

# User-Story Driven Threat Modeling

Granite State Code Camp (GSCC) 2018  
November 3, 2018  
Robert Hurlbut  
[@RobertHurlbut](#)



Who am I?



**Robert Hurlbut**  
SVP, Threat Modeling Architect / Lead  
Cyber Security Technology  
Bank of America



## Agenda

What is Threat Modeling?

Threat Modeling Process

Threat Modeling in Agile / DevOps?

Modern Approaches



## What is Threat Modeling?



What is threat modeling?

You probably (hopefully!) already do these in your security strategy:

Penetration testing

Vulnerability assessments

DAST / SAST tools

Other automated tools ...

**But, if not threat modeling – you are missing a lot!**



What is threat modeling, continued?

Something we all do in our personal lives ...

... when we lock our doors to our house

... when we lock the windows



... when we lock the doors to our car



What is threat modeling, continued?

When we ...

think ahead on what could go wrong

*(i.e. the “what if” questions),*

weigh the risks,

and act accordingly ...

... we are “**threat modeling**”



What is threat modeling, continued?

**Threat modeling** is:

Process of understanding  
your system and potential  
threats against your system

i.e. ***Critical Thinking*** about Security



## Approaches to Threat Modeling

### Asset-centric

Assets, Attack trees

### Software-centric

Secure design, DFDs

### Attacker-centric

Profile, patterns



## Threat Modeling your House

### Asset-centric

Family, irreplaceable photos, valuable artwork



### Software-centric

Physical features (pool or front porch)

### Attacker-centric

Who might break in, current security system



What is threat modeling?

**Threat model** includes:

understanding of system,  
identified threat(s),  
proposed mitigation(s),  
priorities by risk



Threat Modeling Process

1. Diagram / understand your system and data flows
2. Identify threats through answers to questions
3. Determine mitigations and risks
4. Follow through



When? Make threat modeling first priority

In SDLC – Requirements and Design phase(s):  
[Requirements](#) > [Design](#) > [Development](#) > [Test](#) > [Deployment](#)

Threat modeling -> new requirements

Incremental threat modeling ->  
Agile / DevOps  
(User Stories, Abuser / Attacker Stories)

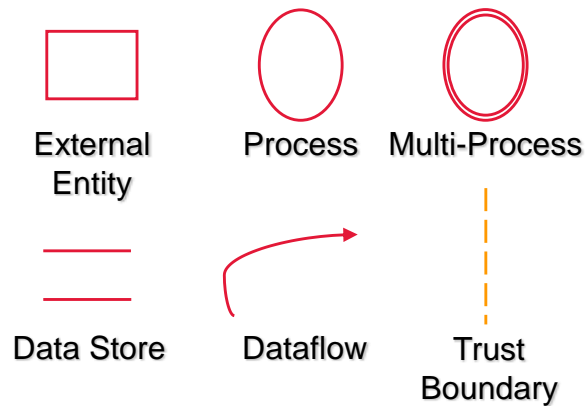


## Threat Modeling Process



Understand the system

## DFD – Data Flow Diagrams (MS SDL)



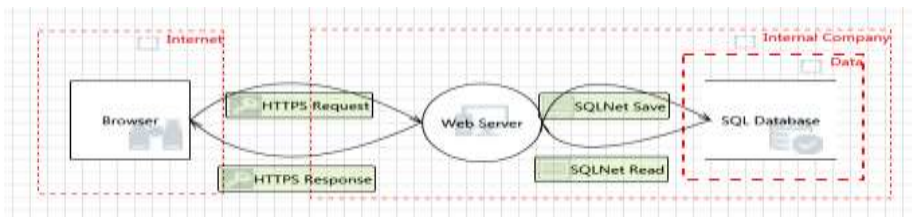
Understand the system

How do the interactors, processes and data stores connect?  
Connect the info points with the data flow arrows.

Where are the trust boundaries?

For example:

- Browser (interactor) sends / receives data (data flow) with a web service (process) which saves / reads data (data flow) using a SQL Database (data store)
- Trust boundaries indicate where trust changes — authenticate / authorize / validate





Identify threats – Many Ways

STRIDE

Attack Trees

Bruce Schneier - Slide deck

Threat Libraries

CAPEC, ATT&CK, OWASP Top 10, SANS Top 25

Checklists

OWASP ASVS, OWASP Proactive Controls

Card Games

OWASP Cornucopia, Elevation of Privilege

Use Cases / Abuse Cases



17

STRIDE Framework – Data Flow

Threat	Examples	Property we want
Spoofing	Pretending to be someone else	Identity Assurance
Tampering	Modifying data that should not be modifiable	Integrity
Repudiation	Claiming someone didn't do something	Non-repudiation
Information Disclosure	Exposing information	Confidentiality
Denial of Service	Preventing a system from providing service	Availability
Elevation of Privilege	Doing things that one isn't suppose to do	Least Privilege



## Identify Threats – Functional

Input and data validation

Authentication

Authorization

Configuration management

Data Classification

- Public, Proprietary, Confidential



## Identify Threats – Functional

Session management

Cryptography

Parameter manipulation

Exception management

Auditing, logging, and monitoring



## Identity Threats – Ask Questions

Who's interested in app and data (threat agents)?

