RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: ASD-R01

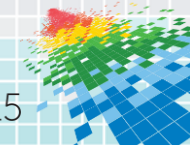
Rapid Threat Modeling Techniques

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!

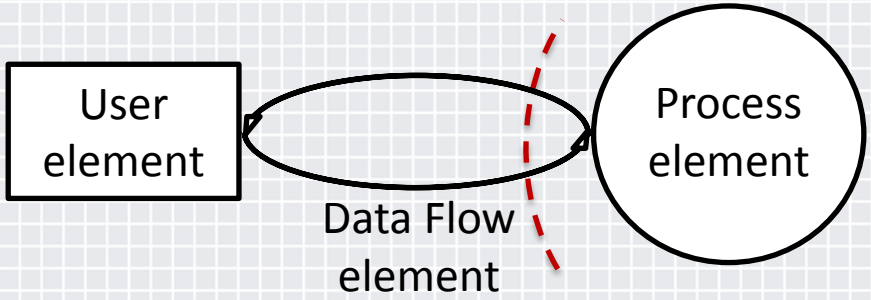


What is Threat Modeling?

- Design practice from the Software Assurance Forum (SAFECode)
  - Attack trees
  - Threat library (CAPEC, OWASP Top Ten)
  - Use Cases
  - STRIDE
    - **S**poofing
    - **T**ampering
    - **R**epudiation
    - **I**nformation Disclosure
    - **D**enial of Service
    - **E**levation 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

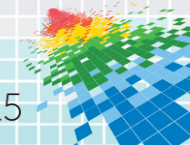


STRIDE by elements

Threats	Data Flows	Data Stores	Processes	Interactors
Spoofing			X	X
Tampering	X	X	X	
Repudiation		X	X	X
Information Disclosure	X	X	X	
Denial of Service	X	X	X	
Elevation of Privilege			X	

