Software Security

Lecture 1

What is Software Security ?

- Not the same as security software
  - Firewalls, intrusion detection, encryption
  - Protecting the environment within which the software operates
- Engineering software so that it continues to function under attack
- The ability of software to **recognize, resist, tolerate, and recover** from events that threaten it
- **The goal: Better, defect-free software that can function more robustly** in its operational production environment

Why Software Security?

- Developed nations' economies and defense depend, in large part, on the reliable execution of software
- Software is ubiquitous, affecting all aspects of our personal and professional lives.
- Software vulnerabilities are equally ubiquitous, jeopardizing:
  - Personal identities Intellectual property
  - Consumer trust
  - Business services, operations, & continuity
  - Critical infrastructures & government
- Most successful attacks result from:
  - Targeting and exploiting known, unpatched software vulnerabilities
  - Insecure software configurations
- Many of these are introduced during software design & development
- Increasing trend of assembling systems from purchased parts means there can be vulnerabilities before the software can be built.

Cost of Some Prominent Security Breach

- Target Breach (2013)
  - Stole 40M credit and debit records, 70M customer records
  - Cost: ~$200M
- Sony Hack (2014)
  - Leaked employee personal information, copies of unreleased and future films
  - Cost: ~$100M
- Bangladesh Bank Cyber Heist (2016)
  - Attempted for $1B, could get away with $101M
- Equifax Data Breach (2017)
  - 605M user records
  - Cost $700M

Software Security vs Application Security

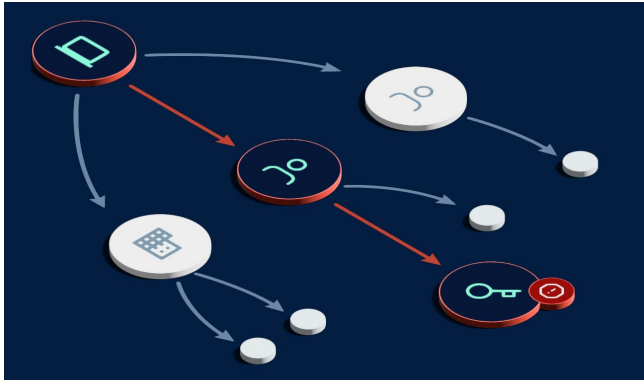
Software Security	Application Security
Defend against vulnerabilities and attacks by building software securely in the first place.	Defend against vulnerabilities and attacks after development and deployment.
Proactive Approach	Reactive Approach

Security vs Dependability

- The safety and security communities use different languages
- For us, dependability = reliability + security
- Reliability and security are often strongly correlated in practice
- One example for each
    - Reliability: “Bob will be able to read this file”
    - Security: “The Chinese Government won’t be able to read this file”

Software Security Terminologies

- Assets : Objects which require protection.
- Attack Path/Vector : Mechanism/technique applied to access an asset.
- Attack Surface : Sum of all possible attack paths.
- Threat : Potential danger that might cause harm or damage to a system.
- Defects/Weakness/Bugs : Errors that might result in unexpected or undesired behavior.
- Vulnerabilities : Defects exploiting a threat to compromise a system.



Continued

- A principal can be
  - A person
  - Equipment (PC, phone, smartcard, car…)
  - A role (the officer of the watch)
  - A complex role (Alice or Bob, Bob deputising for Alice)
- Secrecy is technical – mechanisms limiting the number of principals who can access information.
- Privacy means control of your own secrets.
- **Confidentiality** is an obligation to **protect someone else's secrets**. Ex - Your medical privacy is protected by your doctors' obligation of confidentiality.
- **Anonymity** has various meanings, from **not being able to identify subjects** to **not being able to link their actions**; it's often about access to metadata.
- An object' s **integrity** lies in its **not having been altered** since the last authorised modification
- **Authenticity** means you 're **speaking to the right principal**.

