Information Security and Privacy

INFO30006

Lecturer: Heidi Tscherning

Lecture 11: information security

AGENDA

I INTRODUCTION

II SECURITY THROUGH OBSCURITY

III BASIC SECURITY ANALYSIS

IV KNOWLEDGE LEAKAGE TALK

WHAT IS SENSITIVE INFORMATION?

https://www.youtube.com/watch?v=3hHnT1szO7c

WHAT IS INFORMATION SECURITY?

Protecting information systems against misuse and interference from external parties.

"*Building systems to remain dependable in the face of malice, error or mischance*"

(Ross Anderson, professor of security engineering)

PROPERTIES OF A SECURE SYSTEM

CONFIDENTIALITY:

- Information* is protected from unintended disclosure (secrecy, privacy, access control)

INTEGRITY:

- System, data and information* are maintained in a correct and consistent condition

AVAILABILITY:

- System, data and information* are usable when needed (includes timeliness)

* We are increasingly discussing knowledge along with information (knowledge leakage talk today)

SECRECY, CONFIDENTIALITY

SECRECY

- Keep data hidden
- E.g. Alice kept an incriminating secret

CONFIDENTIALITY

- Keep (someone else's) data hidden from unauthorised entities
- E.g. banks keep much account information confidential

PRIVACY, ANONYMITY

PRIVACY

- Use/disclose a person's data according to a set of rules
- E.g., to protect Alice's privacy, company XYZ removed her name before disclosing information about her purchases

ANONYMITY

- Keep identity of a protocol participant secret (think security audit!)
- E.g. to hide her identity from the web server, Alice uses The Onion Router (TOR) to communicate

INTEGRITY

DATA INTEGRITY

- Ensure data is “correct” (i.e., corrected syntax and unchanged)
- Prevents unauthorised or improper changes
- E.g., Trent always verifies the integrity of his data after restoring a backup, to ensure that no incorrect records exist

Integrity, Authentication

Entity authentication or identification

- Verify the identity of another protocol participant
- E.g., Alice authenticates Bob each time they establish a secure connection

Data authentication

- Ensure that data originates from claimed sender
- E.g., for every message Bob sends, Alice authenticates it to ensure that it originates from Bob

Integrity, Authentication

Data integrity

- Ensure data is “correct” (i.e., correct syntax & unchanged)
- Prevents unauthorized or improper changes
- E.g., Trent always verifies the integrity of his database after restoring a backup, to ensure that no incorrect records exist

Entity authentication or identification

- Verify the identity of another protocol participant
- E.g., Alice authenticates Bob each time they establish a secure connection

AGENDA

I INTRODUCTION

II SECURITY THROUGH OBSCURITY

III BASIC SECURITY ANALYSIS

IV KNOWLEDGE LEAKAGE TALK

SECURITY THROUGH OBSCURITY

QUESTION: WHAT IS "SECURITY THROUGH OBSCURITY"?

SECURITY THROUGH OBSCURITY

QUESTION: WHAT IS "SECURITY THROUGH OBSCURITY"?

1. Is it harder to break into a safe with the lights on or the lights off?
2. Would it be easier for the safe-cracker if they knew the make and model of the safe? Or wouldn't it?
3. What about their ability to see the numbers of the safe?

SECURITY THROUGH OBSCURITY

QUESTION: WHAT IS "SECURITY THROUGH OBSCURITY"?

1. Is it harder to break into a safe with the lights on or the lights off?
2. Would it be easier for the safe-cracker if they knew the make and model of the safe? Or wouldn't it?
3. What about their ability to see the numbers of the safe?

SECURITY THROUGH OBSCURITY

!THE LESS INFORMATION YOU GIVE OUT, THE BETTER!

