CS 6813 – Information, Privacy and Security

Module 2: Threat Modeling
Quick Review

• Threat, Vulnerability, Attack
• Confidentiality, Integrity and Availability
• Security Policy vs. Security Mechanism
• Design Principles
  1. Principle of least privilege
  2. Principle of fail-safe defaults
  3. Principle of economy of mechanism
  4. Principle of complete mediation
  5. Principle of open design
  6. Principle of separation of privilege
  7. Principle of least common mechanism
  8. Principle of psychological acceptability
So far what we have learnt helps us in design, specification and implementation mainly.

What about others?

We start with threat analysis/modeling.
Threats, Vulnerabilities and Attacks

• A *threat* to a system is any potential occurrence, malicious or otherwise, that can have an adverse effect on the assets and resources associated with the system.

• A *vulnerability* of a system is some characteristic that makes it possible for a threat to occur.

• An *attack* on a system is some action that involves exploitation of some vulnerability in order to cause an existing threat to occur.
Risk

• Risk: What (adverse) happens if a threat occurs?
  – Risk can exist when there is a known issue that increases the attack surface. Risk can also exist when there are non-specific issues, unexplored threat areas, or lack of depth-of-knowledge.

• An essential component of Computer security risk analysis and risk management.
Why Threat Modeling

• Helps you understand your application better.
• Discover potential design flaws and vulnerabilities
• Prioritize security analysis
• Understand overall security risk
• Develop mitigating strategies
• Provide more complete analysis
Threat Modeling

- Threats and assets are key – vulnerabilities and attacks are only concerns if there is a threat to an asset to be concerned about.

- How do we identify and evaluate threats?
  - Arbitrary Threat or Attack Lists
    - Random and unstructured
    - Dubious completeness
  - Threat Trees or Attack Trees
    - More structured
    - Modular and Re-usable
    - Currently favored approach
Threat Modeling

• Start with questions like the following:
  – Who are my potential adversaries?
  – What is their motivation, and what are their goals?
  – How much inside information do they have?
  – How much funding do they have?
  – How averse are they to risk?
  – [Be paranoid: do not underestimate the attacker’s capability; do not also ignore easy/dumb attacks]

• Then enumerate threats by stepping through each of the system’s assets, reviewing a list of attack goals for each asset. Assets and threats are closely correlated.
Threat Modeling – main steps

• Understand your system
• Understand what assets/resources need to be protected
• Predict who the potential attackers are against a particular asset and what are the possible (known) attacks
• Perform risk assessment
  – Determine what is the expected risk (quantitative or qualitative) because of an attack
• Perform risk management: Employ security mechanisms (mitigation), if needed
  – Determine if they are cost effective
Module 1: Types of threats

• Can be classified into four broad categories
  – Disclosure - unauthorized access to information
  – Deception - acceptance of false data
  – Disruption - interruption or prevention of correct operation
  – Usurpation - unauthorized control of some part of a system

• Examples include – snooping, sniffing, spoofing, delay, denial of service, theft of computational resources...
STRIDE Model

• In general, threats can be classified into six classes based on their effect:
  • Spoofing - Using someone else’s credentials to gain access to otherwise inaccessible assets.
  • Tampering - Changing data to mount an attack.
  • Repudiation - Occurs when a user denies performing an action, but the target of the action has no way to prove otherwise.
  • Information disclosure - The disclosure of information to a user who does not have permission to see it.
  • Denial of service - Reducing the ability of valid users to access resources.
  • Elevation of privilege - Occurs when an unprivileged user gains privileged status.
Ranking Threats

• Used for prioritizing work
• One methodology for ranking threats is the use of DREAD (used by Microsoft!)
  – Damage Potential
  – Reproducibility
  – Exploitability Cost (or cost and ease of performing attack)
  – Affected Users
  – Discoverability
• DREAD rating is calculated by adding the rating for each component
  – For example, 3: High, 2: Medium, 1: Low
  – For a particular threat, we might have
    • Damage Potential = 3
    • Reproducibility = 3
    • Exploitability Cost (or cost and ease of performing attack) = 2
    • Affected Users = 2
    • Discoverability = 2
    • Total Rating: 12, which might be regarded as High, since one can set 12–15 as High, 8–11 as Medium, and 5–7 as Low risk.
Attack Trees

- Data structure to represent an attack
- Look at system from attackers point of view.