Continued

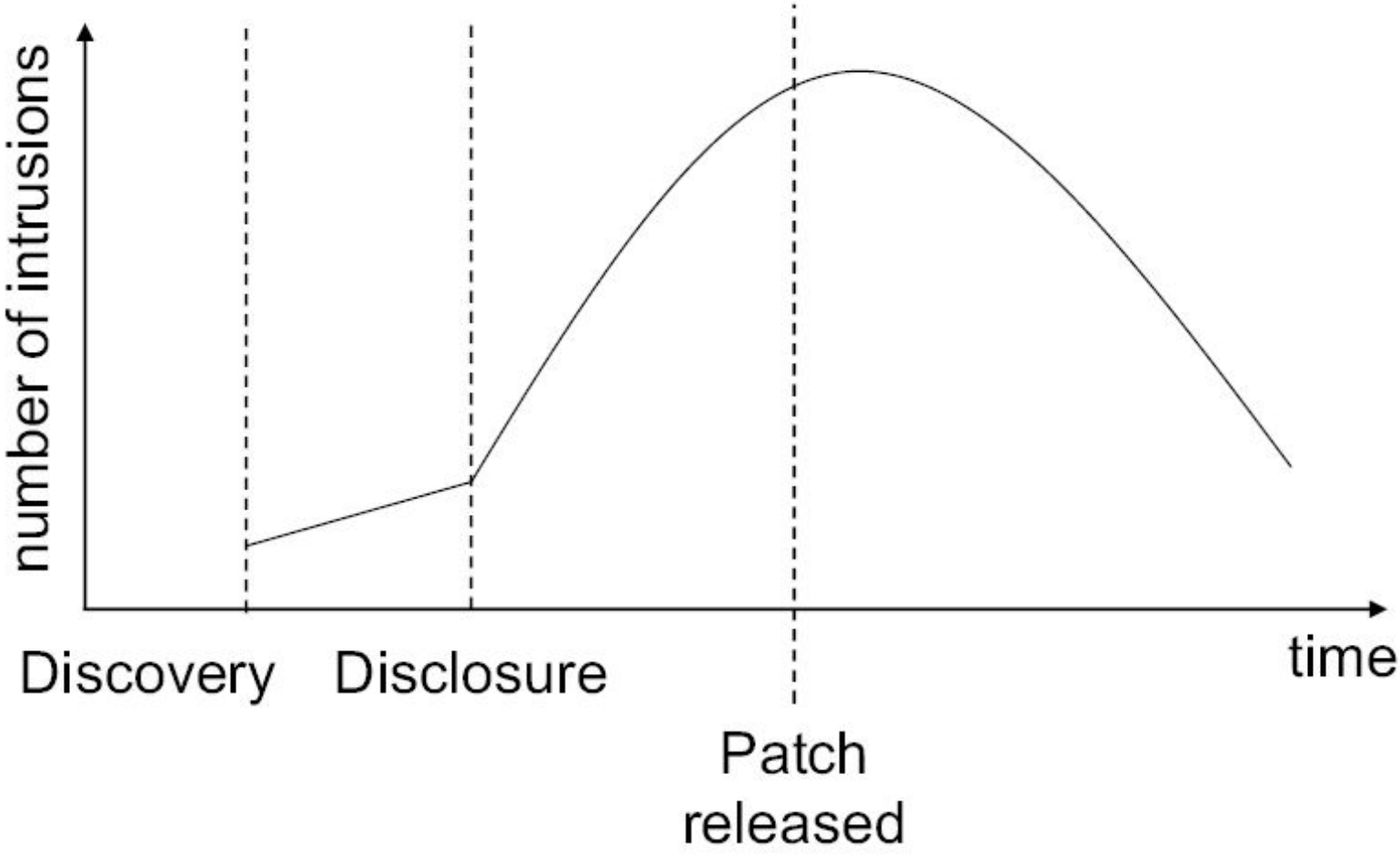
- A hazard is a set of conditions on a system / its environment where failure can lead to an accident
- A critical system, process or component is one whose failure will lead to an accident
- Risk is the probability of an accident
- Uncertainty is where the risk is not quantifiable
- Safety is freedom from accidents.
- Security Policy is a concise statement of protection goals (Typically less than a page)(Security principle for an enterprise)
- Protection Profile is a detailed statement of protection goals (Typically dozens of pages)(Security policy for firewall device)
- Security Target is a detailed statement of protection goals applied to a particular system (May have hundred of pages)(Security policy for XYZ firewall device)

Software Security Dilemma

- Security is typically not the primary competence or focus of the developers or designers
  - 86% developers do not view application security as top priority
  - 29% developers believe vulnerability free code writing needs to be prioritized
  - 67% developers shipped code with know vulnerabilities
- Security is frequently viewed as an impediment to functionality (something that gets in the way).
- Security often contrasts with usability.

Weak Password: abc123
Strong Passphrase: PurpleMonkeyDishwasherFlyingSaucer7

Bad Effects of The Dilemma



Software Assurance

Application of technologies and processes to achieve a required level of confidence that **software systems and services function** in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures.

Security Principles

These are the **set of standards** that are designed to **minimize the vulnerability** of systems and services to attackers who may obtain unauthorized access to sensitive data and misuse it.

