Lecture 5:
Security Risk Analysis

What is **Security engineering**?

---

**Security engineering**
is concerned with lowering the risk of intentional unauthorized harm to valuable assets to level that is acceptable to the system’s stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks.

Firesmith, 2003
Risk Analysis

1. Identify explicitly what system assets are targeted?
2. Use explicit knowledge and previous expertise to characterize potential vulnerabilities of the considered system assets
3. Security analyst should impersonate himself as the threat agent (motive, capabilities, means, opportunities)
4. Attack method should be explicitly stated including its major steps
5. Elicit and state what is the impact of the defined risk event
6. Once all components are gathered state what is the risk
Processing of Information

Everything that IT does, reduces to six functions

- Capturing information
  - Keyboard, bar code reader, digital camera

- Transmitting information
  - Wired-, wireless-phone

- Storing information
  - Hard disk, memory card, internet

- Retrieving information
  - From any storage device

- Manipulating information
  - Calculations, combinations of data

- Displaying information
  - Monitor, printer
Functional Decomposition

- **User interaction**
  - Interfacing and/or interacting with users

- **Data/storage management**
  - Storing and management of applications or information

- **Resource management**
  - Resource allocation, global scheduling, process migration,
  - Dynamic configuration of active software components

- **Distribution control**
  - Component collaboration
  - Coordination of local/remote execution
  - Synchronization/concurrency control

- **Communication**
  - Network communication

- **Addressing**
  - Address, identifier and/or name allocation, distribution and discovery/lookup
Risk Analysis

1. Identify explicitly what **system assets** are targeted?

2. Use explicit knowledge and previous expertise to characterize potential **vulnerabilities** of the considered system assets

3. Security analyst should impersonate himself as the threat agent (motive, capabilities, means, opportunities)

4. Attack method should be explicitly stated including its major steps

5. Elicit and state what is the impact of the defined risk event

6. Once all components are gathered state what is the risk
Security Risk Management
Domain Model

Common Vulnerabilities and Exposures: [https://cve.mitre.org/cve/](https://cve.mitre.org/cve/)
National vulnerability database: [https://nvd.nist.org](https://nvd.nist.org)
OWASP vulnerability database: [https://www.owasp.org/index.php/Vulnerability](https://www.owasp.org/index.php/Vulnerability)

Seven Pernicious Kingdoms

1. Input validation and Representation
2. API Abuse
3. Security Features
4. Time and State
5. Error Handling
6. Code Quality
7. Encapsulation

* Environment

<table>
<thead>
<tr>
<th>1. Input validation and Representation</th>
<th>5. Error Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. API Abuse</td>
<td>6. Code Quality</td>
</tr>
<tr>
<td>4. Time and State</td>
<td>* Environment</td>
</tr>
</tbody>
</table>

**Caused by**
- Meta-characters, alternate encoding, numeric representation

**Problems result from**
- Lack of input validation
- Representation issues
  - easy target
  - often-used point of attack

**Resulting problems**
- Buffer overflows
- Cross-site scripting attacks
- SQL injection
- Command injection
- Setting Manipulation
- String termination error
- ...

**Caused by**
- The callee failing to honor its end of the contract

**Case**
- If a program fails to call `chdir()` after calling `chroot()`, it violates the contract that specifies how to change the active root directory in a secure fashion

**Resulting problems**
- Dangerous functions
- Often misused exception handling
- Unchecked return value
- Directory restriction
- ...
1. Input validation and Representation

2. API Abuse

3. Security Features
   - Software security is not security software

4. Time and State
   - In order for more than one component to communicate, state must be shared, and all that takes time

5. Error Handling

6. Code Quality

7. Encapsulation

---

**Caused by**
- Incorrect implementation
- Incorrect use of security features like
  - Authenticity, Access control, Cryptography, Digital signatures, ...