- If a company is known to use e.g. Apache 2.2 on their web server, hackers search for known security holes in just one type of software.
- Information help hackers by narrowing field of potential exploits
- SOLUTION?
  1. Limit exposed information
  2. "What is the least information to get the job done? (all public information is a potential clue for a hacker)
  3. Obscurity does NOT mean (intended) "misdirection"! May violate the principle that "SIMPLE IS MORE SECURE"

AGENDA

I INTRODUCTION

II SECURITY THROUGH OBSCURITY

III BASIC SECURITY ANALYSIS

IV KNOWLEDGE LEAKAGE TALK

REMEMBER SECURITY THREATS FROM W2?

Common security threats towards organisations:

- Human errors
- compromise to IP
- espionage
- extortion/ransomware
- theft
- software and hardware attacks
- forces of nature…

REAL WORLD SECURITY

REAL-WORLD SECURITY BOILS DOWN TO THE FOLLOWING:

- Specification/policy: What is the system supposed to do?
- Implementation/mechanism: How does it do it?
- Correctness/assurance : Does it really work?
- Human nature: Can the system survive "clever" users?

BASIC SECURITY ANALYSIS

How do we as organisations secure system x? Is system x secure?

1. Who/what are we PROTECTING?
2. Who/what is the ADVERSARY/POTENTIAL THREAT?
3. What are the SECURITY REQUIREMENTS?
4. What SECURITY STRATEGIES are effective?

1. WHAT ARE WE PROTECTING?

- Enumerate information and knowledge ASSETS and their VALUE
- Understand architecture of the system
- Useful questions to ask:
  1. What is the operating value, i.e., how much would we lose per day/hour/minute if the resource stopped?
  2. What is the replacement cost? How long would it take to replace it?

2. WHO IS THE ADVERSARY?

1. IDENTIFY potential attackers
   - How motivated are they?
2. Estimate ATTACKER RESOURCES
   - Time and money
3. Estimate NUMBER OF ATTACKERS, PROBABILITY OF ATTACK

2. COMMON (ABSTRACT) ADVERSARY?

ATTACKER ACTION

Passive attacker: eavesdropping

Active attacker: eavesdropping + data injection

ATTACKER SOPHISTICATION

Ranges from script kiddies to government-funded group of professionals

ATTACKER ACCESS

External attacker: no knowledge of cryptographic information, no access to resources

Internal attacker: complete knowledge of all cryptographic information, complete access

- Result of system compromise

3. WHAT ARE THE SECURITY REQUIREMENTS?

ENUMERATE SECURITY REQUIREMENTS

1. Confidentiality
2. Integrity
3. Authenticity
4. Availability
5. Auditability
6. Access control
7. Privacy
8. …

4. STRATEGIES TO ACHIEVE SECURITY

NO SECURITY

- Legal protection (deterrence)
- Innovative: patent attack, get protection through patent law

BUILD STRONG SECURITY DEFENCE

- Use cryptographic mechanisms
- Perimeter defence (firewall), VPN

4. STRATEGIES TO ACHIEVE SECURITY

RESILIENCE TO ATTACK

- Multiple redundant systems (“hot spares”)

DETECTION AND RECOVERY (& OFFENSE ?)

- Intrusion detection system
- Redundancy, backups, etc.
- Counterstrike? (Legal issues?)

4. STRATEGIES TO ACHIEVE SECURITY

TYPE OF SECURITY STRATEGIES

- Prevention
- Deterrence
- Surveillance
- Detection and response
- Perimeter defense
- Compartmentalization
- Layering

4. STRATEGIES TO ACHIEVE SECURITY

A. PREVENTION AS A STRATEGY

- Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure.
- Priority is to block attacks on organization by implementing barriers around valuable assets in anticipation of attack

4. STRATEGIES TO ACHIEVE SECURITY

B. COUNTERMEASURE AS A STRATEGY

- Preventive Countermeasures are simply barriers
- The barrier prevents the attacker from getting access to the asset behind it
- Gold: Fort Knox
- Turtle: Turtle Shell
- Satellite: (Outer) Space

