Software and Systems Security

Hamid R. Barzegar, Ph.D.

Introduction to Information Security

- Today our world is one in which citizens from all nations are compelled to continually protect themselves and their property from attacks by adversaries.
- Random shootings, suicide bombings, assassinations, and other types of physical violence occur almost daily around the world with no end in sight.
- To counteract this violence, new types of security defenses have been implemented.
  - Passengers using public transportation are routinely searched.
  - Borders are closely watched.
  - Telephone calls are secretly monitored.
  - These attacks and security defenses have significantly impacted how all of our work, play and live.

Introduction to Information Security

- These attacks are not just physical. One area that has also been an especially frequent target of attacks is an information technology (IT).
- A seemingly endless array of attacks is directed at individuals, schools, businesses, and governments through desktop computers, laptops, and smartphones.
- Internet web servers must resist thousands of attacks every day. Identity theft using stolen electronic data has skyrocketed.
- An unprotected computer connected to the Internet may be infected in fewer than 60 seconds.
- Viruses, phishing, worms, and botnets—virtually unheard of just a few years ago—are now part of our everyday technology vocabulary.

Some definitions:

- There are many types of **virus**. **Viruses** and spyware are also known as 'malware' A worm, for example, can exploit **security** vulnerabilities to spread itself automatically to other computers through networks.

- **Phishing** is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

- A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

- A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack, steal data, send spam, and allows the attacker to access the device and its connection.

Introduction to Information Security

- The need to defend against these attacks directed toward our technology devices has created an element of IT that is now at the very core of the industry. **Known as information security**, it is focused on protecting the electronic information of enterprises and users.

Understanding Security

- What is security? The word comes from the Latin, meaning free from care.
- Sometimes security is defined as the state of being free from danger, which is the goal of security.
- It is also defined as the measures taken to ensure safety, which is the process of security.
- Since complete security can never be fully achieved, the focus of security is more often on the process instead of the goal.
- In this light, security can be defined as the necessary steps to protect from harm.

Defining Information Security

- Several terms are used when describing security in an IT environment:
  - Computer security,
  - IT security,
  - Cybersecurity, and
  - Information assurance.

What Is Information Security?

- Information security is often used to describe the tasks of securing information that is in a digital format, whether it be manipulated by a microprocessor (such as on a personal computer), preserved on a storage device (like a hard drive or USB flash drive), or transmitted over a network (such as a local area network or the Internet).

The goal of information security

- The goal of information security is to ensure that protective measures are properly implemented to ward off attacks and prevent the total collapse of the system when a successful attack does occur. Thus, information security is first protection.

- Second, information security is intended to protect information that provides value to people and enterprises.

- There are three protections that must be extended over information:
  - Confidentiality,
  - Integrity, and
  - Availability—or CIA:

Confidentiality

- It is important that only approved individuals can access important information.
- For example, the credit card number used to make an online purchase must be kept secure and not made available to other parties.
- Confidentiality ensures that only authorized parties can view the information.
- Providing confidentiality can involve several different security tools, ranging from software to scramble the credit card number stored on the web server to door locks to prevent access to those servers.