**Resulting problems**
- Insecure randomness
- Missing access control
- Password management
- Privacy violation
- ...

---

**Caused by**
- Distributed computing
- Sharing state
- Multithreading
- A programmer’s belief that everything happens in one continuous sequence

**Resulting problems**
- Deadlock
- Failure to begin a new session upon authentication
- Insecure temporary file
- File access race condition (TOCTOU)
- ...

---
1. Input validation and Representation
2. API Abuse
3. Security Features
4. Time and State

5. Error Handling
   - Errors and error handling represent a class of API
   - Errors related to error handling are so common that they deserve a special kingdom of their own

* Environment

- Caused by
  - Unexpected input – unexpected behaviour
  - Concept of exceptions in modern programming languages
  - Insecure use and handling of exceptions

- Resulting problems
  - Catch NullPointerException
  - Empty catch block
  - Overly-broad catch block
  - Overly broad throw declaration
  - Unchecked return value

---

1. Input validation and Representation
2. API Abuse
3. Security Features
4. Time and State

5. Error Handling
6. Code Quality
7. Encapsulation

* Environment

- Caused by
  - Lack of compliance with design
  - Insecure code is buggy code
  - Code readability
  - Complexity of code vs. complexity the human brain is able to manage
  - Forgetting to remove old code

- Resulting problems
  - Inconsistent implementation
  - Memory leak
  - Obsolete code
  - Underfined behaviour
  - Uninitialised variable
  - Unreleased resource
  - Use after free
  - …
• **Caused by**
  - Lack of clear boundaries
    - Between WebApp and system resources
    - Between validated and unvalidated data
    - Between classes with various methods
  - Lack of attention to trust models and trust boundaries

• **Resulting problems**
  - Comparing classes by name
  - Data leaking between users
  - Leftover debug code
  - Mobile code: non-final public field
  - Trust boundary violation
  - …

• **Caused by**
  - The software you are developing running on a machine…
  - … with an operating systems…
  - … and other software…
  - … quite possibly connected to other machine through a network…
  - … all the stuff that is outside the code but is still critical to the security of the created software

• **Resulting problems**
  - Misconfiguration issues
  - Insecure compiler optimisation
  - …
Risk Analysis

1. Identify explicitly what system assets are targeted?
2. Use explicit knowledge and previous expertise to characterize potential vulnerabilities of the considered system assets

3. Security analyst should impersonate himself as the threat agent (motive, capabilities, means, opportunities)

4. Attack method should be explicitly stated including its major steps

5. Elicit and state what is the impact of the defined risk event

6. Once all components are gathered state what is the risk

Threat agent

(ben Othmane ET AL, 2014)
Characteristics of Threat agent
(ben Othmane et al. 2014; Shostack 2014)

• Opportunity – time to perform a successful attack

<table>
<thead>
<tr>
<th>Object type</th>
<th>Capability examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware device</td>
<td>Physical access</td>
</tr>
<tr>
<td>Software component</td>
<td>Local access (e.g., copying); Communicate with the component from within the local domain; Communicate with the component from outside the local domain.</td>
</tr>
<tr>
<td>Database</td>
<td>Query the database and modify the data files.</td>
</tr>
<tr>
<td>Communication link</td>
<td>Intercept messages and modify messages, or remove messages.</td>
</tr>
</tbody>
</table>

• Motivation
  – Curiosity
  – Personal fame
  – Personal gain
  – National interest
    • Legitimate
    • Illegitimate

• Expertise
  – Script kiddie
  – Undergraduate
  – Experts
  – Specialist

Threat Agent Expertise
(Shostack, 2014)

• Script kiddie
  – Use the tools an applications created by others
  – No real system knowledge
  – Follow instructions and use different available tools

• Undergraduate
  – Mostly use tools and applications other write
  – Can do minor modification (to these tools)
  – Lack skills to do anything more than twist and adjust a few dials and settings

• Expert
  – Supply tools and applications
  – Write worms and viruses
  – Write applications that snoop networks for weaknesses
  – Comfortable by working in kernel, reading protocol traces