4. STRATEGIES TO ACHIEVE SECURITY

PREVENTION

- Prevention is passive (always there, working all the time in the background)
- Not all preventive measures are physical
  - Some computer software is sold with codes built in that prevents them from being copied properly
- Prevention is the hardest strategy to implement and often the most expensive
- Protecting a VIP 24 hours a day, 365 days a year from assassination (and expensive) with a high degree of readiness is difficult
- And an expert assassin will still get their target

4. STRATEGIES TO ACHIEVE SECURITY

D. DETECTION AND RESPONSE

- Detection is aimed at identifying behaviors that impact security to enable response (taking appropriate corrective action) in a targeted manner
  - E.g. alarm, IDS system, etc.
- Response takes appropriate corrective actions against identified attacks
  - E.g. guards

4. STRATEGIES TO ACHIEVE SECURITY

DETERRENCE AS A STRATEGY

- Deterrence employs disciplinary action to influence human behavior and attitude
- Influenced by two factors:
  - Certainty of sanctions
  - Severity of sanctions
- Example – Provisions in security policy may deter employees from criminal acts by specifying punishments for violations

4. STRATEGIES TO ACHIEVE SECURITY

SURVEILLANCE AS A STRATEGY

- Surveillance is the systematic monitoring of the security environment towards developing situational awareness to assist in adapting to fast changing circumstances and threats
- Surveillance has broader aims (to understand the environment) than detection (to identify a specific behaviour)
- Example – Monitoring activity logs
- Example – CCTV used to monitor surroundings of organization

4. STRATEGIES TO ACHIEVE SECURITY

DECEPTION

- Deception distracts an attacker's attention from its goal by using decoys or equivalent to lead the attacker to waste time and resources
- Examples:honeypots and honeynets

4. STRATEGIES TO ACHIEVE SECURITY

PERIMETER DEFENSE

- Perimeter defense is a physical or logical boundary defined for a domain or enclave within which a security policy or security architecture applies
- In information security this technique is commonly used by means of a firewall choking off incoming traffic to information assets

4. STRATEGIES TO ACHIEVE SECURITY

COMPARTMENTALISATION

- Compartmentalisation limits an attacker's opportunities by dividing the target area into zones that are secured separately
- This way an attacker with access to one zone does not automatically get access to other zones
- A typical example is a DMZ

4. STRATEGIES TO ACHIEVE SECURITY

LAYERING OR DEFENSE-IN-DEPTH

LAYERING OR DEFERENCE-IN DEPTH

- Layering constructs multiple barriers that complement each other thereby increasing the effectiveness of the defensive system
- This strategy is predicated on the belief that a single strategy is insufficient
- System is resilient because it overlaps countermeasures so that if one fails another backs it up (example forthcoming)

THREAT MODELS

CAN'T PROTECT AGAINST EVERYTHING

- Too expensive
- Too inconvenient
- Not worth the effort

IDENTIFY MOST LIKELY WAYS SYSTEM WILL BE ATTACKED

- Identify likely attackers and their resources
- Dumpster diving or rogue nation?
- Identify consequences of possible attacks
- Mild embarrassment or bankruptcy?
- Design security measures accordingly
- Accept that they will not defend against all attacks

THINK LIKE AN ATTACKER

- Adversary is targeting assets, not defences
- Will try to exploit the weakest part of the defences
  - E.g., bribe human operator, social engineering, steal (physically) server with data

EXERCISE

Class discussion on security of a house

- What are we protecting?
- Who is the adversary?
- What are the security requirements?
- What security approaches are effective?

"The problem is not that there are problems. The problem is expecting otherwise and thinking that having problems is a problem."

Theodore I. Rubin

AGENDA

I INTRODUCTION

II INFORMATION SECURITY

III BASIC SECURITY ANALYSIS

IV KNOWLEDGE LEAKAGE TALK

NEXT SESSION – 10-11

KNOWLEDGE LEAKAGE PRESENTATION BY CARLOS!