BEACH

CECS 378: Intro to Computer Security Principles

Lecture 1

Louis Uuh

Week 1

History of Cyber Security

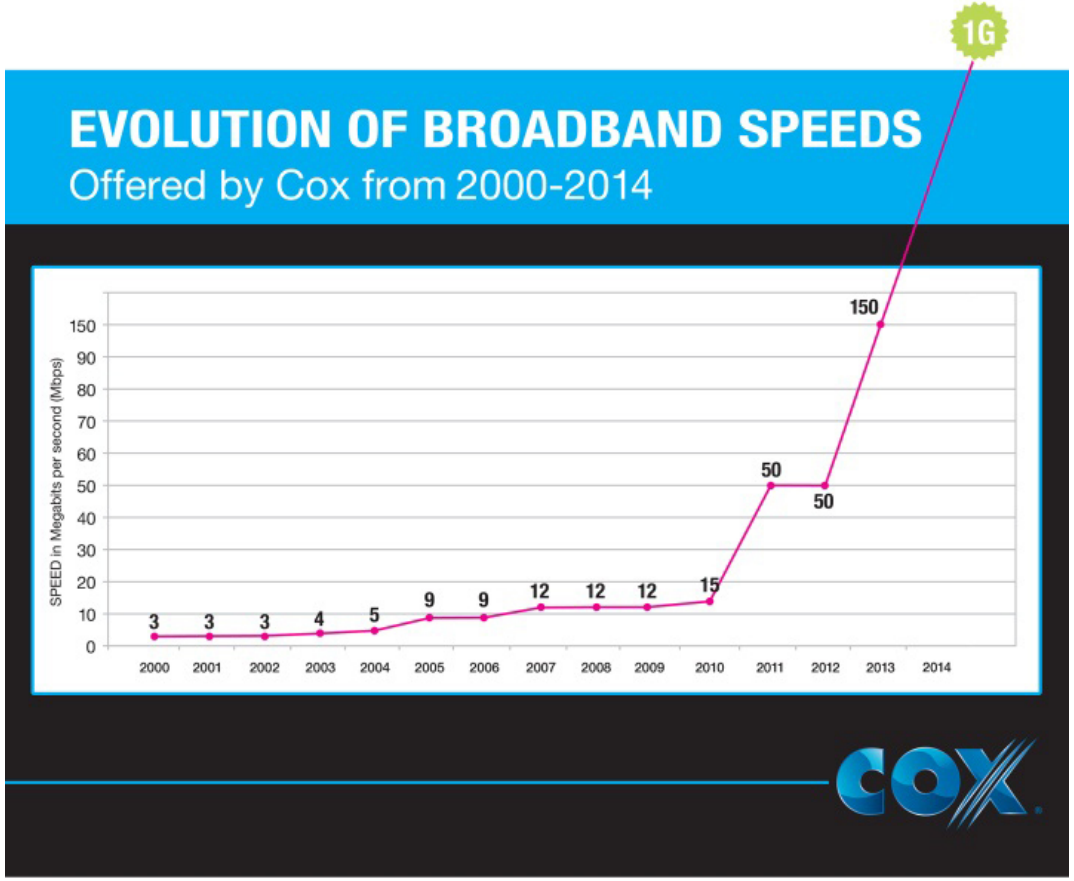
BEACH

- Late-1970s – Kevin Mitnick
- Late-1980s – Computer Worms
- 1990s – Viruses
- 2000s – Fifteen-year-old Michael Calce, known as “Mafiaboy”
- Mid-2000s – Credit Card Attacks
- 2013 – Target Breach
- 2014/2015 – Sony, Home Depot, J.P. Morgan Chase Breach

So what's changed?

BEACH

- Avarage broadband speeds have drastically increased



So what's changed?

BEACH

- Technology has advance way too fast
- iPad has only been around since 2010
- iPhone was first introduced in 2007
- Cloud Services
- Rise in cybercrime

What is security?

