Software Security Concepts

Lecture-3

Department of CSE, IUT

What is Computer Security

- Most developers and operators are concerned with **correctness: achieving desired behavior. (What should DO?)**
  - A working banking web site, word processor, blog,…

- Security is concerned with **preventing undesired behavior. (What should Not Do?)**
  - Consider an employee/opponent/hacker/adversary who is actively and maliciously trying to circumvent any protective measures you put in place

A definition of Computer security

Computer security:

The **protection** afforded to an automated information system

in order **to attain** the applicable objectives of

preserving the **integrity, availability and confidentiality**

of information system resources

(includes **hardware, software, firmware, information/data, and telecommunications**)

NIST 1995

What is Software Security

Software security is a kind of computer security that **focuses** on **the secure design and implementation of software.**

- Using the best language, tools, methods

- **Focus of study:**

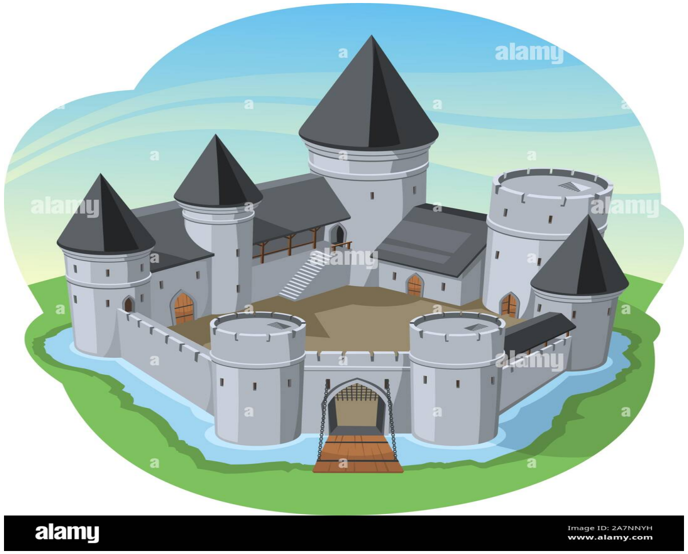
  The Code

Software Security: Approaches

By contrast:

- many popular **approaches to security** treat software as a black box(ignoring the code)
  - OS security, Anti-Virus, Firewalls etc
- White box approach (focus on internal the code and architecture)

Why Software Security?



Anti-Virus, Firewalls are like building **walls** around a **weak interior**

Attacker often **can bypass** the often **defenses** to **attack the weakness within**

Software Security aims to address weakness directly

Security Enforcement Approaches:
Operating System Security

- Operating Systems **mediate a program's actions**
  - **system calls:**
    - Reading and writing files
    - Sending and receiving network packets
    - Starting new program, etc.
- Enforceable policies control actions
  - Programs run by Alice cannot read files owned by Bob
  - Programs run by Bob cannot use TCP port 80
  - Programs run in directory D cannot access files outside of D

Limitation of OS Security

- **Operation System Security focus:**
  - OS security mostly works like **execution monitor only:**
    - **Decision are based on past and current actions**
  - **Whether to allow / dis-allow a program action based on current execution context and program prior actions.**
- **Cannot enforce application-specific policies**, which can be too fine-grained
  - Example: database management system (DBMS)
- **Cannot (precisely) enforce Information Flow Policies**

Security Enforcement Approaches:
Firewalls and IDSs

Limitation of Firewalls and IDSs

Why Software Security is Important??

Follow the video lectures

Software Security – Coursera

https://www.coursera.org › learn › software-security

Offered by **University** of **Maryland**, College Park.

References

Software Security – Coursera

https://www.coursera.org › learn › software-security

Offered by **University** of **Maryland**, College Park.