Some major security principles are,

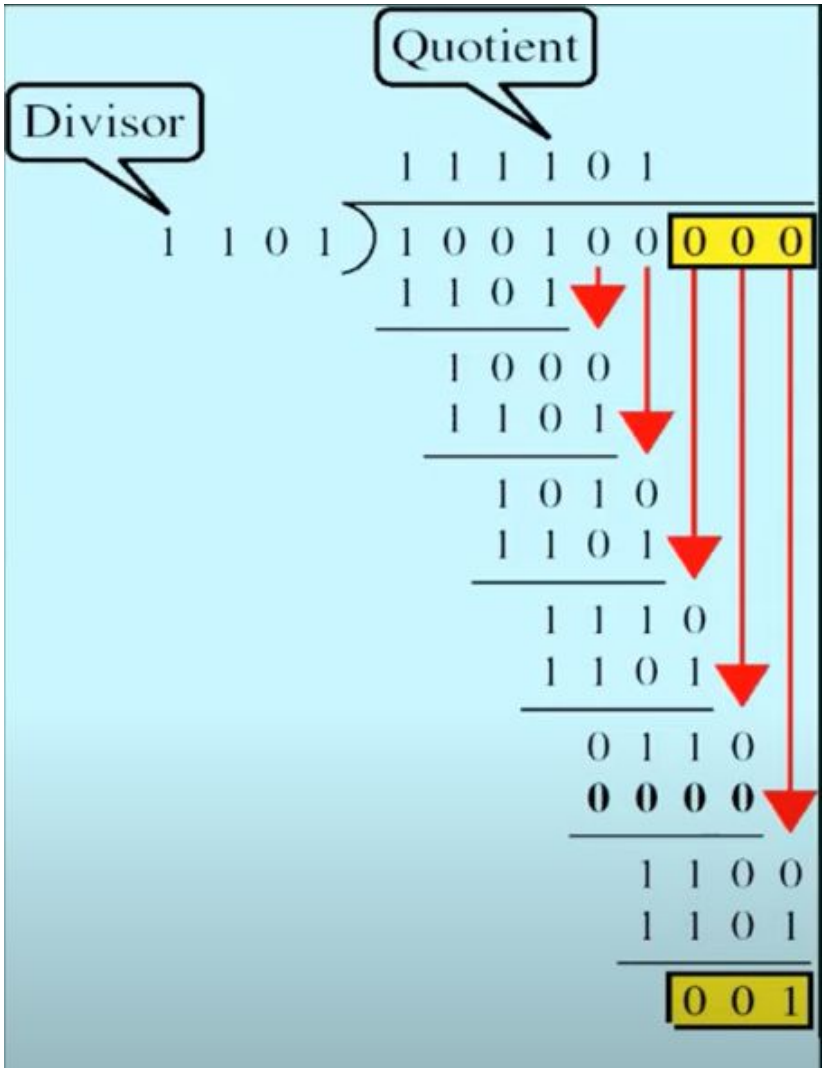
- Confidentiality
- Integrity
- Availability
- Non-Repudiation

Confidentiality

- Resources can only be accessed by authorized entities. And here access means one authorized personnel can **understand or use the resource**.
- Technique : **Encryption** and allowing physical storage media access to only authorized personnel etc.
- Sending sensitive information to unauthorized personnel is loss of confidentiality.
- Suppose, someone knew somehow that an encrypted confidential message is being passed over the network. So, he intercepted the message in the hopes of reading the secret content inside it. Is this a violation of confidentiality?
    - No, because confidentiality means unauthorized entity won't be able to understand the data. Knowing there's some secret is not breach of confidentiality.

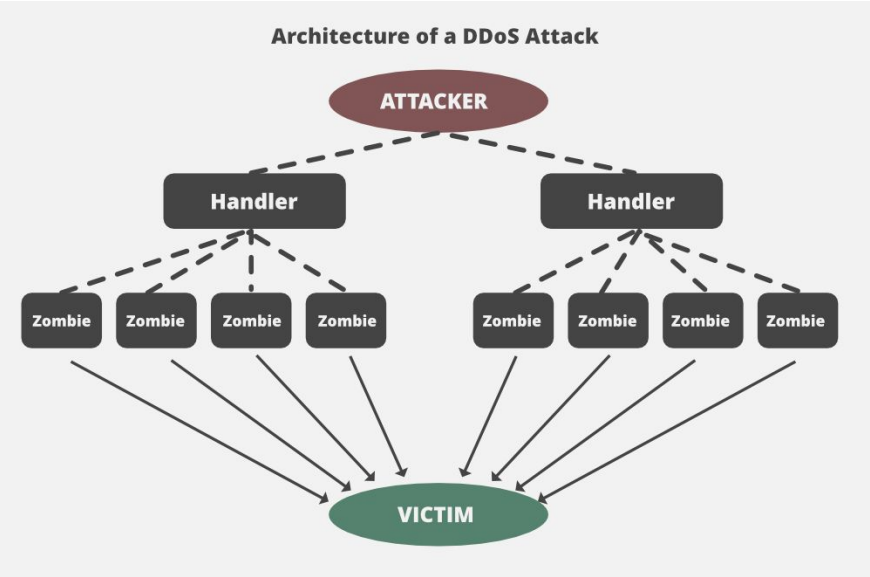
Integrity

- Information resources can not be modified/altered by unauthorized entities.
- Technique : CRC codes, Hash functions (MD5, SHA256)
- The right side image is the process for CRC code generation.
- Change the CGPA in students' result database without authorization is a loss of integrity.



Availability

- Resources are accessible when needed to authorized entities.
- Technique : Redundancy. Having multiple server saving same data.
- Loss of Availability
  - Denial of Service (DoS) or Distributed Denial of Service (DDoS)
  - Ransomware encrypting system data making resources inaccessible



Non-Repudiation

- No party can deny the sending or receiving of a message if they sent or received it.
- Supplements integrity
  - If an authorized individual alters some data maliciously, later it can be proved using non-repudiation techniques. Simply, hacker can not say he is not a hacker.
- Technique : Logs, Digital Signature.
- Detect a problem in the bottom-right scenario.
- What happens if someone steal Alice's private key? That's why you should not write credentials in text files.