Rapid Threat Modeling Techniques

Chad Childers
IT Security
Ford Motor Company
Agenda

- Threat Modeling background
- Lessons Learned to make threat modeling faster
- Techniques specifically for DFD and STRIDE effectiveness
- Issues
- Customizations & other security analysis tools
- Success!
What is Threat Modeling?

- Design practice from the Software Assurance Forum (SAFECode)
- Attack trees
- Threat library (CAPEC, OWASP Top Ten)
- Use Cases
- STRIDE
  - Spoofing
  - Tampering
  - Repudiation
  - Information Disclosure
  - Denial of Service
  - Elevation of Privilege
What is Threat Modeling?

- Microsoft Security Development Lifecycle - Threat Modeling tool
- Architectural model based on Data Flow Diagram
- Each element of the diagram generates a set of STRIDE threats
## STRIDE by elements

<table>
<thead>
<tr>
<th>Threats</th>
<th>Data Flows</th>
<th>Data Stores</th>
<th>Processes</th>
<th>Interactors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spoofing</strong></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Tampering</strong></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Repudiation</strong></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Information Disclosure</strong></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Denial of Service</strong></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Elevation of Privilege</strong></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Why Rapid Threat Modeling?

Professional benefits
- Security skill in demand
- Architects make issues surface, clarify design issues
- Developers can avoid rework, prioritize

Deliver Results
- Teams can see value quickly, understand vulnerabilities
- Answer “What do I do now?”
Security hurdles

- Controls documentation
- Paperwork exercise
- Last minute gate review
- Athletes have the right training
- They prepare and practice
- They are not surprised
Who should use Threat Modeling tools

- Facilitated by security experts
  - Provide mitigation advice and consulting
  - Guide team
    - Mindset “What is the worst that can happen?”
    - Keep on-track and fast paced
- Self-Service
  - Security knowledge prefilled within tool can provide guidance
  - Can be updated immediately if design or controls changed
Set yourself up for success

- Session Duration: 90 minutes ± 30
- Cadence: 2 sessions a week
- Web sessions save time, projector bulbs, more productive
- Group size
  - Architect – who can answer design and controls questions
  - SME – who can answer business impact questions
  - Split up sessions per SME to save valuable time
  - Too many cooks…
What to Threat Model?

- High risk (Confidentiality/Integrity, external facing, reputational, compliance…)
- Complex interactions between systems, emergent properties
- Data or control transfer across a boundary
- New technology/architecture to your company
- Architect has trouble thinking through potential issues
What not to Threat Model?

- A repeat implementation using all standard controls
- No significant revisions to application or data
- You already have a fully documented Control Review and all the questions fit well
…make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation…

- Einstein

Threat Modeling Is Like Playing A Violin

- Shostack
Data Flow Diagram elements

External Application

Application

User

Admin

Data Store

Application out of scope
### Generate STRIDE Threats - Analyze Model

<table>
<thead>
<tr>
<th>Threat:</th>
<th>Data Flow Sniffing</th>
<th>Category:</th>
<th>Information Disclosure</th>
<th>Mitigated</th>
</tr>
</thead>
</table>

**Description**

PII Data in transit exposed. Default text appears here and can be customized so it makes sense to your users

**Justification for threat state change**

- **Description/Impact** - What’s the worst that can happen if this Threat is manifested? (or certify that it is not a threat)
- **Review common impacts to help customize default Description**
<table>
<thead>
<tr>
<th>Threat:</th>
<th>Data Flow Sniffing</th>
<th>Category:</th>
<th>Information Disclosure</th>
<th>Mitigated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>PII Data in transit exposed</td>
<td>Justification for threat state change</td>
<td>TLS encrypted</td>
<td></td>
</tr>
</tbody>
</table>

- Solution/Justification for state change - What Mitigations or Controls do we have in place or plan to put in place as a solution?
- Common mitigations may help customize controls elements
When you find an issue that needs investigation, do provide security consulting, but don’t stop, add it to the issues list and move on.

<table>
<thead>
<tr>
<th>Threat:</th>
<th>Insufficient Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category:</td>
<td>Repudiation</td>
</tr>
<tr>
<td>Needs investigation</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Justification for threat state change</td>
</tr>
<tr>
<td>Does the log capture enough data to understand what happened and what the source of the change was?</td>
<td>Need to determine strategy to assure that logs provide traceability</td>
</tr>
<tr>
<td>Threat:</td>
<td>Insufficient Auditing</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Does the log capture enough data to understand what happened and what the source of the change was?</td>
</tr>
</tbody>
</table>

- When you find an issue that needs investigation, do provide security consulting, but don’t stop, add it to the issues list and move on.
When you find an issue that needs investigation, do provide security consulting, but don’t stop, add it to the issues list and move on.
Capture an Issues List

- Paste actions/controls gaps into a spreadsheet or immediately enter in backlog, test tool, or project management tool
- A-ha moments: “oh, we never thought of that!”
- Critical controls that are not already documented anywhere else
- The mitigation sounds like a reason we can’t figure out how to mitigate
- Nonstandard controls that need to be tested
## Sample Issues