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

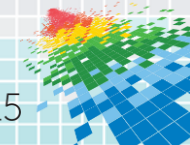
Art of the Data Flow Diagram

…make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation…

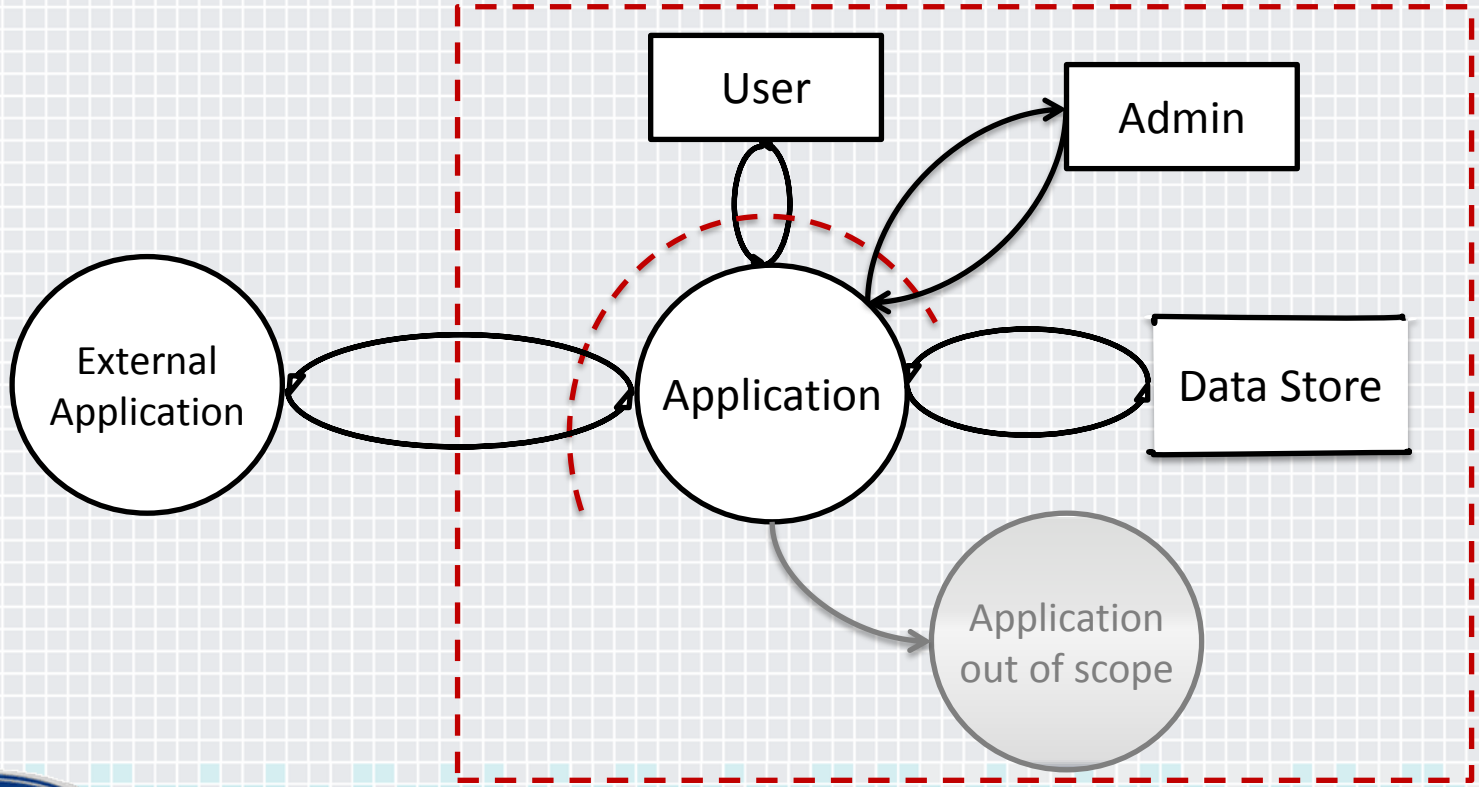
- *Einstein*

Threat Modeling Is Like Playing A Violin

- *Shostack*



Data Flow Diagram elements



Generate STRIDE Threats - Analyze Model

Threat:	Data Flow Sniffing	Category:	Information Disclosure	Mitigated
Description		**Justification for threat state change**		
PII Data in transit exposed. Default text appears here and can be customized so it makes sense to your users				

- 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

Generate STRIDE Threats - Analyze Model

Threat:	Data Flow Sniffing	Category:	Information Disclosure	Mitigated
Description		**Justification for threat state change**		
PII Data in transit exposed		TLS encrypted		

- 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

Generate STRIDE Threats - Analyze Model

Threat:	Insufficient Auditing	Category:	Repudiation	Needs investigation
Description		**Justification for threat state change**		
Does the log capture enough data to understand what happened and what the source of the change was?		Need to determine strategy to assure that logs provide traceability		

- 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.

Generate STRIDE Threats - Analyze Model

Threat:	Insufficient Auditing	Category:	Repudiation	Needs investigation
Description		**Justification for threat state change**		
Does the log capture enough data to understand what happened and what the source of the change was?		Need to determine strategy to assure that logs provide traceability		

- 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.

Generate STRIDE Threats - Analyze Model

Threat:	Insufficient Auditing	Category:	Repudiation	Needs investigation
Description		**Justification for threat state change**		
Does the log capture enough data to understand what happened and what the source of the change was?		Need to determine strategy to assure that logs provide traceability		

- 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

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

Generate STRIDE Threats - Analyze Model

Threat Priority	High

- 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

Protocol	C	I
HTTP	1	1
HTTPS	3	2
FTP	1	1
FTPS	3	2
SFTP	3	2
OFTP1	1	1
OFTP2	3	3
SMTP	1	1

Table 2.3 CIA Capability for Basic Interoperability Security Tech

Tech	C	I	A
Crypt/FMCCrypt [a]	3	2	N/A
DS	N/A	3	N/A
HA	N/A	N/A	3
SSL/MQSSL	3	2	N/A
SSH	3	2	N/A
Secure VPN	3	2	2
IC	N/A	2	N/A
WSL	N/A	N/A	N/A

[a]: Can support I=2 only data in transport with message integrity check

Common Controls - Customize

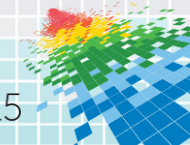
	MODEL ELEMENTS			
THREATS	Data Flows	Data Stores	Processes	Interactors
Spoofing	N/A	N/A	WSL	WSL Strong Auth Active Directory
Tampering	SSL TLS	Config validation Database Encryption	APS	N/A
Repudiation	N/A	Oracle/SQL Farm Turn on table level logs	Logs Digital Signing	Logs
Information Disclosure	SSL TLS	Database Encryption	APS	N/A
Denial of Service	CDN ANX	Oracle/SQL Farm	Config Validation CSP	N/A
Elevation of Privilege	N/A	N/A	Config Validation CSP	N/A