BEACH

- *“Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.”*
- Protecting our assets

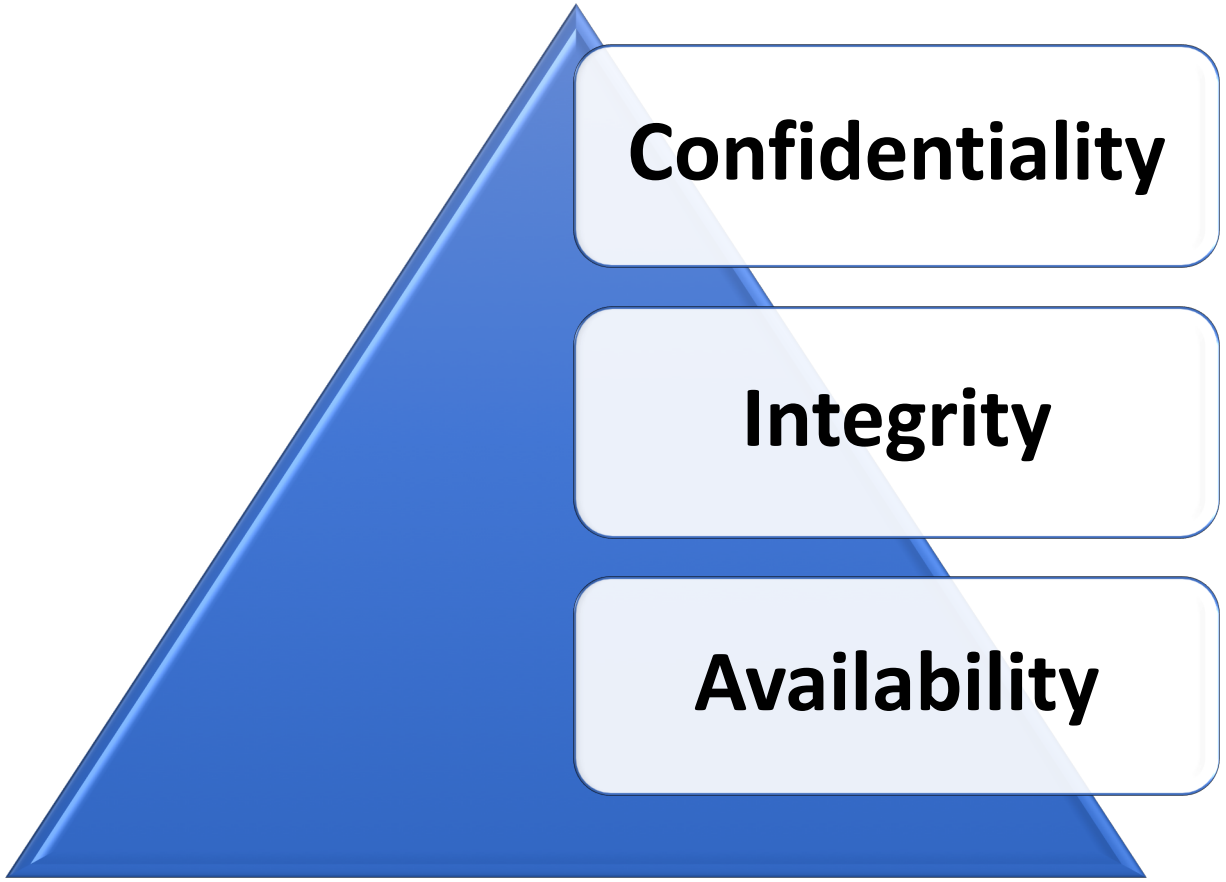
3 Types of Assets

BEACH

- Physical Assets
  - Computer Hardware
  - Gold Bullion
- Logical Assets
  - Passwords
  - Biometrics
  - Software
  - Data
- People

Triad (CIA)

BEACH



Confidentiality

BEACH

- Necessary component of privacy
- Only authorized users should have to access the data
- Unauthorized users should be block
- Clearance Levels
  - Confidential
  - Secret
  - Top Secret

Integrity

BEACH

- Refers to the ability to prevent data from being changed
- No changes should be made to the data, unless those authorized
- Hashes (MD5, SHA1, SHA2)
- Operating systems permissions

Availability

BEACH

- Refers to availability to access our data
- Keeping the system running
- Keeping the data available
- Redundant servers
- Critical Infrastructure

