Lesson Title:
Threat Modeling

Copyright © 2008 by Dale R. Thompson {d.r.thompson@ieee.org}

Dale R. Thompson
Computer Science and Computer Engineering Dept.

University of Arkansas

This material is based upon work supported by the National Science Foundation under Grant No. DUE-0736741.
Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation (NSF).

http://rfidsecurity.uark.edu
Terminology

- **Threat** – It is a potential event that causes damage.
- **Threat modeling** – It is a security analysis to determine the most important security risks to a system. The goal is to reduce the risk to an acceptable level by determining threats to mitigate and the steps to mitigate the identified threats.
- **Vulnerability** – It is a weakness in the system.
- **Attack** – This is when an attacker takes advantage of vulnerability.
- **Asset** – It is something of value and in threat modeling is called a threat target.
- **Threat target** – It is an asset.

http://rfidsecurity.uark.edu
Three components of security

- Assets
- Vulnerabilities
- Attackers
Assemble Team

• Design, sales, marketing, manufacturing, etc.
• Led by someone with security background

http://rfidsecurity.uark.edu
Threat Modeling Process

• Decompose the system
  – High-level context diagram
  – High-level physical view
  – List components

• Determine the threats to the system
  – Apply STRIDE
  – Create threat tree for each threat target

• Determine risk for each threat tree
  – Apply DREAD

• Rank threats by decreasing risk

• Mitigation
  – Choose whether to respond to threat
  – Choose technique to mitigate threat
  – Choose appropriate technologies
Threat Modeling a Robotic Dog

• System: Robotic dog that roams the house, can bark, avoid obstacles, investigates sound, walks, sees visible and infrared, and can be controlled over the Internet.

http://rfidsecurity.uark.edu
Data flow diagram

A process transforms or manipulates data (verbs and nouns)

Multiple processes

A data store is a location for storing temporary or permanent data (nouns)

Boundary such as machine, physical, address space, ...

Interactor - input to system

Data flow - data flows to or from data stores, processes, or interactors

http://rfidsecurity.uark.edu
High-level context diagram
Next-level context diagram

[Diagram of a flowchart showing interactions between User, Service A/V, Retrieve History, Authentication Data, Enforce Policy, and Gather A/V with feedback loops and data updates.]
High-level physical view

http://rfidsecurity.uark.edu
List components (threat targets = assets)

- User
- Web browser
- User computer
- Internet
- Network equipment
- Robotic dog
- Administrator
STRIDE* threat categories

• Spoofing identity
• Tampering with data
• Repudiation
• Information disclosure
• Denial of service
• Elevation of privilege


http://rfidsecurity.uark.edu
Apply STRIDE Threat Model to Robotic Dog

<table>
<thead>
<tr>
<th>STRIDE Category</th>
<th>Threat target(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing identity</td>
<td>User, admin</td>
</tr>
<tr>
<td>Tampering with data</td>
<td>Internet, wireless network</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Admin, User</td>
</tr>
<tr>
<td>Information disclosure</td>
<td>Internet, wireless, dog</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Internet, wireless, dog, browser</td>
</tr>
<tr>
<td>Elevation of privilege</td>
<td>User, Admin</td>
</tr>
</tbody>
</table>
Threat Tree

Threat #1
View A/V on Internet

1.1 Data is unprotected

1.2 Attacker views traffic

1.2.1 Attacker compromises web browser
1.2.2 Attacker compromises computer
1.2.3 Attacker sniffs Internet traffic
1.2.4 Attacker sniffs wireless network

http://rfidsecurity.uark.edu
Assign Risk with DREAD*

- **Damage potential (1-10)** – Measure of damage
- **Reproducibility (1-10)** – Measure of how easy it is to work
- **Exploitability (1-10)** – Measure of effort and expertise required
- **Affected Users (1-10)** – Measure of percentage of affected users
- **Discoverability (1-10)** – Measure of how easy it is to find

- \( R_{\text{DREAD}} = \text{average score} \)


http://rfidsecurity.uark.edu
Rank threats by decreasing risk
Mitigation

• Choose whether to respond to threat
• Choose technique to mitigate threat
• Choose appropriate technologies
## Mitigation Techniques

<table>
<thead>
<tr>
<th>Category</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing identity</td>
<td>Appropriate authentication, Protect secrets, Don’t store secrets</td>
</tr>
<tr>
<td>Tampering with data</td>
<td>Appropriate authentication, Hashes, Message authentication codes, Digital signatures, Tamper-resistant protocols</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Digital signatures, Timestamps, Audit trails</td>
</tr>
<tr>
<td>Information disclosure</td>
<td>Authorization, Privacy-enhanced protocols, Encryption, Protect secrets, Don’t store secrets</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Appropriate authentication, Appropriate authorization, Filtering, Throttling, Quality of Service</td>
</tr>
<tr>
<td>Elevation of privilege</td>
<td>Run with least privilege</td>
</tr>
</tbody>
</table>
Choose appropriate technologies

• DES, AES, XOR?
Threat Modeling Process

• Decompose the system
  – High-level context diagram
  – High-level physical view
  – List components
• Determine the threats to the system
  – Apply STRIDE
  – Create threat tree for each threat target
• Determine risk for each threat tree
  – Apply DREAD
• Rank threats by decreasing risk
• Mitigation
  – Choose whether to respond to threat
  – Choose technique to mitigate threat
  – Choose appropriate technologies
Contact Information

Dale R. Thompson, Ph.D., P.E.
Associate Professor
Computer Science and Computer Engineering Dept.
JBHT – CSCE 504
1 University of Arkansas
Fayetteville, Arkansas 72701-1201

Phone: +1 (479) 575-5090
FAX: +1 (479) 575-5339
E-mail: d.r.thompson@ieee.org
WWW: http://comp.uark.edu/~drt/
Copyright Notice, Acknowledgment, and Liability Release

• Copyright Notice
  – This material is Copyright © 2008 by Dale R. Thompson. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or incorporated in commercial documents without the written permission of the copyright holder.

• Acknowledgment
  – These materials were developed through a grant from the National Science Foundation at the University of Arkansas. Any opinions, findings, and recommendations or conclusions expressed in these materials are those of the author(s) and do not necessarily reflect those of the National Science Foundation or the University of Arkansas.

• Liability Release
  – The curriculum activities and lessons have been designed to be safe and engaging learning experiences and have been field-tested with university students. However, due to the numerous variables that exist, the author(s) does not assume any liability for the use of this product. These curriculum activities and lessons are provided as is without any express or implied warranty. The user is responsible and liable for following all stated and generally accepted safety guidelines and practices.

http://rfidsecurity.uark.edu