Using and Customizing Microsoft Threat Modeling Tool 2016

Boston Code Camp 27

March 25, 2017

Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut

Boston Code Camp 27 - Thanks to our Sponsors!

- Platinum
  - Microsoft
- Gold
  - HealthcareSource Quality Talent Suite™
  - NCache
  - NosDB
- Silver
  - BLUEMETAL
  - Progress Telerik
  - Robert Half Technology
- Bronze
  - RGood Software
  - Robert Hurlbut Consulting Services
  - Infragistics
  - Syncfusion
  - Redfin
  - jhc
  - Benjamin Day Consulting
  - Brainshark Power your content. Power your sales.

- In-Kind Donations
  - GrapeCity
  - Manning User Group Program Member
  - steema software
  - VR KIX Virtual Reality Will Blow Your Mind!
  - Wiley

Robert Hurlbut

Software Security Consultant, Architect, and Trainer

- Owner / President of Robert Hurlbut Consulting Services
- Microsoft MVP – Developer Security 2005-2009, 2015, 2016
- (ISC)2 CSSLP 2014-2017
- Co-host with Chris Romeo – Application Security Podcast

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut, @AppSecPodcast

© 2017 Robert Hurlbut Consulting Services

ROBERT HURLBUT CONSULTING SERVICES

securedevelop.NET

What is threat modeling?

Threat modeling helps you think strategically about your software design, in particular your secure software design.

A “way of thinking” tool – not automated security tool

© 2017 Robert Hurlbut Consulting Services

What is threat modeling?

Threat modeling is:

> Process of understanding your system and potential threats against your system

i.e. Critical Thinking about Security

© 2017 Robert Hurlbut Consulting Services

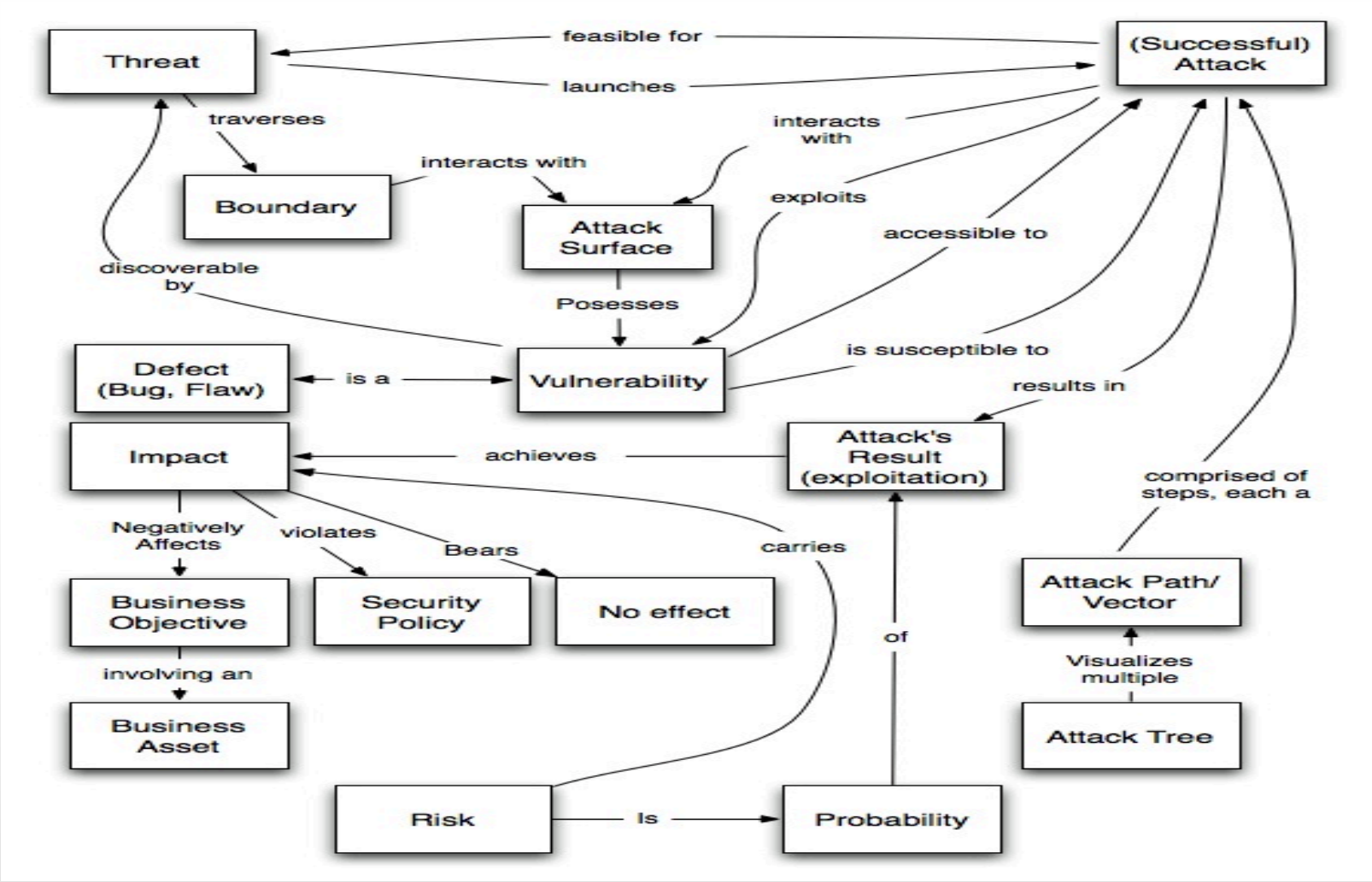
What is threat modeling?