• Specialist
  – Specialised training
  – Access critical resources
  – Do not leave traces of their work
  – Work carefully and methodically
  – Snooping and breaking computer is their job
Characteristics of Threat agent

(ben Othmane ET AL, 2014; Shostack, 2014)

- **Opportunity**
  - Time to perform a successful attack

- **Motivation**
  - Curiosity
  - Personal fame
  - Personal gain
  - National interest

- **Expertise**
  - Script kiddy
  - Undergraduate
  - Experts
  - Specialist

Risk Analysis

1. Identify explicitly what **system assets** are targeted?
2. Use explicit knowledge and previous expertise to characterize potential **vulnerabilities** of the considered system assets
3. Security analyst should impersonate himself as the **threat agent** (motive, capabilities, means, opportunities)
4. **Attack method** should be explicitly stated including its major steps
5. Elicit and state what is the impact of the defined risk event
6. Once all components are gathered state what is the risk
STRIDE
(Microsoft)

- **Spoofing** – pretending to be someone/something than intended
- **Tampering** – modifying something on the disk/file/network/memory
- **Repudiation** – claiming that someone did not do something or were not responsible
- **Information disclosure** – providing information to someone not authorised to see it
- **Denial of service** – absorbing resources needed to provide the service
- **Elevation of privileges** – allowing someone to do something they are not authorised to do

Threats to (Distributed) System
(first level threats)

- Identify attacks
- Network communication attacks
- Network protocol attacks
- Passing illegal data attacks
- Stored data attacks
- Remote information inference
- Loss of accountability
- Uncontrolled operations
Threats to (Distributed) System
(first level threats)

• Identify attacks
  • Network communication attacks
  • Network protocol attacks
  • Passing illegal data attacks
  • Stored data attacks
  • Remote information inference
  • Loss of accountability
  • Uncontrolled operations

• Attacker attempts to fabricate or misuse identities in a system

• Examples
  – Identity spoofing
  – Advantageous identity allocation

Threats to (Distributed) System
(first level threats)

• Identify attacks
  • Network communication attacks
  • Network protocol attacks
  • Passing illegal data attacks
  • Stored data attacks
  • Remote information inference
  • Loss of accountability
  • Uncontrolled operations

• Threats to communication between distributed components

• Examples
  – Message secrecy violation
  – Message integrity violation
  – Message authenticity violation
  – Traffic analysis, protocol sniffing
  – Covert network channel
  – Session hijacking
  – Session state poisoning
  – Route poisoning
  – Message flooding
Threats to (Distributed) System
(first level threats)

- Identify attacks
- **Network communication attacks**
  - Network protocol attacks
  - Passing illegal data attacks
- Stored data attacks
- Remote information inference
- Loss of accountability
- Uncontrolled operations

- Threats to communication between distributed components

- **Examples**
  - Message secrecy violation
  - Message integrity violation
  - Message authenticity violation
  - Traffic analysis, protocol sniffing
  - Covert network channel
  - Session hijacking
  - Session state poisoning
  - Route poisoning
  - Message flooding
Threats to (Distributed) System
(first level threats)

- Identify attacks
- Network communication attacks
- Network protocol attacks
- Passing illegal data attacks
- Stored data attacks
- Remote information inference
- Loss of accountability
- Uncontrolled operations

Threats to communication between distributed components

Examples
- Message secrecy violation
- Message integrity violation
- Message authenticity violation
- Traffic analysis, protocol sniffing
- Covert network channel
- Session hijacking

Messages in transit
- intercepted and their contents read by an attacker
- intercepted and modified, replaced, corrupted or simply deleted by an attacker

Threats to (Distributed) System
(first level threats)
Threats to (Distributed) System
(first level threats)

- Identify attacks
- Network communication attacks
- Network protocol attacks
- Passing illegal data attacks
- Stored data attacks
- Remote information inference
- Loss of accountability
- Uncontrolled operations
- Threats specifically to the network protocols used for communication

