Silverfish - Red Team Exercise

Nancy Mead, Sam Perl, **Forrest Shull**

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0485

Threat Modeling Process with Timing

#	Process (based on SEI hTMM)	Time budget
1	Iterative brainstorming of potential set of attacks of concern, based upon: • Analysis of system models and engineering decisions. For each attack, record assets (system components) affected. • "Adversary method" taxonomy (see later slide)	90 Min
2	For each attack, identify adversary(ies) and skillsets (i.e., "personas") required to execute. • Exclude attacks based on infeasible skill reqts • Exclude attacks based on mitigating measures (e.g. denial of access to physical system)	60 min
3	For each remaining attack, develop high-level misuse case.	45 min
4	For each remaining attack, document and conduct risk assessment (characterize consequence and likelihood).	45 min
5	Flesh out requirements / design for needed mitigations	(outside of red team)

Outcome Template

ID	Intended Effect	Attack Profile	Attack Method	Attack Architecture	Cost (time, test, difficulty, monetary)	Mitigation Potential

- Intended effect
  - What consequences are the attackers seeking? E.g. gain control of weapons, deny use of weapons
- Attack Profile
  - Potential way to achieve the intended effect e.g. code injection, delay data transfer, data element change.
- Attack Method
  - Supply Chain, Insider, Network, Reuse of existing attack
- Attack Architecture/ATT&CK

  Does this attack consist of a sequence of attacks to achieve an outcome, if so what are they?
- Cost
  - The cost in terms of time, testing needed for the attack, the difficulty of the attack, and any monetary costs
- Mitigation Potential
  - How easy would it be for the defenders to make this attack too difficult, impossible, etc.?

Process mapping to outcome template

#	Process (based on SEI hTMM)	Mapping to Outcome
1	Brainstorming potential set of attacks …	• Intended Affect • Attack Profile • Attack Method
2	Identify persona(s)…	• Cost • Mitigation Potential • Attack Method
3	Develop misuse cases...	• Attack Architecture
4	Conduct risk assessment (consequence and likelihood)…	• Cost • Mitigation Potential

Job Aid – Step 1
Adversary Methods Categories

As an aid to brainstorming, consider threats to: Networks, applications, and facilities.

From: **The Security Cards: A Security Threat Brainstorming Toolkit.** T. Denning, B. Friedman, and T. Kohno. 2013. http://securitycards.cs.washington.edu/

Types of threats: How might the adversary…

- **Technological Attack**
  …perform technical attacks over an analog or digital link?
- **Multi-phase Attack**
  …leverage multiple attack phases on a single or multiple targets in order to execute more complicated or covert attacks?
- **Physical Attack**
  …gain or take advantage of physical access to a system component?
- **(Exploitation of) Processes**
  …take advantage of technical or bureaucratic processes to perform an attack?
- **Indirect Attack**
  …use an unexpected or overlooked system property in order to bypass your system's direct defenses?
- **Manipulation or Coercion**
  …manipulate or coerce people into divulging information or performing actions that affect your system's security?
- **Attack Cover-up**
  …alter awareness, understanding, or evidence surrounding an attack?

Job Aid – Step 2
"Persona non Grata" Template

The point of the template is to think through types of attackers, what they are aiming to achieve and whether they have the requisite skills – to inform likelihood of attacks.

Descriptor

- Description of the role / type of attacker

Goals

- Consequences being sought – Needs to be plausible for the identified type of attacker

Skills

- Cyber-attack skills available to this persona. E.g., consider:
  - Level of proficiency required
  - Number of attack personnel required
  - Physical access to system required
  - Time required for attack
- Need to achieve the goals identified

Job Aid – Step 3
Example Misuse Cases

Marvin's Misuse Cases which Threaten Correct Operation of the ICD	
1.	Snoop on the data transmitted along the serial cable between the ICDs reprogramming equipment and communication device in order to retrieve the patient's name, ID, and basic medical history which is all stored in the ICD.
2.	Transmit commands to replace the patient's personal information in the ICD.
3.	Transmit commands to shut off the device's ability to respond to cardiac events
4.	Transmit commands to switch to test mode so that a carefully-timed current triggers an arrhythmic test event which could stop the heart entirely.

Examples from Implantable Cardioverter Defibrillator (ICD).

Note:

- Need not be extensive / detailed at this stage
- Do need to capture enough information to convey the attack and hint at components / interfaces affected.
- More detailed misuse cases will be needed later – but we just want to sketch them in our red teaming time.

Job Aid – Step 4
Prioritization Schemes

Select 1 or 2 scales that fit well with current thinking:

Cost Likert Scale

1. Attack is not difficult to implement, nor does it require much overhead
2. Attack is not difficult to implement, but requires some testing or time before implementation
3. Attack is moderately difficult and/or requires testing/time before implementation
4. Attack is very difficult to implement and requires significant overhead

Mitigation Likert Scale

1. Securing against this attack would require significant prevention or resiliency measures to be implemented in the system
2. Some defense or resiliency measures would make this attack significantly more difficult to implement
3. Simple defense or resiliency measures would eliminate this attack as a viable option

Questions?