Integrity

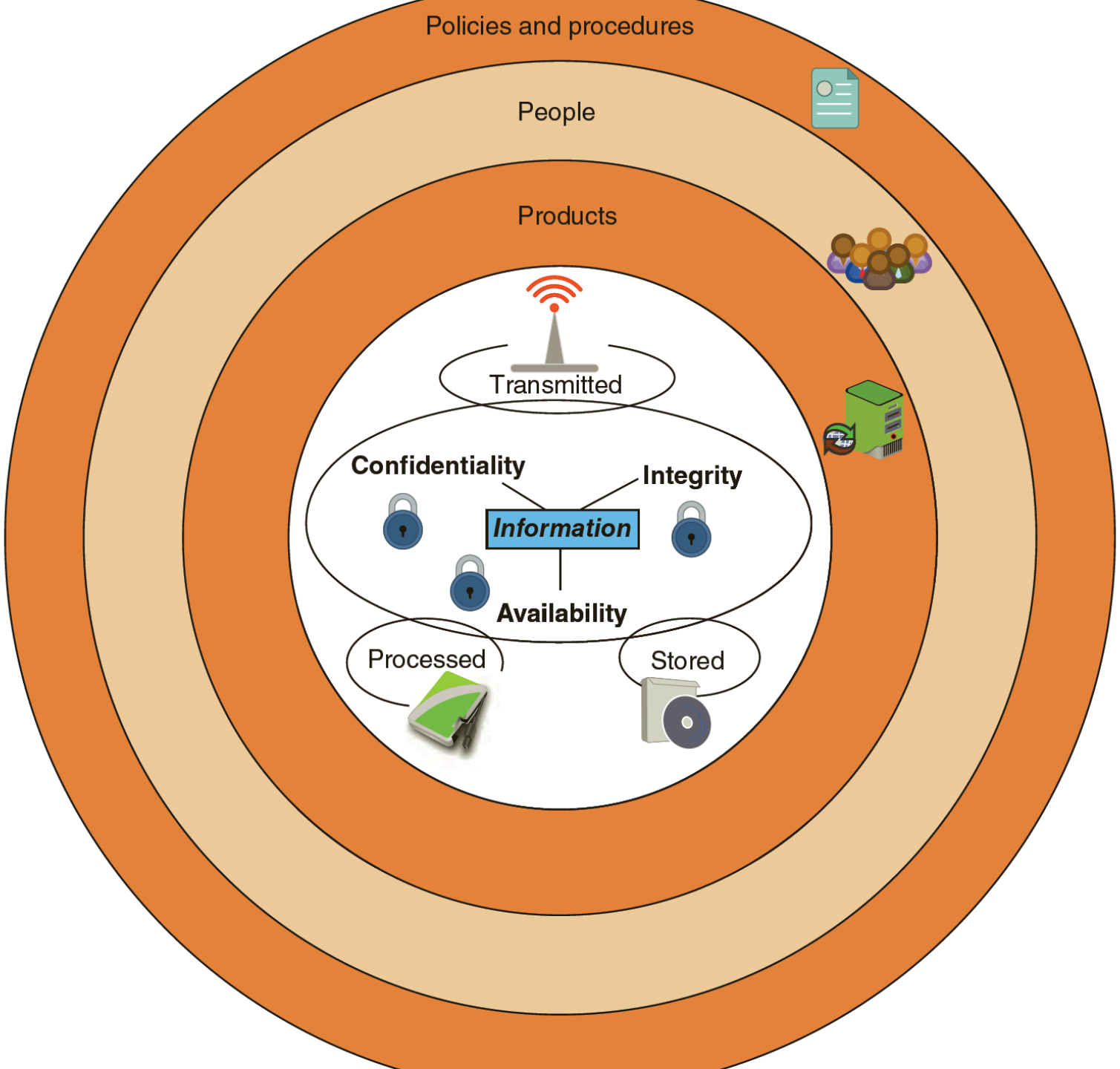
- Integrity ensures that the information is correct and no unauthorized person or malicious software has altered the data.

- In the example of the online purchase, an attacker who could change the amount of purchase from $10,000.00 to $1.00 would violate the integrity of the information.

Availability

- The information has value if the authorized parties who are assured of its integrity can access the information.
- Availability ensures that data is accessible to authorized users. This means that the information cannot be “locked up” so tight that no one can access it. It also means that attackers have not performed an attack so that the data cannot be reached.
- In this example the total number of items ordered as the result of an online purchase must be made available to an employee in a warehouse so that the correct items can be shipped to the customer.