- Examples
  - Message secrecy violation
  - Message integrity violation
  - Message authenticity violation
  - Traffic analysis, protocol sniffing
  - Covert network channel
  - Session hijacking
  - Session state poisoning

Secure communication
- message encryption
- message hashing, error detection codes
Threats to (Distributed) System

(first level threats)

• Identify attacks
• Network communication attacks
• Network protocol attacks
  • **Passing illegal data attacks**
• Stored data attacks
• Remote information inference
• Loss of accountability
• Uncontrolled operations

• Input data is manipulated by attacker for some malicious purpose
  
  • **Examples**
    – Injection

Threats to (Distributed) System

(first level threats)

• Identify attacks
• Network communication attacks
• Network protocol attacks
• Passing illegal data attacks
  • **Stored data attacks**
• Remote information inference
• Loss of accountability
• Uncontrolled operations

• Threats on storage data
  
  • **Examples**
    – Corruption
Threats to (Distributed) System
(first level threats)

- Identify attacks
- Network communication attacks
- Network protocol attacks
- Passing illegal data attacks
- **Remote information inference**
- Loss of accountability
- Uncontrolled operations

- Extracting information from a component or remotely, i.e., over network

- **Examples**
  - Scanning (information gathering)
  - Probing (vulnerability checking)
  - Output information disclosure
  - Data inference

- Impact accountability attributes

- **Examples**
  - Track erasing
  - Repudiation
Threats to (Distributed) System  
(first level threats)

- Identify attacks
- Network communication attacks
- Network protocol attacks
- Passing illegal data attacks
- Remote information inference
- Loss of accountability
- **Uncontrolled operations**

- Exploits existing system functionality in ways that would not normally be allowed (e.g., race conditions, access to data)

- **Examples**
  - Unauthorized access
  - Invoking unauthorized operations
  - Spoofing privileged processes
  - Unsafe code execution
  - Exploitation of tight component coupling
  - Process overflow attack
  - Exploiting concurrency flaws
  - Resource exhaustion
  - Targeted process crashing

---

Security risk management process
Threats to Security Infrastructure
(second level threats)

• Cryptography attacks
• Countermeasure design
• Configuration/administration
• Network protocol threats

Threats to Security Infrastructure
(second level threats)

• Cryptography attacks
• Countermeasure design
• Configuration/administration
• Network protocol threats

• Threats to countermeasures using cryptography

• Examples
  – Forging cryptographic credentials
  – Abuse of weak algorithm
  – Exploiting vulnerable security protocol
  – Password attacks (guessing, brute force, rainbow tables)
Threats to Security Infrastructure  
(second level threats)

• Cryptography attacks
• Countermeasure design
• Configuration/administration
• Network protocol threats

• Threats to the way certain countermeasures are (or may be) designed

• Examples
  – Use of default credentials
  – Bypassing controls
  – Leveraging authorization model

Threats to Security Infrastructure  
(second level threats)

• Cryptography attacks
• Countermeasure design
• Configuration/administration
• Network protocol threats

• Threats related to configuration and/or administration of the security system

• Examples
  – Exploiting bad policies
  – Unauthorized modification of rights
Threats to Security Infrastructure
(Second level threats)

- Cryptography attacks
- Countermeasure design
- Configuration/administration
- Network protocol threats

- Also at the first level
- Threats applicable to secure protocol design

Risk Analysis

1. Identify explicitly what **system assets** are targeted?
2. Use explicit knowledge and previous expertise to characterize potential **vulnerabilities** of the considered system assets
3. Security analyst should impersonate himself as the **threat agent** (motive, capabilities, means, opportunities)
4. **Attack method** should be explicitly stated including its major steps
5. Elicit and state what is the **impact** of the defined risk event
6. Once all components are gathered state what is the risk
Malicious software

https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101/

- Software used to cause **harm** to the computer
  - Compromise computer functions
  - Steal data
  - Bypass access controls
  - …
Malicious software
https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101/