- The root node of the tree is the global goal of the attacker
- Children are refinements of this goal
- Nodes can be conjunctive (AND) or disjunctive (OR)
Notations for nodes

• Can be represented graphically or textually

• Conjunctive (AND) node
  – To achieve G0, you must achieve G1 AND G2 ... AND GN

• Disjunctive (OR) node
  – To achieve G0, you must achieve G1 OR G2 ... OR GN
Attack Trees

- Attack trees consist of any combination of conjunctive and disjunctive nodes.
- Individual intrusion scenarios are created by depth first traversal.

So the tree to the left leads to the attack scenarios:

\(<G_4, G_5, G_2, G_6>\)
\(<G_4, G_5, G_2, G_7>\)
Another Example

• What are the attack scenarios for the tree below?
Yet another...

- What are the attack scenarios for the tree below?
Attack Trees – a funny example
Attributes: Boolean

• You can assign attributes to nodes in the tree to help you reason about them
  – Can be useful in understanding what sorts of attackers can launch certain attacks
• “Possible” and “Impossible” are one way to assign attributes to the tree
An example
Attributes: Boolean

• “Possible” and “Impossible” are only one way to assign attributes to the tree

• Any Boolean value can be assigned to the leaf nodes and then propagated up the tree structure: AND/OR of the children node values
  – Easy vs. hard
  – Expensive vs. Inexpensive
  – Legal vs. Illegal
  – Special Equipment vs. no Special Equipment
Special Equipment

Diagram:

- Open Safe
  - Pick Lock SE
  - Learn Combo
  - Cut Open Safe SE
  - Install Improperly NSE

  - Find Written Combo NSE
  - Get Combo From Target

    - Threten NSE
    - Blackmail NSE
    - Eavesdrop
    - Bribe NSE

    and
    - Listen to Conversation SE
    - Get Target to State Combo NSE

NSE = No special equipment
SE = Special equipment
Attributes: Continuous

- Expensive vs. Inexpensive is fine, but good to say the amount, e.g.
- Continuous values can also be assigned to the nodes of the attack tree, and can be propagated up the tree
  - OR nodes have the value of their cheapest child
  - AND nodes have the value of the sum of their children
Cheapest attack

- Open Safe $10K
  - Pick Lock $30K
  - Learn Combo $20K
  - Cut Open Safe $10K
  - Install Improperly $100K
    - Find Written Combo $75K
    - Get Combo From Target $20K
      - Threaten $60K
      - Blackmail $100K
      - Eavesdrop $60K
      - Bribe $20K

$ = Cost of attack

- Listen to Conversation $20K
- Get Target to State Combo $40K
All attacks with cost < $100K
Combination of attributes: cheapest attack with no special equipment

**Diagram:**

- **Open Safe**
  - NSE/$20K

- **Pick Lock**
  - SE/$30K

- **Learn Combo**
  - NSE/$20K

- **Cut Open Safe**
  - SE/$10K

- **Install Improperly**
  - NSE/$100K

- **Find Written Combo**
  - NSE/$75K

- **Get Combo From Target**
  - NSE/$20K

- **Threaten**
  - NSE/$60K

- **Blackmail**
  - NSE/$100K

- **Eavesdrop**
  - SE/$60K

- **Bribe**
  - NSE/$20K

- **Listen to Conversation**
  - SE/$20K

- **Get Target to State Combo**
  - NSE/$40K

**Abbreviations:**
- NSE = No special equipment
- SE = Special equipment required
- $ = Cost of attack
Case Study – ACME Enterprise
ACME High Level Attack Tree