What goals (assets)?

What attack methods (how)?

Any attack surfaces (trust boundaries) exposed?

Any input/output (data flows) missing?



Determine mitigations and risks

### Mitigation Options:

- Leave as-is

- Remove from product

- Remedy with technology countermeasure

- Warn user

Make the mitigations part of your Security acceptance criteria

What is the risk associated with the vulnerability and threat identified?



Risk Rating

Risk is product of two factors:  
Ease of exploitation  
Business impact



Follow through

Document findings and decisions

File bugs or new requirements (as stories)

Verify bugs fixed / new requirements (stories)  
implemented

Did we miss anything? Review again

Anything new? Review again



# Threat Modeling in Agile / DevOps?



## Threat Modeling approaches – Waterfall vs Agile\*

	<b>Waterfall: Threat Model Documents</b>	<b>Agile: Bugs and conversations</b>
<b>System Model</b>	<ul style="list-style-type: none"> <li>• Big complex scope</li> <li>• System diagrams and essays</li> <li>• Gates, dependencies</li> </ul>	<ul style="list-style-type: none"> <li>• Scope tiny: this sprint's change</li> <li>• Big picture as security debt</li> </ul>
<b>Finding Threats</b>	<ul style="list-style-type: none"> <li>• Brainstorm</li> <li>• STRIDE</li> <li>• Kill Chain</li> </ul>	<ul style="list-style-type: none"> <li>• Same, aim at in-sprint code</li> </ul>
<b>Fixes</b>	<ul style="list-style-type: none"> <li>• Controls</li> <li>• Mitigations</li> <li>• Test Cases</li> </ul>	<ul style="list-style-type: none"> <li>• Spikes to understand</li> <li>• Security-focused stories in sprint, backlog, or epic</li> <li>• Security acceptance criteria</li> </ul>
<b>Quality</b>	<ul style="list-style-type: none"> <li>• Test plans</li> </ul>	<ul style="list-style-type: none"> <li>• Test automation</li> </ul>



\*Adapted from Adam Shostack's talk at BlackHat 2018 on Threat Modeling in 2018

When?

There are many out-of-band activities (as opposed to inline activities such as coding, etc.)

Sprint planning

Spikes

Add Threat Modeling as another out-of-band activity

and/or

In addition to when you create User Stories (or Abuser Stories)



User stories

User stories written typically like this:

***As a <type of user>, I want <some goal> so that <some reason>***

Examples:

- As a user, I can backup my entire hard drive.
- As a power user, I can specify files or folders to backup based on file size, date created, and date modified.
- As a user, I can indicate folders not to backup so that my backup drive isn't filled up with things I don't need saved.



## Security User stories

Security user stories are similar to regular user stories, but are sometimes more difficult to manage – there may be too many of them.

Examples:

- As a user, I want to log into the application.
- As a user, I want to be able to see my account information and not other users' information.
- As an admin, I want to have access to configuration settings in the application.



## Abuser stories

Abuser / attacker stories do this differently:

***As <someone with malicious intent>, I want to <do some bad thing>***

Examples:

- As a hacker, I want to read the application log files.
- As an insider, I want to access a customer's account information.
- As a disgruntled employee, I want to change pricing for some products.

See OWASP Abuse Case Cheat Sheet for help in creating these.  
[https://www.owasp.org/index.php/Abuse\\_Case\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Abuse_Case_Cheat_Sheet)



## Typical Threat Modeling Session (Agile / DevOps version)

### In Sprint Planning:

- Team
- Focused scope to set of stories
- Understand requirements, keep business / technical goals in mind

**Important:** Be honest, leave ego at the door,  
no blaming!



Prioritize issues in the backlog

Work through your user stories / abuser stories – determine threats and mitigations as you go

As you find issues, write these to the backlog

Prioritize based on risk





# Modern Approaches



## Modern Approaches

### Incremental Threat Modeling

Agile approaches – Irene Michlin ([@IreneMichlin](#))

### Lateral Movement

“The Industrial Revolution for Lateral Movement”  
BlackHat 2017

Think STRIDE + LM

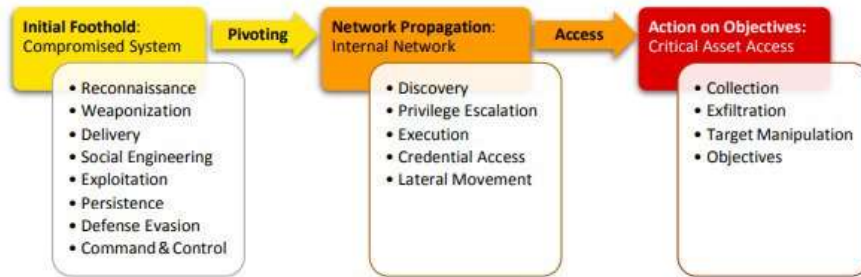
### Privacy by Design (addressing GDPR, etc.)