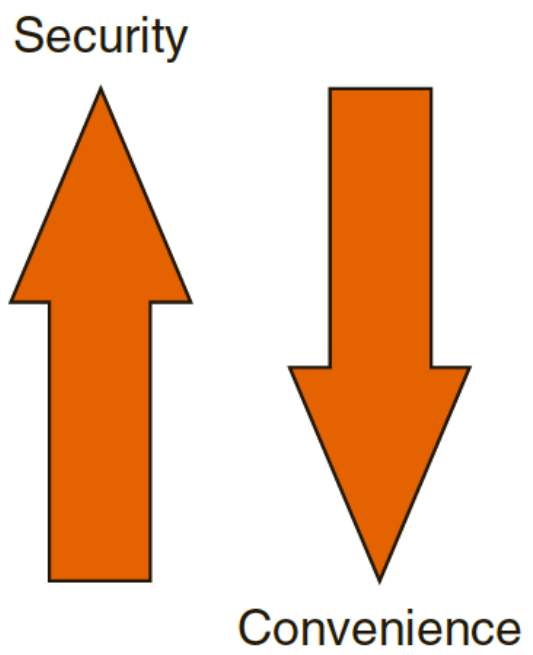
Information security layers



Relationship of security to convenience

- It is important to understand the relationship between security and convenience.

- As security is increased, convenience is often decreased. That is, the more secure something is, the less convenient it may become to use (security is said to be inversely proportional to convenience).



Reasons for Successful Attacks

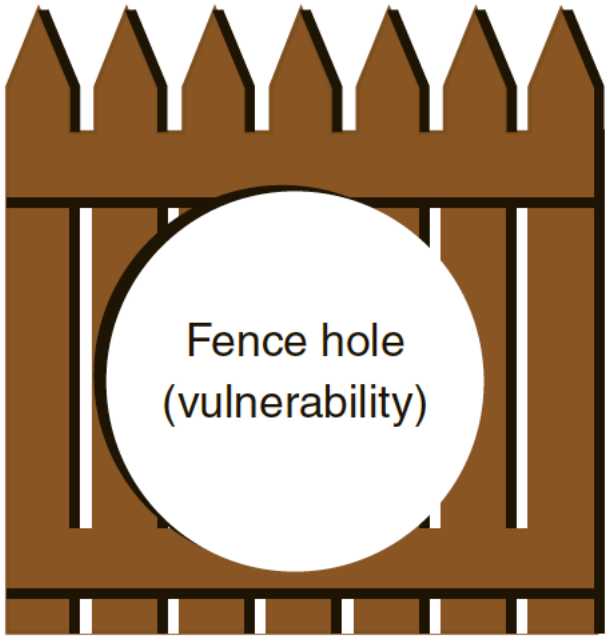
- Widespread vulnerabilities.
- Configuration issues.
- **Poorly designed software.**
- Hardware limitations.
- Enterprise-based issues.

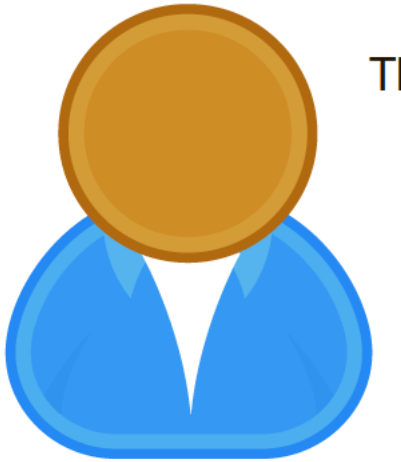
Difficulties in Defending Against Attacks

- Universally connected devices.
- Increased speed of attacks.
- Greater sophistication of attacks.
- Availability and simplicity of attack tools.
- Faster detection of vulnerabilities.
- Delays in security updating.
- Weak security update distribution.
- Distributed attacks.
- Use of personal devices.
- User confusion.

Information security components analogy

Attack vector
(go through
fence hole)





Thief (threat actor)

Theft of scooter
(threat)

Stolen scooter (risk)

Scooter (asset)

Asset

- Ellie's new scooter is an asset, which is defined as an item that has value.
- In an enterprise, assets have the following qualities: they provide value to the enterprise; they cannot easily be replaced without a significant investment in expense, time, worker skill, and/or resources; and they can form part of the enterprise's corporate identity.