• Symptoms:
  – Increased CPU usage
  – Slow computer or web browser speeds
  – Problems connecting to networks
  – Freezing or crashing
  – Modified or deleted files
  – Appearance of strange files, programs, or desktop icons
  – Programs running, turning off, or reconfiguring themselves
  – Strange computer behavior
  – Emails/messages being sent automatically and without user’s knowledge

Adware  Rootkit
Spyware  Trojan horse
Bot      Virus
Bug      Worm
Ransomware  Spam
Malware types

https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101/

- **Adware**
  - (advertising supported software)
  - automatically delivers advertisements
  - Pop-up ads on Websites
  - Come with spyware
    - to track-user activities
    - to steal information

- **Spyware**
  - spy on user activity without their knowledge
    - activity monitoring
    - collecting keystrokes
    - data harvesting
      - (account information, logins, financial data)

- **Bot**
  - automatically perform specific operations
  - used in botnets – collections of computers to be controlled by third parties
    - DDoS attacks
    - spambots

- **Bug**
  - A flaw that produces an undesired outcome
  - Security bugs are the most severe type of bugs
    - Attackers can
      - bypass user authentication
      - override access privileges
      - steal data
Malware types
https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101/

• Ransomware
  – holds a computer system captive while demanding a ransom
  – restricts user access to the computer
    • encrypting files
    • locking down the system and displaying messages to force the user to pay the malware creator

• Rootkit
  – remotely access or control a computer without being detected
    • remotely execute files
    • access/steal information
    • modify system configurations
    • alter software (especially security software that could detect the rootkit)
    • install concealed malware
    • control the computer as part of a botnet

Malware types
https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101/

• Virus
  – copying itself and spreading to other computers
    • by attaching themselves to various programs, executing code when a user launches those programs
    • through script files, documents, and cross-site scripting vulnerabilities in web apps
  – used to
    • steal information, money
    • harm host computers and networks
    • create botnets
    • render advertisements

• Worm
  – spread over computer networks by exploiting operating system vulnerabilities
  – harm to host networks by consuming bandwidth and overloading web servers
  – Have the ability to self-replicate and spread independently
  – Worms often spread by sending mass emails with infected attachments to users’ contacts
Malware types

- Trojan Horse
  - disguises itself as a normal file or program to trick users into downloading and installing malware
  - can give a malicious party remote access
  - once an attacker has access to an infected computer
    - to steal data
    - install more malware
    - modify files
    - monitor user activity
    - use the computer in botnets
    - ...

- Spam
  - electronic sending of mass unsolicited messages
    - email, instant messages, texting, blogs, web forums, search engines, social media
  - it is very common for malware to spread through spamming
    - when infected computers (with viruses, worms, ...) are used to distribute spam messages containing more malware

Risk Analysis

1. Identify explicitly what system assets are targeted?
2. Use explicit knowledge and previous expertise to characterize potential vulnerabilities of the considered system assets
3. Security analyst should impersonate himself as the threat agent (motive, capabilities, means, opportunities)
4. Attack method should be explicitly stated including its major steps
5. Elicit and state what is the impact of the defined risk event
6. Once all components are gathered state what is the risk
State Risk Explicitly

Security Analysis Techniques

- Secure Tropos
- KAOS extension for security
- Abuse frames
- Misuse cases

- **Attack trees**

Schneier B., Attack Trees: Modeling security threats, Dr. Dobb’s Journal December 1999
ATTACK TREES

BRUCE SCHNEIER

Counterpane Systems
101 East Minnehaha Parkway, Minneapolis, MN 55419
Phone: (612) 823 1098; Fax: (612) 823-1590
schneier@counterpane.com
http://www.counterpane.com

SANS Network Security 99
New Orleans, LA
8 October 1999