<table>
<thead>
<tr>
<th>Threat model Issue</th>
<th>Approach/Plan to Address</th>
<th>Priority</th>
<th>Status</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine strategy to assure that logs provide traceability</td>
<td>Interface team has item in their backlog, test plan to be developed</td>
<td>Medium</td>
<td>Mitigated</td>
<td>Judy</td>
</tr>
<tr>
<td>Make sure that any PII or Secret data is encrypted before drop off or transfer</td>
<td>Encryption in place, key transfer out of band</td>
<td>High</td>
<td>Mitigated</td>
<td>Chad</td>
</tr>
<tr>
<td>How are we going to manage customer data, who owns CRM interface?</td>
<td></td>
<td>High</td>
<td></td>
<td>Lou</td>
</tr>
<tr>
<td>Host based IDS rules turn off unused ports/protocols?</td>
<td></td>
<td>Medium</td>
<td></td>
<td>Chris</td>
</tr>
</tbody>
</table>
Generate STRIDE Threats - Analyze Model

- Don’t waste time assessing threat priority by committee
- Priority may have value for Needs Investigation issues
- Priority may have value if you use it to reduce workload
Security unit test – regression test

- Develop from Threat Model issues list
  - *Example*: verify that all changes from any source are logged
- Work with QC to develop test cases for nonfunctional requirements
- Run at each iteration before release
- Run annually to validate controls
Common Controls
- Example: Guide to Interoperability

**Table 2.2 CI capability for Core Interoperability Transport Protocols**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>C</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>HTTPS</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>FTP</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>FTPS</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>SFTP</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>OFTP1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>OFTP2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>SMTP</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Table 2.3 CIA Capability for Basic Interoperability Security Tech**

<table>
<thead>
<tr>
<th>Tech</th>
<th>C</th>
<th>I</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypt/FMCCrypt [a]</td>
<td>3</td>
<td>2</td>
<td>N/A</td>
</tr>
<tr>
<td>DS</td>
<td>N/A</td>
<td>3</td>
<td>N/A</td>
</tr>
<tr>
<td>HA</td>
<td>N/A</td>
<td>N/A</td>
<td>3</td>
</tr>
<tr>
<td>SSL/MOSSL</td>
<td>3</td>
<td>2</td>
<td>N/A</td>
</tr>
<tr>
<td>SSH</td>
<td>3</td>
<td>2</td>
<td>N/A</td>
</tr>
<tr>
<td>Secure VPN</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>IC</td>
<td>N/A</td>
<td>2</td>
<td>N/A</td>
</tr>
<tr>
<td>WSL</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

[a]: Can support I=2 only data in transport with message integrity check
# Common Controls - Customize

<table>
<thead>
<tr>
<th>THREATS</th>
<th>MODEL ELEMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Flows</td>
</tr>
<tr>
<td>Spoofing</td>
<td>N/A</td>
</tr>
<tr>
<td>Tampering</td>
<td>SSL TLS</td>
</tr>
<tr>
<td>Repudiation</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Turn on table level logs</td>
</tr>
<tr>
<td>Information</td>
<td>SSL TLS</td>
</tr>
<tr>
<td>Disclosure</td>
<td></td>
</tr>
<tr>
<td>Denial of Service</td>
<td>CDN ANX</td>
</tr>
<tr>
<td>Elevation of Privilege</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Common Controls - Customize

- Add your standard controls to StandardElementCollection.XML
- Don’t ask threat questions where a control is already covered
  - Modify ThreatTypes.XML
  - Example: TLS Data Flow doesn’t need to answer Sniffing question
- Make sure an issue is addressed in future threat models
  - Modify ThreatTypes.XML
  - Add “assure that logs provide traceability” or add a new Repudiation threat that occurs for specified elements
Security Analysis Tools

- Portfolio Risk Assessment – what to threat model
- Threat Modeling
- Secure Code training and manual code review
- Static Analysis (SAST)
- Dynamic Analysis (DAST)
- Penetration Testing
- External Audit
TAM - Quantitative analysis with DREAD

Confidentiality Threat

Ford DREAD Calculations

Please select appropriate values for the following threat:

- Unauthorised disclosure of <1> packs goods into > using <Basket> by <Little Red Riding Hood>

Business Impact:
- Damage Potential: Minor
- Affected Users: User or few users

Weighted Calculations:
- Impact: 0.400
- Probability: 1.000
- Risk Score: 0.700

RSA Conference 2015
Metrics

- What does success look like?
  - Don’t impact project timing
  - Head off issues that could delay launch

- Number of sessions completed is more meaningful than number of threat models, but not much

- Number of threats
  - Mitigated with common control
  - Mitigated with nonstandard control
  - Unmitigated or Accepted
Futures

- How do we define “finished”?
  - Send XML TMS file to Security Consulting
  - Check off mitigation jointly with Security
  - Mitigations completed
  - Actions entered in Backlog/Test plan
  - File as Control Review attachment

- Custom elements

- What do YOU think we need?
Summary

- Threat Modeling makes Security look good
- Treat SME time like gold and they will treasure you
- Include only irreducible elements where answers are different
- Resolving issues is the hard part!
- Don’t be afraid to customize especially to save time
- Success is every A-ha moment
- Massive success is when the SMEs want to do it themselves
Apply Threat Modeling in your organization

- Next week you should:

- In the first three months following this presentation you should:
  - Think about new projects in your organization that are good candidates for Threat Modeling and complete your first Threat Model

- Within six months you should:
  - Review what you have learned in your organization and determine who else can benefit from using Threat Modeling
Questions?

- Please use the microphones
Acknowledgements

- Michael Jones photograph “400M Hurdles” from the 2012 Olympics, Creative Commons license CC BY-NC-SA 2.0
- Adam Shostack, “New Foundations for Threat Modeling”
- Albert Einstein, “On the Method of Theoretical Physics”