Information technology assets

Element name	Description	Example	Critical asset?
Information	Data that has been collected, classified, organized, and stored in various forms	Customer, personnel, production, sales, marketing, and finance databases	Yes: Extremely difficult to replace
Customized business software	Software that supports the business processes of the enterprise	Customized order transaction application	Yes: Unique and customized for the enterprise
System software	Software that provides the foundation for application software	Operating system	No: Can be easily replaced
Physical items	Computers equipment, communications equipment, storage media, furniture, and fixtures	Servers, routers, DVDs, and power supplies	No: Can be easily replaced
Services	Outsourced computing services	Voice and data communications	No: Can be easily replaced

Information Security Terminology

- Ellie must decide: what is the likelihood that the threat will come to fruition and her scooter stolen?
- This can be understood in terms of risk. A risk is a situation that involves exposure to some type of danger. There are different options available when dealing with risks, called risk response techniques:
  - Accept.
  - Transfer.
  - Avoid.
  - Mitigate.

Summary of information security terms

Information security terminology

Term	Example in Ellie's scenario	Example in information security
Asset	Scooter	Employee database
Threat	Steal scooter	Steal data
Threat actor	Thief	Attacker, hurricane
Vulnerability	Hole in fence	Software defect
Attack vector	Climb through hole in fence	Access web server passwords through flaw in operating system
Likelihood	Probability of scooter stolen	Likelihood of virus infection
Risk	Stolen scooter	Virus infection or stolen data

Who Are the Threat Actors?

- Threat actor is a generic term used to describe individuals who launch attacks against other users and their computers (another generic word is simply attackers).
  - Script Kiddies
  - Hactivists
  - Nation State Actors
  - Insiders

Fundamental Security Principles

- Layering
- Limiting
- Diversity
- Obscurity
- Simplicity

Hack and Hacker

- Life hack (or life hacking) is any trick, shortcut, skill, or novelty method that increases productivity and efficiency, in all walks of life.
- The term was primarily used by computer experts who suffer from information overload or those with a playful curiosity in the ways they can accelerate their workflow in ways other than programming.
- A computer hacker is any skilled computer expert who uses their technical knowledge to overcome a problem.
- While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems.

Three main types of hackers

- **White Hat**: People who specialized hacking check the faults of the system.
- **Grey Hat**: Exploit a security to the attention of the owners.
- **Black Hat**: People who break into networks and/system and harm to the networks and property.