STRIPED + LM



## Kill Chain as Alternative to STRIDE

### Kill Chain – useful for operational threat models



See Paul Pols' work on Unified Kill Chain:

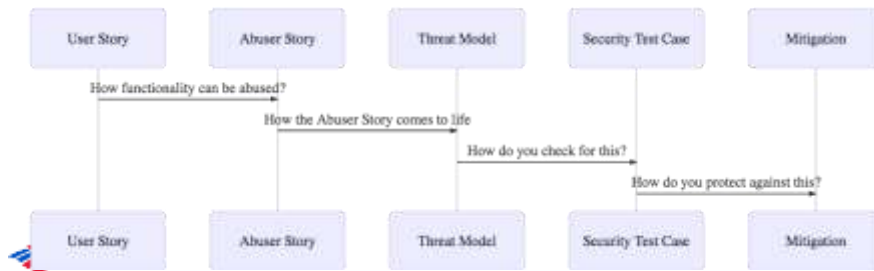
<https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf>

## Threat Modeling as Code – applying “Spec” based systems

- ThreatPlaybook  
([@abhaybhargav](#))



Providing a way to combine User / Abuser stories, threat scenarios, and automated security testing.



36

## Threat Modeling as Code – applying “Spec” based systems

- ThreatPlaybook  
([@abhaybhargav](#))



```

1 (create_customer_profile):
2   description: As an end-user, I would like to create customer profile and upload information to the customer profile. This will have the
3   abuse_cases:
4     - api_unavailable:
5       description: As a malicious user, I would render the upload and API system unavailable to the organization
6       threat_scenarios:
7         - malware_file_upload:
8           description: Upload files with malware that brings down the system or subjects it to ransomware
9           severity: 3
10          cwe: 434
11          cves:
12            - template_injection_auto
13            - nmap_vulnerability_scan
14            - oss_auto
15            - malicious_file_upload
16        steal_customer_sensitive_files:
17          description: As a malicious user, I would like to steal customer PII from the uploaded files for me to be able to monetize this info
18          threat_scenarios:
  
```



37

## Threat Modeling as Code – applying “Spec” based systems

- ThreatSpec [@ThreatSpec](#)
- Fraser Scott [@zeroXten](#)



ThreatSpec - Have developers and security engineers write threat specifications alongside code, then dynamically generate reports and data-flow diagrams from the code.



38

## Threat Modeling as Code – applying “Spec” based systems

- ThreatSpec [@ThreatSpec](#)
- Fraser Scott [@zeroXten](#)



39

## Resources - Books

### Threat Modeling: Designing for Security

*Adam Shostack*

### Securing Systems: Applied Architecture and Threat Models

*Brook S.E. Schoenfield*

### Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis

*Marco Morana and Tony UcedaVelez*

### Measuring and Managing Information Risk: A FAIR Approach

*Jack Jones and Jack Freund*



## Resources - Tools

### Microsoft Threat Modeling Tool

<http://www.microsoft.com/en-us/download/details.aspx?id=49168> (2016)

<https://blogs.msdn.microsoft.com/secdevblog/2018/09/12/microsoft-threat-modeling-tool-ga-release/> (2018)

### ThreatModeler – Web Based (in-house) Tool

<http://myappsecurity.com>

### IriusRisk Software Risk Manager

<https://iriusrisk.continuumsecurity.net>

### OWASP Threat Dragon

[https://www.owasp.org/index.php/OWASP\\_Threat\\_Dragon](https://www.owasp.org/index.php/OWASP_Threat_Dragon)



## Resources - Tools

### Attack Trees – Bruce Schneier on Security

<https://www.schneier.com/attacktrees.pdf>

### Elevation of Privilege (EoP) Game

<http://www.microsoft.com/en-us/download/details.aspx?id=20303>

### OWASP Cornucopia

[https://www.owasp.org/index.php/OWASP\\_Cornucopia](https://www.owasp.org/index.php/OWASP_Cornucopia)

### OWASP Application Security Verification Standard (ASVS)

[https://www.owasp.org/index.php/Category:OWASP\\_Application\\_Security\\_Verification\\_Standard\\_Project](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)

### OWASP Top 10 Proactive Controls 2018

[https://www.owasp.org/index.php/OWASP\\_Proactive\\_Controls](https://www.owasp.org/index.php/OWASP_Proactive_Controls)



## Resources - Tools

### ThreatPlaybook

<https://we45.gitbook.io/threatplaybook>

### ThreatSpec

<https://threatspec.org/>



43

Questions?



[@RobertHurlbut](#)



Thank you!

