User-Story Driven Threat Modeling

CodeMash 2019
January 10, 2019

Robert Hurlbut
@RobertHurlbut @AppSecPodcast

Who am I?

Robert Hurlbut

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

Agenda

Why, What, When - Threat Modeling?

Threat Modeling Process

Threat Modeling in Agile / DevOps?

Modern Approaches

Why, What, When - Threat Modeling?

Brook Schoenfield @BrkSchoenfield June 29, 2015

"As I practice it, threat modeling cannot be the province of a tech elite. It is best owned by all of a development team."

Why 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!

Why threat modeling?, continued

Common scenario: How do I secure data in the cloud?

Storage?
Accessed?
Monitored?
Configured properly?

Threat Modeling helps us focus on these questions and answers to lead to <u>secure design</u>

Why threat modeling?, continued

Common data breach problem:

Misconfigured AWS S3 Buckets

Impacted in 2017-2018 *:

- FedEx
- GoDaddy
- Accenture
- Verizon
- American voter data (198 million American voters)
- National Credit Federation
- Booz Allen Hampton
- Dow Jones
- Keeper and Blur (password managers)

* https://www.zdnet.com/article/security-lapse-exposes-198-million-united-states-voter-records/

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

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

Threat Modeling Process

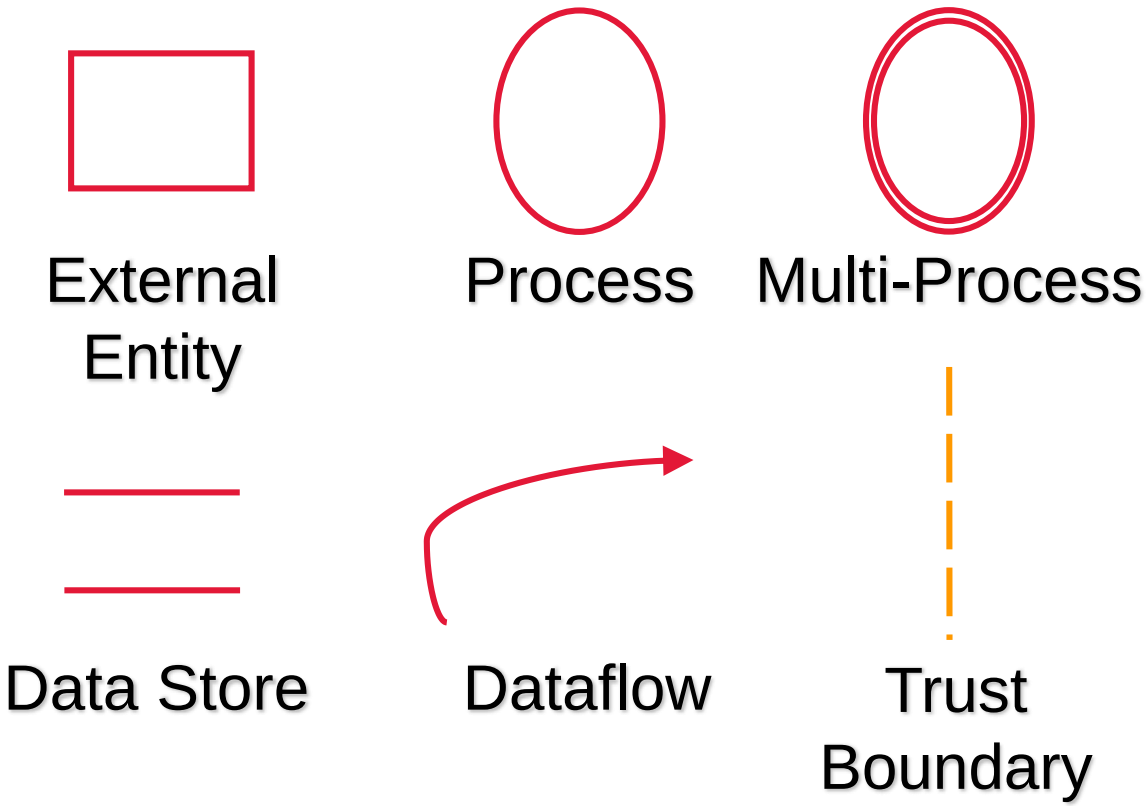
Threat model includes:

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

DFD – Data Flow Diagrams (MS SDL)

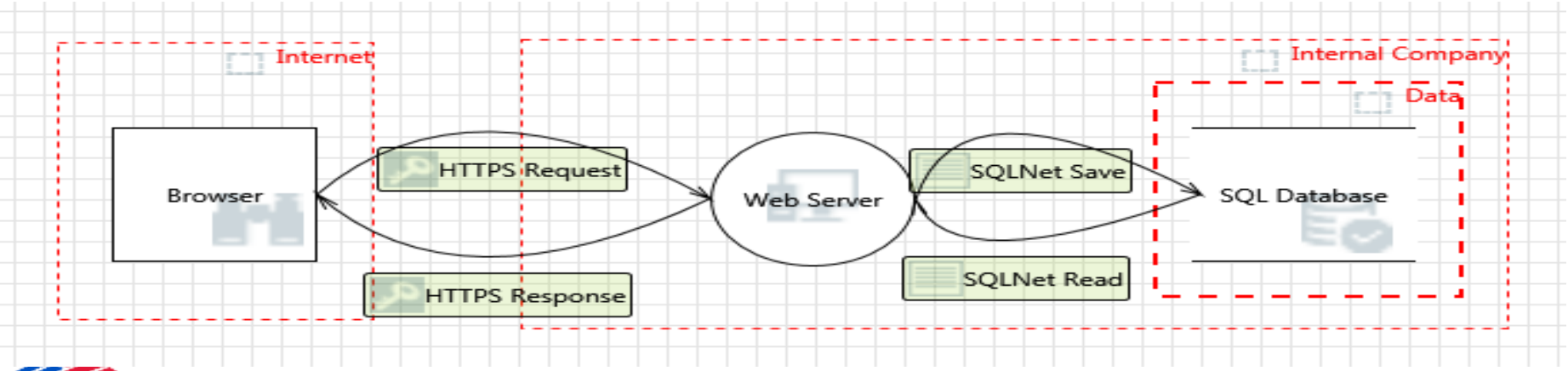


Understand the system

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



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 – 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

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

Simple Tools

Whiteboard

Visio (or equivalent) – diagraming

Word (or equivalent) / Excel (or equivalent) - documenting threats / mitigations

Other Tools

Tool	Cost	Platforms
MS Threat Modeling Tool (2016/2018)	Free	Windows OS Install only
ThreatModeler	Paid	Web Based
IriusRisk	Paid	Web Based
OWASP Threat Dragon	Free	Web Based / Windows, Mac, Linux installs
Draw.IO	Free	Web Based / Windows, Mac, Linux installs

Threat Modeling in Agile / DevOps?

Value of threat modeling

Ed Moyle (2017):

*"Very few organizations will have the time or resources to **threat model** their entire ecosystem. Assuming you do not have that luxury, you still can realize quite a bit of **value** just by adopting the mindset of looking for blind spots and questioning assumptions."* *

* (Quoted from an article by Ed Moyle: https://www.ecommercetimes.com/story/Invisible-Technologies-What-You-Cant-See-Can-Hurt-You-84852.html)

Threat Modeling approaches – Waterfall vs Agile*

	Waterfall: Threat Model Documents	Agile: Bugs and conversations
System Model	• Big complex scope • System diagrams and essays • Gates, dependencies	• Scope tiny: this sprint's change • Big picture as security debt
Finding Threats	• Brainstorm • STRIDE • Kill Chain	• Same, aim at in-sprint code
Fixes	• Controls • Mitigations • Test Cases	• Spikes to understand • Security-focused stories in sprint, backlog, or epic • Security acceptance criteria
Quality	• Test plans	• Test automation

*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 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

Abuser stories applied to OWASP Top 10 *

A2:2017-Broken Authentication

Epic:

Attackers have access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools. Session management attacks are well understood, particularly in relation to unexpired session tokens.