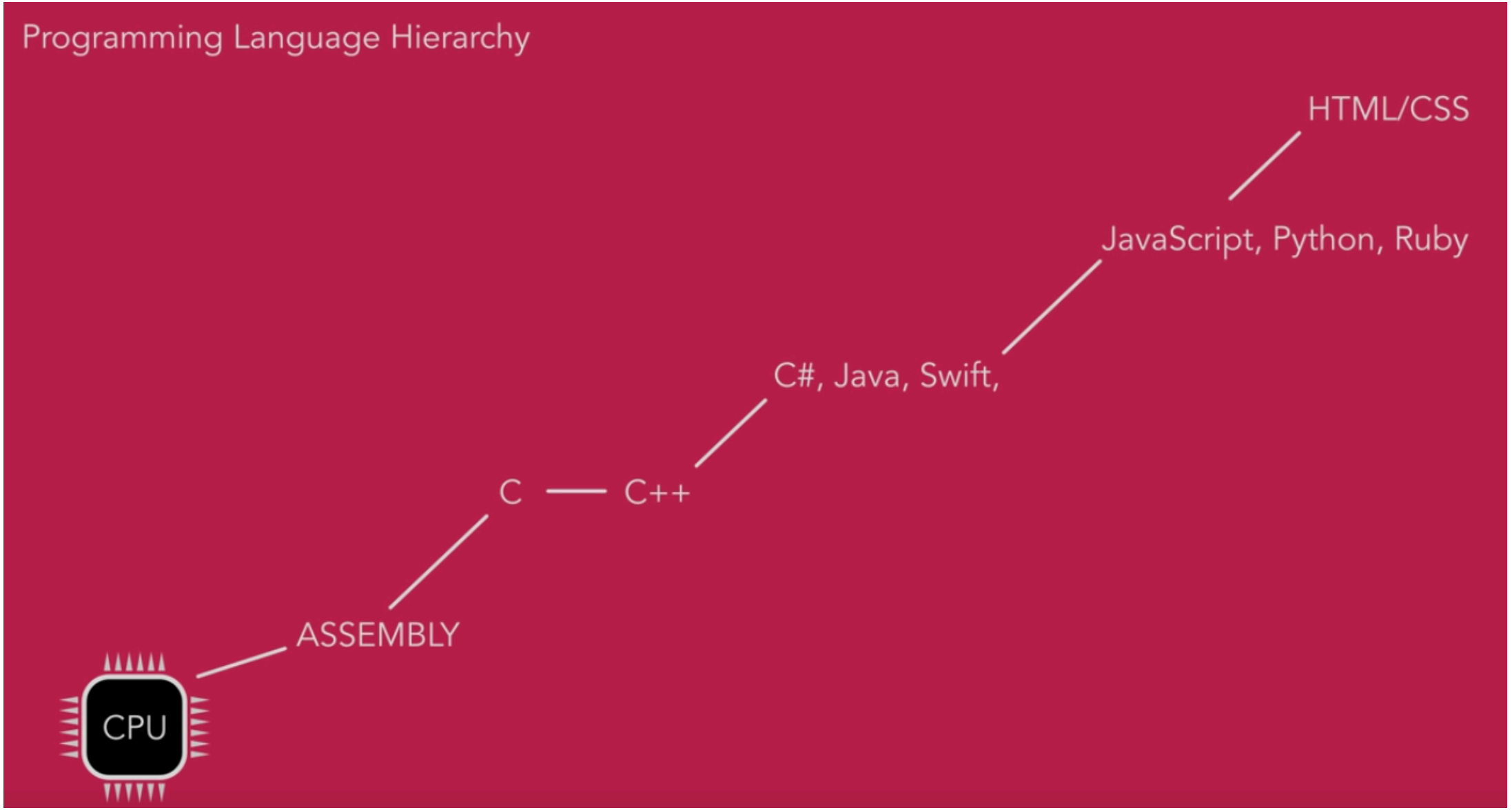
Coronavirus and Hacking

- The Coronavirus Papers unlocked: 5,352 scientific articles covering the coronavirus - fully searchable and free.
- https://www.reddit.com/r/Coronavirus/comments/exdtjt/the_coronavirus_papers_unlocked_5352_scientific/

- Hackers taking advantage of coronavirus scare to spread malware:
- https://www.digitaltrends.com/computing/hackers-coronavirus-malware/

- Dataset about the Coronavirus:
- https://www.kaggle.com/sudalairajkumar/novel-corona-virus-2019-dataset

Best Programming Languages for Cyber Security


Programming Language Hierarchy
HTML/CSS
JavaScript, Python, Ruby
C#, Java, Swift,
C
C++
ASSEMBLY
CPU

unibz

Python

- Python undoubtedly is considered to be one of the most useful programming languages for cyber security considering its:
  - Extensive library of powerful packages that supports Rapid Application Development (RAD)
  - Clean syntax code and modular design.
  - Automatic memory management and dynamic typing capability.
  - Mixed code environments to combine different programming languages (MicroPython, Cython, Jython, Skulpt (JS), PyPy).
- The use of Python in cyber security operations is common due to some of its essential features such as better response time, user-friendly data structure and security.

JavaScript

- JavaScript is the most popular and widespread programming language.
- It's one of the best cybersecurity programming languages you can learn. If you want to steal cookies, manipulate event handlers, and perform cross-site scripting, JavaScript is for you.
- ReactJS, jQuery, NodeJS — do these sound familiar? JavaScript is everywhere. That also means that, due to the language's widespread usage, programs and applications using it are popular targets.
- With JavaScript, a website owner can run any code whenever a visitor comes to a website.

https://ec.europa.eu/info/cookies_en

EN English

Search

Home > Cookies policy

Cookies policy

To make Commission websites work properly, we sometimes place small data files called cookies on your device.

