Recall the Security Life Cycle

So far what we have learnt helps us in design, specification and implementation mainly.

What about others?

Let us focus on 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 the 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
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.

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

\[ \text{Graphical:} \quad G_3 \quad \text{Textual:} \quad \text{Goal } G_0 \quad \text{AND} \quad G_1 \quad G_2 \quad \ldots \quad G_n \]

- Disjunctive (OR) node

\[ \text{Graphical:} \quad G_3 \quad \text{Textual:} \quad \text{Goal } G_0 \quad \text{OR} \quad G_1 \quad G_2 \quad \ldots \quad G_n \]

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

• What are the attack scenarios for the tree below?

Attack Trees – a funny example
A simple example

Possible attacks?
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

- Open Safe
- Pick Lock SE
- Learn Combo
- Cut Open Safe SE
- Install Improperly NSE
- Find Written Combo NSE
- Get Combo From Target
- Threaten NSE
- Blackmail NSE
- Eavesdrop NSE
- Bribe NSE

HFE = no special equipment
SE = Special equipment

Lecture 7 - Threat Modeling
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
  \[\text{Pick Lock $30K} \quad \text{Learn Combo $20K} \quad \text{Cut Open Safe $10K} \quad \text{Install Improperly $100K}\]
  \[\text{Find Written Combo $75K} \quad \text{Get Combo From Target $20K}\]
  \[\text{Threaten $50K} \quad \text{Blackmail $100K} \quad \text{Eavesdrop $75K} \quad \text{Brick $20K}\]
```

$ = Cost of Attack

Listen to Conversation $25K
Get Target to State Combo $10K
All attacks with cost < $100K

Combination of attributes: cheapest attack with no special equipment
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 = ALE(without S) – ALE(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, each 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.
  - 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"

Lecture 7 - Threat Modeling

Qualitative Approach: DREAD Model

- Used for prioritizing work
- One methodology for ranking threats is the use of DREAD (used by Microsoft!)
  - Damage Potential
  - Reproducibility
  - Exploitability (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 (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.
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
   1. Use attack trees to document these threats
3. Perform risk assessment
4. Perform risk management
   1. If needed, 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

A Case Study

• Password Authentication
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.