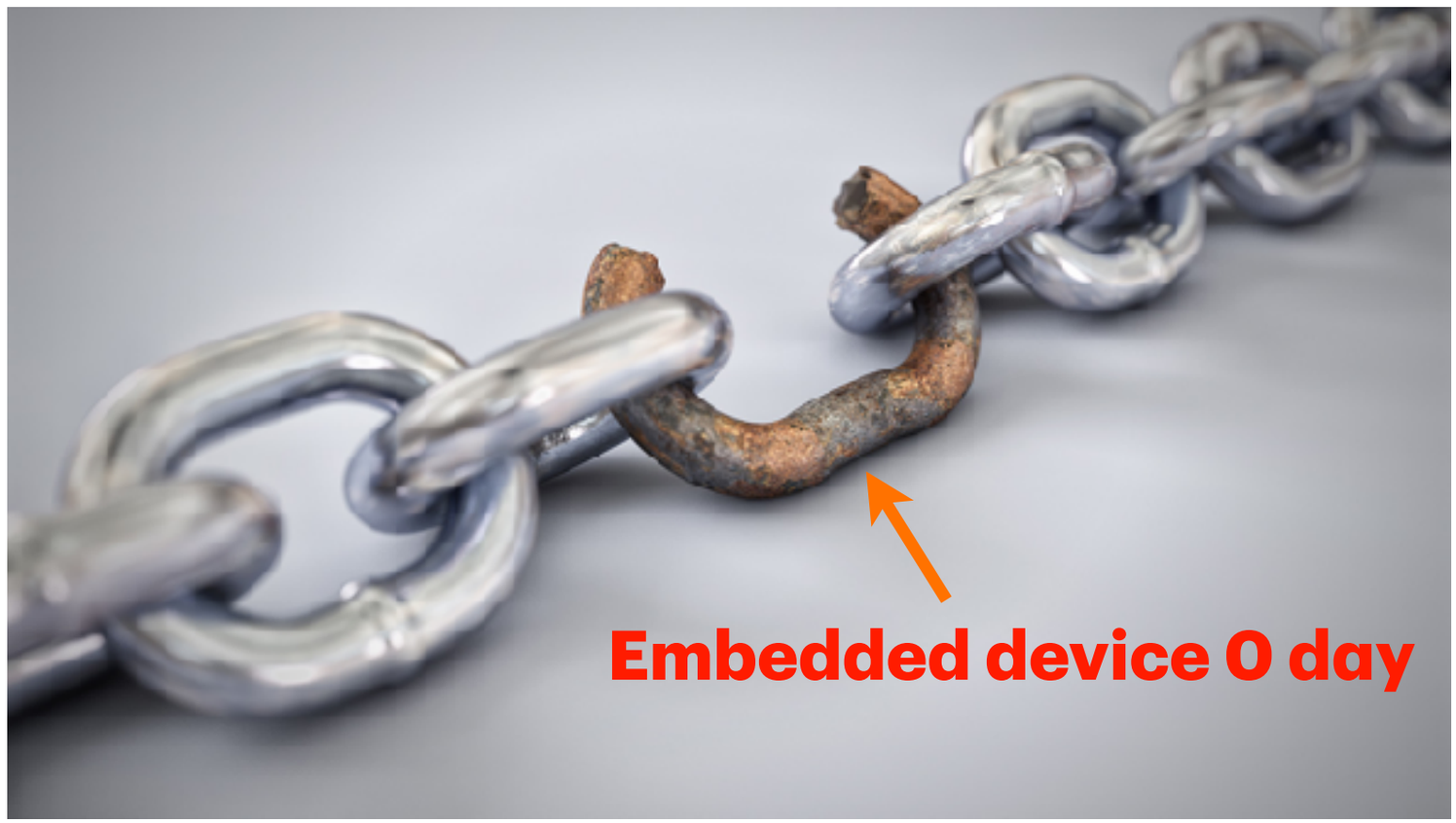
- **Game over**: The BES account is a local admin on a machine containing all the companies credentials, including the domain admin.

```
HACKINGTEAM  BESAdmin       bes32678!!!
HACKINGTEAM  Administrator  uu8dd8ndd12!
HACKINGTEAM  c.pozzi        P4ssword      <---- lol great sysadmin
HACKINGTEAM  m.romeo        ioLK/(90
HACKINGTEAM  l.guerra       4luc@=.=
HACKINGTEAM  d.martinez     W4tudul3sp
HACKINGTEAM  g.russo        GCBr0s0705!
HACKINGTEAM  a.scarafile    Cd4432996111
HACKINGTEAM  r.viscardi     Ht2015!
HACKINGTEAM  a.mino         A!e$$andra
```

A taste of realworld hack

Hack the]HackingTeam[

What went wrong



A taste of realworld hack

Hack the]HackingTeam[

What went wrong

Weak links

- Vulnerable (?) network-facing infra
- Physical security system without digital security
- The backup storage system should be isolated on a separate network
- Continued use of stale password
- No multi-factor authentication
- Sensitive emails backed up rather than deleted promptly

Ethics

- **RULE NUMBER ONE**: do not do anything illegal
- Never hack into a system without explicit permission to hack
- Never attempt to find vulnerabilities in a system without explicit permission

Questions?