Lecture 7: Threat Modeling

CS 392/6813: Computer Security
Fall 2007

Polytechnic UNIVERSITY

Nitesh Saxena

*Adopted from a previous lecture by Nasir Memon

---

Course Admin

- HW 1 to 5 are graded; solutions provided
- HW6 being graded
  - Solution will be posted soon
- HW7 due next Wednesday midnight
Recall the Security Life Cycle

- Threats
- Policy
- Specification
- Design
- Implementation
- Operation and Maintenance

So far what we have learnt helps us in specification and design 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: The chance of something going wrong.
  - 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.

*Computer security can be viewed as process of risk analysis and management.*

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 – For example by brainstorming process done with experts
    - Random and unstructured
    - Dubious completeness
  - Threat Trees or Attack Trees
    - More structured
    - Currently favored approach
**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**

- 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?
- 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

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 averaging the number of each property and dividing by 5

### Attack Trees

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

- Can be represented graphically or textually
- Conjunctive (AND) node
  
  **Graphical:**
  
  ![Graphical Conjunctive Node]
  
  **Textual:** Goal $G_0$
  
  \[
  \text{AND } G_1 \\
  G_2 \\
  \ldots \\
  G_n
  \]

- Disjunctive (OR) node
  
  **Graphical:**
  
  ![Graphical Disjunctive Node]
  
  **Textual:** Goal $G_0$
  
  \[
  \text{OR } G_1 \\
  G_2 \\
  \ldots \\
  G_n
  \]

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 intrusion scenarios:

\[
< G_3, G_5, G_6 > \\
< G_4, G_5, G_6 >
\]
Another Example

- What are the intrusion scenarios for the tree below?

Attack Trees – a funny example

- An attack tree is a tree in which nodes represent attacks.
  - 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)
### Attack Forest

- A system typically has a set, or forest, of attack trees that are relevant to its operation. The root of each tree in a forest represents an event that could significantly harm the system's mission. Each attack tree enumerates and elaborates the ways that an attacker could cause the event to occur. Each path through an attack tree represents a unique intrusion.

### 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** 2. Inspect dumpster contents on-site

2. Inspect refuse after removal from site

2. Monitor emigrations from ACME machines

**AND** 1. Survey physical perimeter to determine optimal monitoring position

2. Acquire necessary monitoring equipment

3. Setup monitoring site

4. Monitor emigrations 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
**Attack Patterns**

**Access Control Discovery Attack Pattern:**
- **Goal:** Identify firewall access controls
- **Precondition:** Attacker knows firewall IP address
- **Attack:**
  1. Search for specific default listening ports
  2. Scan ports broadly for any listening ports
  3. Scan ports stealthily for listening ports
- **Postcondition:** Attacker knows firewall access controls

**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
Information Security Risk Concept

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 for to protect the value of the assets.

Information Security Risk Analysis

- For the rest of this course “risk” will usually refer to information security risk.
- By restricting the domain to information security, we can be more specific about the kinds of negative events that put assets at risk. Negative events are often called compromises of the system.
- Since we are only concerned with information security risks, any asset at risk will have to be mapped back to an IT asset at risk.
  - Example: in a system that uses personal information such as name, SSN, etc., “identity theft” is a risk. The related IT asset at risk is the confidentiality of that information. The impact of a compromise is the potential for identity theft.
  - Example: in a battlefield communications system, human lives are at risk if the system cannot be used to call in support. The related IT asset is the availability of the system, and the impact of a failure is potential for loss of life.
- “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.
"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
- If the owner of the IT system does not suffer the impact of a compromise, what is the motivation to pay for the needed controls for proper risk management?
- Business relationships and corporate/political image can create serious impacts for the IT asset owner if there is 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
- Many laws and government policies to be discussed later are effective methods to create impacts that the IT system owners have to include in their risk analysis and risk management

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.

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

S is cost effective if ANB(S) > 0
Quantitative Methodology: Example 1

Suppose due to a software flaw, a company's web site sometimes leaves 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 it 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.

- 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

- 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

1. Enumerate assets
2. Determine the threats to the system
3. Perform risk assessment
4. Perform risk management
5. Perform risk mitigation by developing cost-effective security mechanisms
- Why do people always say that installing a security mechanism is an overhead
- Because they anticipate the loss due to an attack to be ZERO!!!
  - \( ANB(S) = 0 - ACS(S) \)
- We studied that security mechanism is installed only if it is cost effective

In Class Exercise
- Let us build an attack tree for the Secure Flight System:
Secure Flight

- Collection of information by the airlines. Reportedly considering requiring passengers to provide their dates of birth.
- Authentication check. TSA will send passengers’ names and dates of birth (or whatever other information is collected) to commercial data services - companies like Choicepoint or Axiom that will report back to the TSA whether the information provided by the passenger via the airline matches the information in the company’s own records.
- Watch list check. TSA runs passenger through watch lists maintained by the government’s Terrorist Screening Center (TSC), which is supposed to aggregate the many scattered terrorist watch lists that the government was discovered to be holding after 9/11.
- Action at the gate. Security personnel at the airport would be notified if system determines that a passenger is on watch list.

In Class Exercise

- Let us build an attack tree for the following application
Further Reading

- Threat Modeling as a Basis for Security Requirements
- “Attack Modeling for Information Security and Survivability” by Andrew P. Moore, Robert J. Ellison, Richard C. Linger
- Attack Trees by Bruce Schneier.