Survivability Compromise: Disclosure of ACME proprietary secrets

*OR* 1. Physically scavenge discarded items from ACME
   *OR* 1. Inspect dumpster content on-site
   2. Inspect refuse after removal from site
2. Monitor emanations from ACME machines
   *AND* 1. Survey physical perimeter to determine optimal monitoring position
   2. Acquire necessary monitoring equipment
   3. Setup monitoring site
   4. Monitor emanations from site
3. Recruit help of trusted ACME insider
   *OR* 1. Plant spy as trusted insider
   2. Use existing trusted insider
4. Physically access ACME networks or machines
   *OR* 1. Get physical, on-site access to Intranet
   2. Get physical access to external machines
5. Attack ACME intranet using its connections with Internet
   *OR* 1. Monitor communications over Internet for leakage
   2. Get trusted process to send sensitive information to attacker over Internet
   3. Gain privileged access to Web server
6. Attack ACME intranet using its connections with public telephone network (PTN)
   *OR* 1. Monitor communications over PTN for leakage of sensitive information
   2. Gain privileged access to machines on intranet connected via Internet
Expansion of a node

5.3. Gain privileged access to ACME Web server

*AND* 1. Identify ACME domain name
2. Identify ACME firewall IP address

*OR* 1. Interrogate domain name server
2. Scan for firewall identification
3. Trace route through firewall to Web server
3. Determine ACME firewall access control

*OR* 1. Search for specific default listening ports
2. Scan ports broadly for any listening port
4. Identify ACME Web server operating system and type

*OR* 1. Scan OS services’ banners for OS identification
2. Probe TCP/IP stack for OS characteristic information
5. Exploit ACME Web server vulnerabilities

*OR* 1. Access sensitive shared intranet resources directly
2. Access sensitive data from privileged account on Web server
Automated Generation and Analysis of Attack Graphs

Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann and Jeanette M. Wing

http://www.cs.cmu.edu/~scenariograph/sheyner-wing02.pdf
Key Ideas

• Upside-down: Goals are on the bottom
• Attack Model – A graph that represents all interesting state transitions
  – Node – a particular network state
  – Edge – a particular attack (exploit)
• Attack Graph – A subgraph of the Attack Model where the goal is a leaf-node
• Automatically Generated
  – Network topology
  – Exploit (attack) information
• Graph algorithms
Sample Network
Figure 4. Attack Graph

<table>
<thead>
<tr>
<th>no.</th>
<th>attack</th>
<th>host</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>sshd buffer overflow</td>
<td>$ip_a$</td>
</tr>
<tr>
<td>1</td>
<td>ftp .rhosts</td>
<td>$ip_1$</td>
</tr>
<tr>
<td>2</td>
<td>remote login</td>
<td>$ip_2$</td>
</tr>
<tr>
<td>3</td>
<td>local buffer overflow</td>
<td></td>
</tr>
</tbody>
</table>
Risk Assessment and Management
General Concept of Risk Assessment and Management

• A risk consists of something of value (an “asset” at risk) which may lose value if a negative event occurs.
  – Example: a car and its passengers are at risk in the event of an auto accident. Other people, cars, and roadside objects are also at risk
  – Example: Money invested in a stock is at risk in the event that the price of the stock goes down and the owner has to sell

• Risk analysis/assessment is the process of
  – Identifying the assets at risk (cost of asset – cost of most expensive attack)
  – Putting quantitative (e.g., dollars) or qualitative (e.g. low/medium/high) measures on the potential loss (impact)
  – Putting quantitative (i.e., the probability) or qualitative (e.g. low/medium/high) measures on the likelihood of the event happening

• Risk Management is a process for planning on how to control those risks
Non-IT Example 1: Driving risk

- Assets at risk: people’s lives and health, the automobile, other property
- Negative event: auto accident
- Risk Management:
  - Risk reduction: Following DWI laws, defensive driving techniques, ABS, driving slow or just not driving on snowy days
  - Risk mitigation: Seat belts, air bags, “crumple zones” in auto design
  - Risk transfer: insurance
  - Risk acceptance: residual risk of injury, deductible on insurance
Non-IT Example 2: Stock Market Risk (simplified)

• Assume you buy 100 shares of stock at $50 per share. Potential maximum impact: $5000

