Secure Programming

Mehmet Tahir SANDIKKAYA

Spring 2022

Istanbul Technical University
Computer Engineering Department

Syllabus

Week	Date	Rct	Covers	Subject	Announcement	Submit
1	22nd Feb		7	Fundamental concepts of security	TP-A	
2	01st Mar		1, 7	Compilation and Execution		
3	08th Mar		1, 7	Stack overflow and its mitigation	Asg1-A	
4	15th Mar		1, 7	Dynamic memory management		
5	22nd Mar	R	3, 7	Canonicalization attacks and mitigation	Asg2-A	Asg1-S
6	29th Mar		2, 7	Injection attacks	Asg1-G	
7	05th Apr	R	2, 7	Injection mitigation	Asg3-A	Asg2-S
8	12th Apr		4	Reverse engineering and obfuscation	Asg2-G	
9	19th Apr		5	Fundamental cryptography		Asg3-S
A	26th Apr	R	5	Principles of computer communication	Asg3-G	MT
-	03rd May			Spring break		
B	10th May		5	XSS & CSRF attacks and mitigation	Asg4-A	
C	17th May	R	5	Race conditions	MT-G	
D	24th May		6	Permission and authorization mechanisms in contemporary languages		Asg4-S
E	31st May		7	Test and static analysis tools	Asg4-G	TP-S

Security Introduction

Jargon

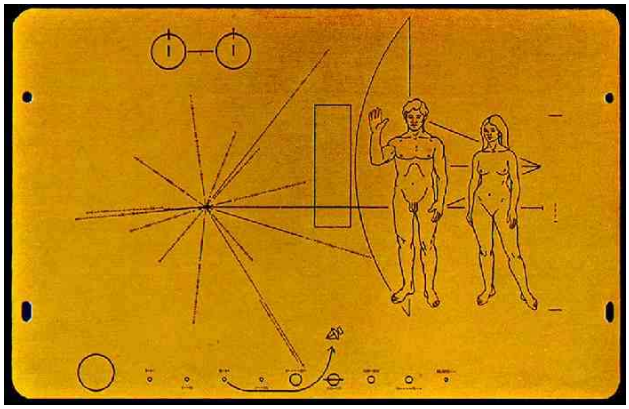
- ✔ What is (computer) security? What is secure programming?
- ✔ Why do we write insecure programs?
- ✔ Open source or closed source?
- ✔ Types of programs (attack surface)
- ✔ How processes work?
- ✔ What are security requirements?

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
  retval = -EINVAL;
```

Any sufficiently advanced stupidity is indistinguishable from malice.

Introduction to Security Concepts

- ✔ Think cost of security: cost of protecting an asset and the real value of an asset
- ✔ A balance in between who spend to protect and who spend to breach the security
- ✔ Next, think of usability for the asset's owner: e.g. Voyager plate



CIA

Confidentiality Confidentiality of information/data. Easy to extend it to privacy when confidential information is relevant to people.
Integrity Integrity of data or the whole working system. Is it authentic? Even if it is not, who is accountable?
Availability Could users of a system or owners of an information benefits from it whenever they want?

Why is security so difficult?

- ✔ Security is not simple
- ✔ It is not an achievement, but a process
- ✔ Requires constant monitoring, it is overwhelming
- ✔ Mostly the flaw is understood after an incident happens
- ✔ It is necessary to decide where to use specific mechanisms
- ✔ Myopic good decisions may badly affect holistic security of a system
- ✔ Mechanisms mostly composed of several sub-algorithms and sub-protocols
- ✔ Marginal benefit after too much investment until a security breach occurs
- ✔ Strong security is mostly perceived as cumbersome

Some Definitions and Terminology

[The International Telegraph and Telephone Consultative Committee, 1991]

Security attack Any action that compromises the security of information owned by an organization
Security mechanism A process or device that is designed to detect, prevent, or recover from a security attack
Security service A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Some Definitions and Terminology

[Shirey, 2007]

Threat A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability
Attack An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system

Any sufficiently advanced negligence is indistinguishable from malice.

Taxonomy of Attacks

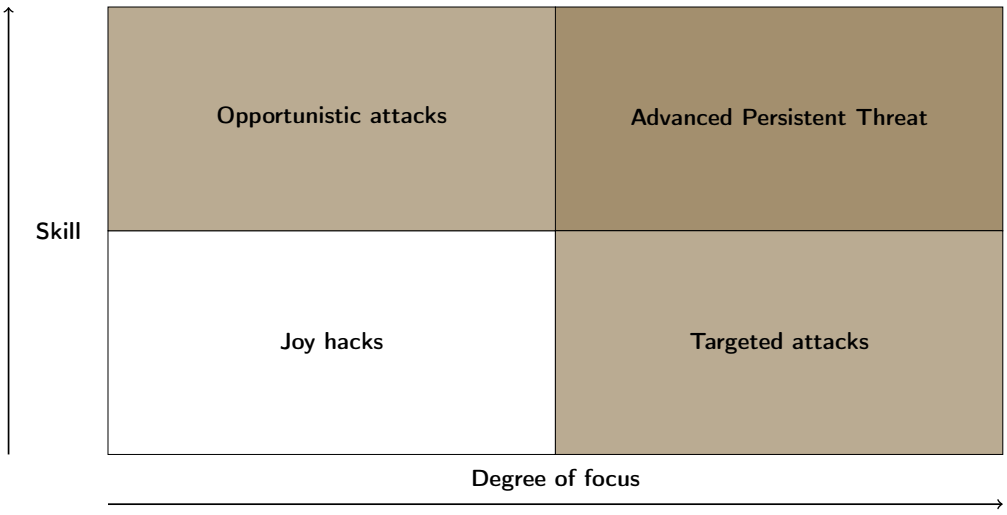
Passive attacks The quieter you become, the more you can hear (eavesdropping, traffic analysis)
Active attacks Have many forms, difficult to prevent (masquerading, replay, message modification, DoS)

Fundamental Design Principles

- ✔ Economy of mechanism
- ✔ Fail-safe defaults
- ✔ Complete mediation
- ✔ Open design
- ✔ Separation of privilege
- ✔ Least privilege
- ✔ Least common mechanism
- ✔ Psychological acceptability
- ✔ Isolation
- ✔ Encapsulation
- ✔ Modularity
- ✔ Layering
- ✔ Least astonishment

Why should someone attack?

The threat matrix



Where can I attack?

The reachable and exploitable vulnerabilities in a system

- ✔ Open ports on outward facing Web and other servers, and code listening on those ports
- ✔ Services available on the inside of a firewall
- ✔ Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- ✔ Interfaces, SQL, and Web forms
- ✔ An employee with access to sensitive information vulnerable to a social engineering attack

Kill Chain

Common steps of an attack

1. Reconnaissance
2. Intrusion
3. Exploitation
4. Privilege Escalation
5. Lateral Movement
6. Obfuscation
7. Denial of Service
8. Exfiltration

References

[Shirey, 2007] Shirey, R. W. (2007). Internet security glossary, version 2. Request for Comments 4949, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4949.txt.

[The International Telegraph and Telephone Consultative Committee, 1991] The International Telegraph and Telephone Consultative Committee (1991). Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800, International Telecommunication Union.