3 Levels of Impact

BEACH

- Low
  - Result in minor damage to organizational assets
  - Result in minor financial loss
  - Result in minor harm to individuals
- Moderate
  - Result in significant damage to organizational assets
  - Result in significant financial loss
  - Result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries
- High
  - Result in major damage to organizational assets
  - Result in major financial loss
  - Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries

3 Levels of Impact

BEACH

- Low
  - Result in minor damage to organizational assets
  - Result in minor financial loss
  - Result in minor harm to individuals
- Moderate
  - Result in significant damage to organizational assets
  - Result in significant financial loss
  - Result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries
- High
  - Result in major damage to organizational assets
  - Result in major financial loss
  - Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries

Threat

BEACH

- Anything that has a potential to cause serious harm to a computer system
- May or may not happen, but has potential to cause serious damage
- Potential for vulnerabilities to turn into attacks
- Threats tend to be more specific to certain environments
- Types of computer threats:
  - Computer viruses, worms, scareware, malware, keyloggers, and rootkits.

Vulnerability

BEACH

- Weaknesses that can be used to harm us
- Holes that can be used by threats
- A system flaw that is left open
- Specific operating system, application, physical location of a office/data center, lack of backup generators, or other factors

Risk

BEACH

- The likelihood that something bad will happen
- In order to have a risk, a threat and a vulnerability are necessary
- A structure made out of wood and set to fire
  - Threat (the fire)
  - Vulnerability (the wood structure)
- A ransomware attack
  - Threat (the ransomware)
  - Vulnerability (the unpatched system, the user, etc)

How to calculate risk

BEACH

Risk	=	Threat	x	Vulnerability
Loss of privacy		The press Angry employees		Software bugs Broken processes
Loss of life		Criminals Government		Human error Legacy systems
Financial losses		Competition Hackers		Ineffective controls Hardware flaws

Difference Between

BEACH

Threat

- A person or thing likely to cause damage or danger
- Can be identify, but cannot be controlled
- Angry or dishonest employees
- Terrorist, Hackers or competitors

Vulnerability

- Being open for attack or damage
- Can be identified and corrected
- Software bugs, broken processes, hardware flaws
- Human error, inadequate Business Continuity Plan (BCP)

4 Types of category attacks

BEACH

Confidentiality	• **Interception / Unauthorized Disclosure**
Integrity	• **Interruption / Disruption** • **Modification / Deception** • **Fabrication / Usurpation**
Availability	• **Interruption / Disruption** • **Modification / Deception** • **Fabrication / Usurpation**

Interception Attack

BEACH

- Attacks that allow unauthorized users access to our data
- Eavesdropping (Passive Attack)
  - listening to phone conversations
  - reading emails
  - Man in the middle attacks (MITM)
- Difficult to detect

Interruption Attack

BEACH

- Cause systems to be unusable or unavailable
  - Temporary
  - Permanent
- Interruption attacks often affect availability, but can also affect integrity
  - DoS Attack on a website (Active Attack)
  - Ransomware

Modification Attack

BEACH

- Involve tampering with the assets
- Primarily consider an integrity attack but could also represent an availability attack
  - Website defacements
  - Involves deletion, insertion, or alteration of data
  - someone can purposefully change the file signature of a file to make it look something else.

Fabrication

BEACH

- Involves generating data, processes, communications, etc.
- Primarily affect integrity, but could also be consider an availability attack
  - Email spoofing
  - Generating additional processes, network traffic, Web traffic

Two Types of Companies

BEACH

- *“There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.” – (Dmitri Alperovitch, 2011)*

Do you think you are secured?

BEACH

- When are we secure?
- Is the use of strong password enough?
- Are systems secure if they are properly patched?
- Are air gap environments secure?
- Are we secure if we disconnect from the internet?

When are we insecure?

BEACH

- When systems are not updated
- When using weak passwords
- When downloading programs
- When opening infected emails
- When using open wireless networks
- When people don’t have the right training

Human Factors

BEACH

- Only secured as your weakest link
- Passwords are compromised
- Tricked into clicking a link or execute a file
- Programming errors
- Programmers creating backdoors
- Easy to exploit
- Insider threat

Semester Project Topics

BEACH

- Phishing Attack
- Social Engineering Attack
- Man in the Middle Attack
- Modification Attack
- DoS Attack