• Risk management strategies:
  – Risk reduction: buy a conservative stock
  – Risk mitigation: buy a “contrary” stock (Buy Dell in addition to HP, in case HP loses significant market share to Dell)
  – Risk transfer: buy an option to sell at $40/share; reduces maximum impact to $1000 (this could also be thought of as a risk mitigation strategy)
  – Risk acceptance: If you buy the options, you accept $1000 of risk
Risk analysis starts with understanding what assets are potentially at risk, what the threats are. This forms the basis for finding the “sweet spot” of putting in enough security to protect the value of the assets.
Information Security Risk Analysis

• “Risk” will usually refer to information security risk
• Negative events are often compromises of the system.
• If we are only concerned with information security risks, any asset at risk will have to be mapped back to an IT asset at risk
• “IT assets” refer to information, IT processes/functionality, and IT systems
• The risk management strategies that we consider are for the IT assets, but the impact is based on the real assets
Example 1

- Example: Given a system that uses personal information such as name, SSN, etc. The related IT asset at risk is the _________ of that information. The impact of a compromise is the potential for _________. 
Example 1

• Example: Given a system that uses personal information such as name, SSN, etc. The related IT asset at risk is the confidentiality of that information. The impact of a compromise is the potential for identity theft.
Example 2

• Example: Given a battlefield communications system. The related IT asset is the _________ of the system, and the impact of a failure is _________.

...
Example 2

- Example: Given a battlefield communications system. The related IT asset is the availability and integrity of the system, and the impact of a failure is loss of life.
“Asset at Risk” Owner vs. “IT Asset at Risk” Owner

• The owner of the asset may not be the owner of the related IT asset at risk
  – Example: an “identity” that may be stolen is an asset of that person, but the related IT asset (SSN, etc.) is under the control of many other entities.
  – Example: a civilian undercover agent (spy) transmits information to which only he has access back to a military organization. If that military organization’s system is compromised, the agent’s life may be at risk
“Asset at Risk” Owner vs. “IT Asset at Risk” Owner

• The owner of the IT system may not suffer the impact of a compromise.
  – Example: in 2005, CardSystems (a processor of credit card transactions) system was compromised and 40 million cardholders’ information was exposed. The potential impact of each compromise was on the credit card holders (fraud, identity theft) and the credit card companies (which cover all fraudulent transactions above $50 per account by law). As a result, both Visa and American Express stopped allowing CardSystems to process their transactions.
  – Such secondary impacts and “business risks” are an important part of the risk analysis.

• Laws may also help share risk
• Business relationships and corporate/political image
Risk Assessment

• Assessment: measures of the impact of an event, and the probability of an event (threat agent exploiting a vulnerability)
• Quantitative (objective) and Qualitative (subjective) approaches both used.
• Quantitative approach:
  – Compute expected monetary value (impact) of loss for all “events”
  – Compute the probability of each type of expected loss
• Qualitative approach: use Low, Medium, High; ratings; other categorical scales
Risk Management

• Once you have risk computed for each threat you can prioritize them and for each do one of the following:
  – Accept the risk - The risk is so low or so costly to mitigate that it is worth accepting.
  – Transfer the risk - Transfer the risk to somebody else via insurance, warnings etc.
  – Remove the risk - Remove the system component or feature associated with the risk if the feature is not worth the risk.
  – Mitigate the risk - Reduce the risk with countermeasures.

• The understanding of risks leads to policies, specifications and requirements.

• Appropriate security mechanisms are then developed and implemented, and then deployed
Quantitative Methodology (terminology)

- SLE: Single Loss Expectancy
- ARO: Annualized Rate of Occurrence
- ALE: Annualized Loss Expectancy
- S: Safeguard (security mechanism)
- ALE(without S)
- ALE(with S)
- ACS(S): Annualized Cost of Safeguard S
- ANB(S): Annualized Net Benefit of S
  \[ ANB(S) = ALE\text{(without S)} - ALE\text{(with S)} - ACS(S) \]
- S is cost effective if \( ANB(S) > 0 \)
Quantitative Methodology: Example 1

• Suppose due to a software flaw, a company’s web site sometimes leave company credit card names and numbers exposed. Each year, an average of 25 exposed numbers are exploited for credit card fraud with an average loss of $1000. A software update to correct the flaw will cost $45,000 to develop, test, and deploy, plus $5,000 per year in additional maintenance costs. The software would be used for 3 years before a planned system upgrade will replace all the software.
  – SLE = $1000
  – ARO = 25
  – ALE = $25,000
  – ACS - ($45,000/3) + $5,000 = $20,000
  – ANB = $25,000 - 0 - $20,000