PAGE CONTENTS

What are cookies?

A cookie is a small text file that a website stores on your computer or mobile device when you visit the site.

- **First party cookies** are cookies set by the website you're visiting. Only that website can read them. In addition, a website might potentially use external services, which also set their own cookies, known as **third-party cookies.**
- Persistent cookies are cookies saved on your computer and that are not deleted automatically when you quit your browser, unlike a session cookie, which is deleted when you quit your browser.

Technical cookies

Name	Service	Purpose	Cookie type and duration
has_js	Corporate content management platform, based on Drupal open source software	Determines whether Javascript is enabled in your browser. This allows our websites to function properly.	First-party session cookie, deleted after you quit your browser
JSESSIONID / CFID / CFTOKEN	Java IT platform / Coldfusion IT platform	Maintain a secure session for you, during your visit.	First-party session cookie, deleted after you quit your browser
ecsi	Website survey tools	Stores information on whether you have already replied to a survey pop-up – so you won't be asked again.	First-party persistent cookie, 1 month
theoplayer-session-id	Audiovisual Service video player	Enables the player's own analytics, currently not used.	localStorage Key, persistent data

Third-party cookies

Some of our pages display content from external providers, e.g. YouTube, Facebook and Twitter.

To view this third-party content, you first have to accept their specific terms and conditions. This includes their cookie policies, which we have no control over.

But if you do not view this content, no third-party cookies are installed on your device.

Third-party providers on Commission websites

You Tube
Internet Archive
Google Maps
Twitter
TV1
Vimeo
Microsoft
Facebook
Google
LinkedIn
Livestream
SoundCloud
European Parliament

These third-party services are outside of the control of the Commission. Providers may, at any time, change their terms of service, purpose and use of cookies, etc.

unibz accommodation

Rooms and flats for university students

The Advisory Service publishes online **the ads of unibz students or those of incoming exchange students** looking for an appropriate accommodation.

To publish your offer or request send your ad to info@unibz.it

Zimmer und Wohnungen für Universitätsstudierende

Die Studienberatung veröffentlicht Angebote für **Studierende der unibz oder jene Anfragen von Studierenden, die während des Studiums oder im Rahmen eines Austauschprogrammes an der unibz** auf der Suche nach einer geeigneten Wohnmöglichkeit sind.

Senden Sie Ihre Anzeige an info@unibz.it

Rooms and apartments for university students

The public service orientation offers of accommodation **for students or requests** that are received by **students dell'unibz** looking for accommodation suitable place for the duration of their studies or as part of an **exchange program at our university** .

Send your ad to info@unibz.it . .

C

- C is great for reverse-engineering and finding vulnerabilities.
- Security-conscious programmers will ensure their code lacks vulnerabilities. Hackers, on the other hand, will use C to *find* vulnerabilities.
- Knowing C will help you get a job as a cybersecurity defence analyst.
- Threat mitigation, emerging threat research, vulnerability assessments — these are some of the job functions you'll perform as a cybersecurity defence analyst.

Security mechanisms

- Security mechanisms are technical tools and techniques that are used to implement security services.
- A mechanism might operate by itself, or with others, to provide a particular service.
- Examples of common security mechanisms are as follows:
  - Cryptography
  - Message digests and digital signatures
  - Digital certificates
  - Public Key Infrastructure (PKI)

What is Cyber attack?

- A cyber attack is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems.

Top 10 Most Common Types of Cyber Attacks

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear-phishing attacks
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

Links

- https://www.ibm.com/support/knowledgecenter/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009730_.htm
- https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
- https://medium.com/cyberdefenders/python-for-cyber-security-lesson-1-introduction-to-python-1976d817976
- https://www.springboard.com/blog/best-programming-language-for-cybersecurity/
- https://www.youtube.com/watch?v=WEGjFP-R7Cs
- https://www.youtube.com/watch?v=vw9MX2i5xNc
- https://www.youtube.com/watch?v=F626c_I6OMo
- https://www.youtube.com/watch?v=gdHyyAwxijo

Think Security First

Thank You