Abuse Case:

As an attacker, I have access to hundreds of millions of valid username and password combinations for credential stuffing.

Abuse Case:

As an attacker, I have default administrative account lists, automated brute force, and dictionary attack tools I use against login areas of the application and support systems.

Abuse Case:

As an attacker, I manipulate session tokens using expired and fake tokens to gain access.

* 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

Mozilla's Rapid Risk Assessment (RRA) *

No time for a full threat model? ***RRA in 30 minutes***

Focused on services and entry points:

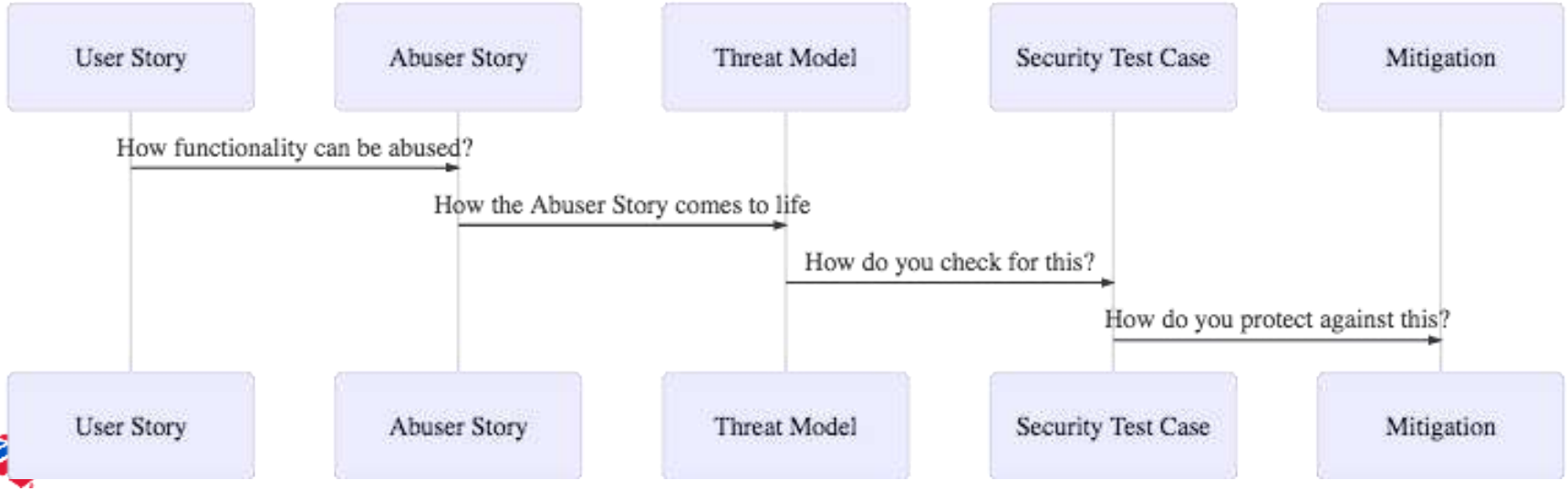
1. Are you making changes to the attack surface? (i.e new entry points)
2. Are you changing the application stack or application security controls?
3. Are you adding confidential/sensitive data?
4. Have threat agents changed? Are we facing new risk?

* https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment.html
Blog post: https://home.edwinkwan.com/rapid-risk-assessments/

Threat Modeling as Code – applying “Spec” based systems

- ThreatPlaybook (@abhaybhargav)

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



Threat Modeling as Code – applying “Spec” based systems

- ThreatPlaybook (@abhaybhargav)


```yaml
create_customer_profile:
  description: As an end-user, I would like to create customer profile and upload information to the customer profile. This will have the
  abuse_cases:
    render api unavailable:
      description: As a malicious user, I would render the upload and API system unavailable to the organization
      threat_scenarios:
        malware file upload:
          description: Upload file with malware that brings down the system or subjects it to ransomware
          severity: 3
          cwe: 434
          cases:
            - template_injection_auto
            - nmap_vulnerability_scan
            - xxe_auto
            - malicious_file_upload
    steal customer sensitive files:
      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
      threat_scenarios:
```