Common Controls - Customize

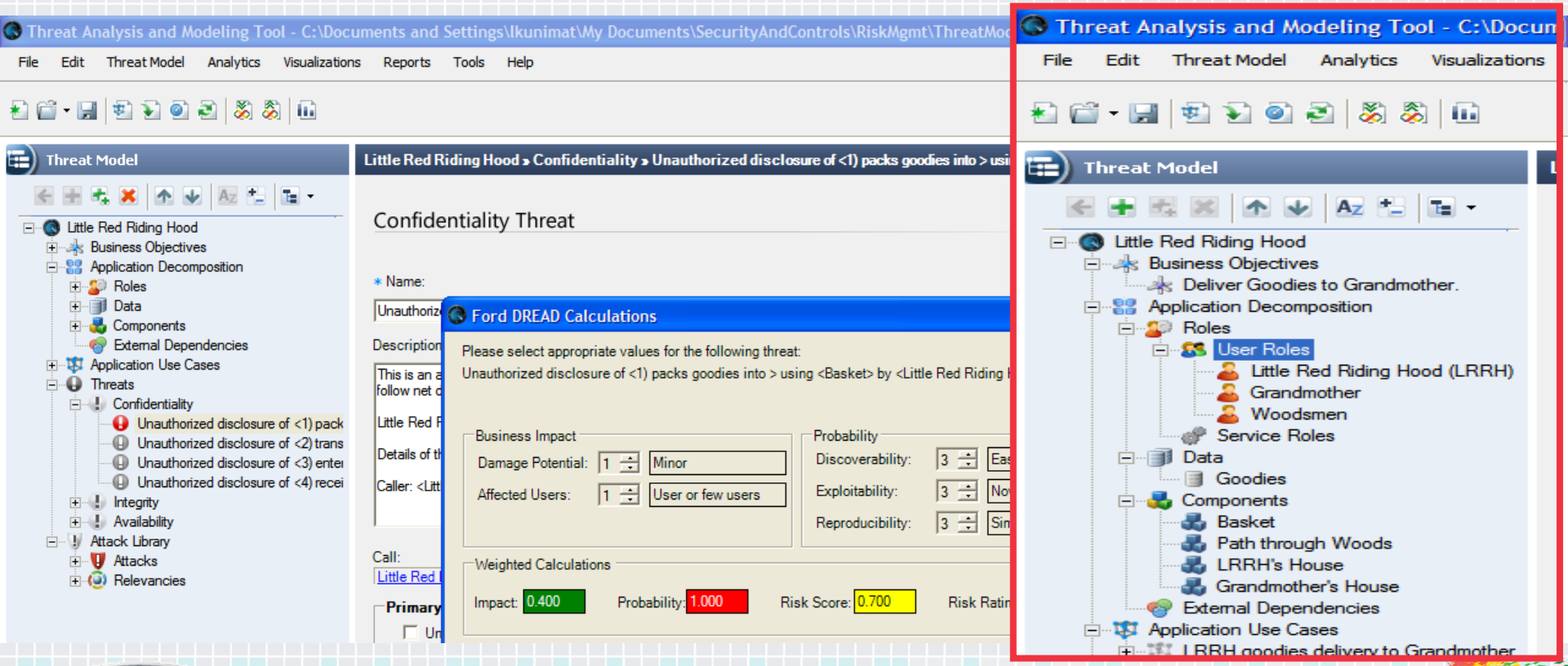
- Add your standard controls to StandardElementCollection.XML
- Don’t ask threat questions where a control is already covered
  - Modify ThreatTypes.XML
  - Example: TLS Data Flow doesn’t need to answer Sniffing question
- Make sure an issue is addressed in future threat models
  - Modify ThreatTypes.XML
  - 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

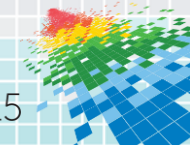


TAM - Quantitative analysis with DREAD



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

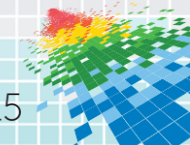
- How do we define “finished”?
  - Send XML TMS file to Security Consulting
  - Check off mitigation jointly with Security
  - Mitigations completed
  - Actions entered in Backlog/Test plan
  - File as Control Review attachment
- Custom elements
- What do YOU think we need?

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

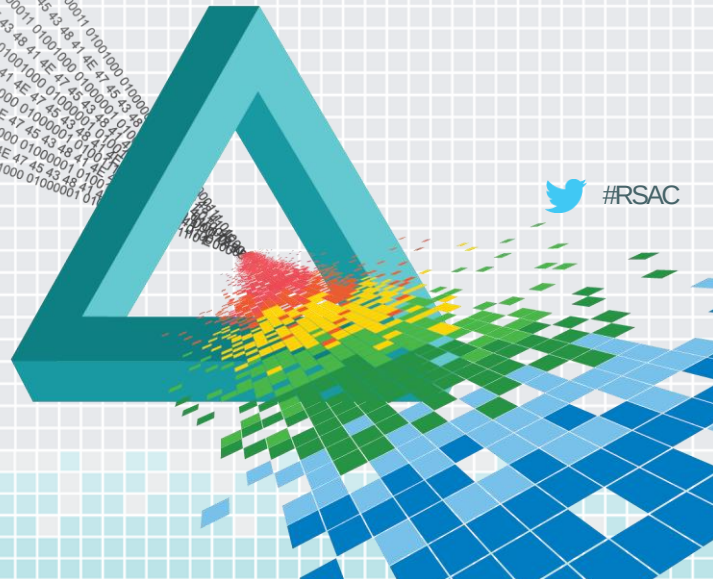
Apply Threat Modeling in your organization

- Next week you should:
  - Install the SDL Threat Modeling tool from http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx
- 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

- SAFECode, “Fundamental Practices for Secure Software Development: A Guide to the Most Effective Secure Development Practices in Use Today”
- Lou Kunimatsu, “My, What Big Teeth You Have: A Threat Analysis and Modeling Fairy Tale”
- 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”