• The software update is cost effective, and should be done.
• If the update costs more that $60,000, then is is not cost effective and the upgrade should not be done.
Quantitative Methodology: Example 2

• A large e-tailer earn $1 M per day on web sales from a distributed set of servers. A DDOS attack could potentially put them off line for a day, with the lost business going to competitors. The CSO estimates the probability of a successful attack over the course of a year is 10%. A new kind of adaptive firewall will block most DDOS attacks, and reduce the probability of a successful attack to 1%. Deploying the firewall at all the server sites will cost $200,000, with an expected useful life of 4 years. Annual maintenance costs are $30,000 per year, including upgrades and maintenance from the firewall supplier and management by the IT department.
Quantitative Methodology: Example 2

- A large e-tailer earn $1 M per day on web sales from a distributed set of servers. A DDOS attack could potentially put them off line for a day, with the lost business going to competitors. The CSO estimates the probability of a successful attack over the course of a year is 10%. A new kind of adaptive firewall will block most DDOS attacks, and reduce the probability of a successful attack to 1%. Deploying the firewall at all the server sites will cost $200,000, with an expected useful life of 4 years. Annual maintenance costs are $30,000 per year, including upgrades and maintenance from the firewall supplier and management by the IT department.
  - SLE = $1,000,000
  - ARO(without S) = .1
  - ARO(with S) = .01
  - ALE(without S) = $100,000
  - ALE(with S) = $10,000
  - ACS - ($200,000/4) + $30,000 = $80,000
  - ANB = $100,000 - $10,000 - $80,000 = $10,000
- The adaptive firewall is cost effective and should be deployed
- If the firewall only reduced the ARO to 2%, it would be break even
- If the firewall only reduced the ARO to 3%, it would not be cost effective
Quantitative: Useful or Not?

• **Pro:**
  – Objective, independent process
  – Solid basis for cost/benefit analysis of safeguards
  – Credibility for audit, management (especially corporate management)
  – This type of approach is useful for many kinds of reliability related design questions (e.g., redundant servers, etc.), where threats and likelihood of “events” can be accurately modeled statistically
  – Quantitative risk assessment is the basis for insurance, risk managed portfolios, etc.

• **Con**
  – In most cases, it is difficult to enumerate all types of events and get meaningful data on probability and impact
  – Very time consuming, costly to do right
  – Many unknowns may give a false sense of control
  – Not reliable for “rare” events or “unthinkable” impacts
Qualitative Approach

• Establish classes of loss values (“impact”), such as
  – Low, medium, high
  – Under $10K, between $10K and $1M, over $1M (used by at least one company)
  – Type of loss (e.g. compromise of credit card #, compromise of SSN, compromise of highly personal data)
  – Minor injury, significant injuries, loss of life, large scale loss of life (used by emergency response organizations to categorize non-IT events)
  – Rank ordering
Qualitative Approach

• DoD classified information:
  – CONFIDENTIAL “shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security”
  – SECRET “shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security”
  – TOP SECRET “shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security”
Qualitative Approach (continued)

• Establish classes of likelihood of compromise
  – Low, medium, high likelihood

• Decide on a risk management approach to each combination of (class of loss, likelihood of loss)

• Focus effort on medium to high loss and/or medium to high likelihood items
Threat Modeling Summary

- Enumerate assets
- Determine the threats to the system
- Perform risk assessment
- Perform risk management
  - If needed, perform risk mitigation by developing cost-effective security mechanisms
Be Realistic About Threats...

A Crypto Nerd's Imagination:

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

What Would Actually Happen:

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.

[*] comic from xkcd
... And Be Realistic About Attacks!

[*] comic from xkcd
Reading Next Week

• Read: Threat Modeling as a Basis for Security Requirements
• Read "Attack Trees" by Bruce Schneier

• Think:
  • How might you get a copy of a 'do-not-duplicate' key?

• Read:

• Purpose: Think about threat modeling!