Threat Modeling as Code – applying “Spec” based systems

- ThreatSpec @ThreatSpec
- Fraser Scott @zeroXten

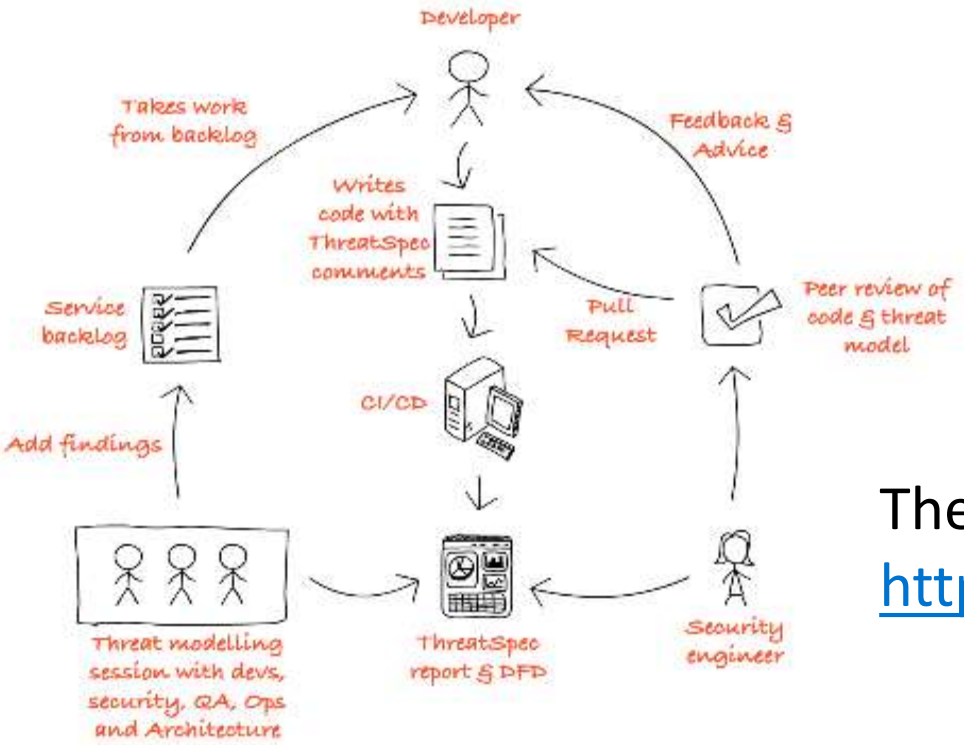
ThreatSpec - Have developers and security engineers write threat specifications alongside code, then dynamically generate reports and data-flow diagrams from the code.

```
@threat SQL Injection as @sqli
@describe @sqli as Nefarious SQL statements are inserted into an entry field for
execution

@architecture MyApp as @myapp
@component Product Service as @product belongs to @myapp
@mitigates @product against SQL Injection with Parameterised queries
```

Threat Modeling as Code – applying "Spec" based systems

- ThreatSpec @ThreatSpec
- Fraser Scott @zeroXten



They would love feedback!
https://threatspec.org/survey/

Conclusion

Threat Modeling is too important not to do it

In an Agile / DevOps world, we still need to think about Secure Design

Find ways to integrate Threat Modeling into your sprints with Abuser Stories, Quick Reviews, Automated Testing, etc.

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 2018

https://aka.ms/threatmodelingtool

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

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

OWASP Application Security Verification Standard (ASVS)

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

Resources - Tools

ThreatPlaybook

https://we45.gitbook.io/threatplaybook

ThreatSpec

https://threatspec.org/

Resources - Videos

Pluralsight

- Several good Threat Modeling videos, including excellent one on MS Threat Modeling Tool

LinkedIn Learning

- New video by Adam Shostack on Threat Modeling

Questions?

Slides:
https://roberthurlbut.com/r/CM19USTM

@RobertHurlbut
@AppSecPodcast

Thank you!