Threat model includes:

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

© 2017 Robert Hurlbut Consulting Services

Threat Modeling Vocabulary*

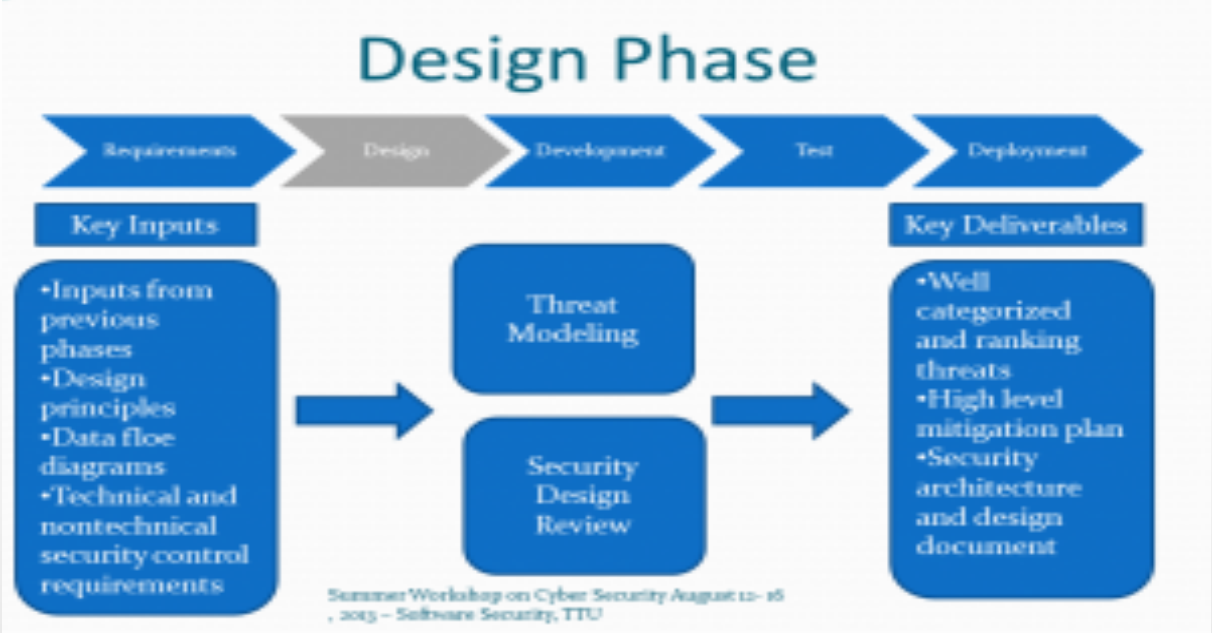


* https://www.cigital.com/blog/threat-modeling-vocabulary/ (John Steven, Cigital)

© 2017 Robert Hurlbut Consulting Services

When? Make threat modeling first priority

In SDLC – Requirements and Design phase

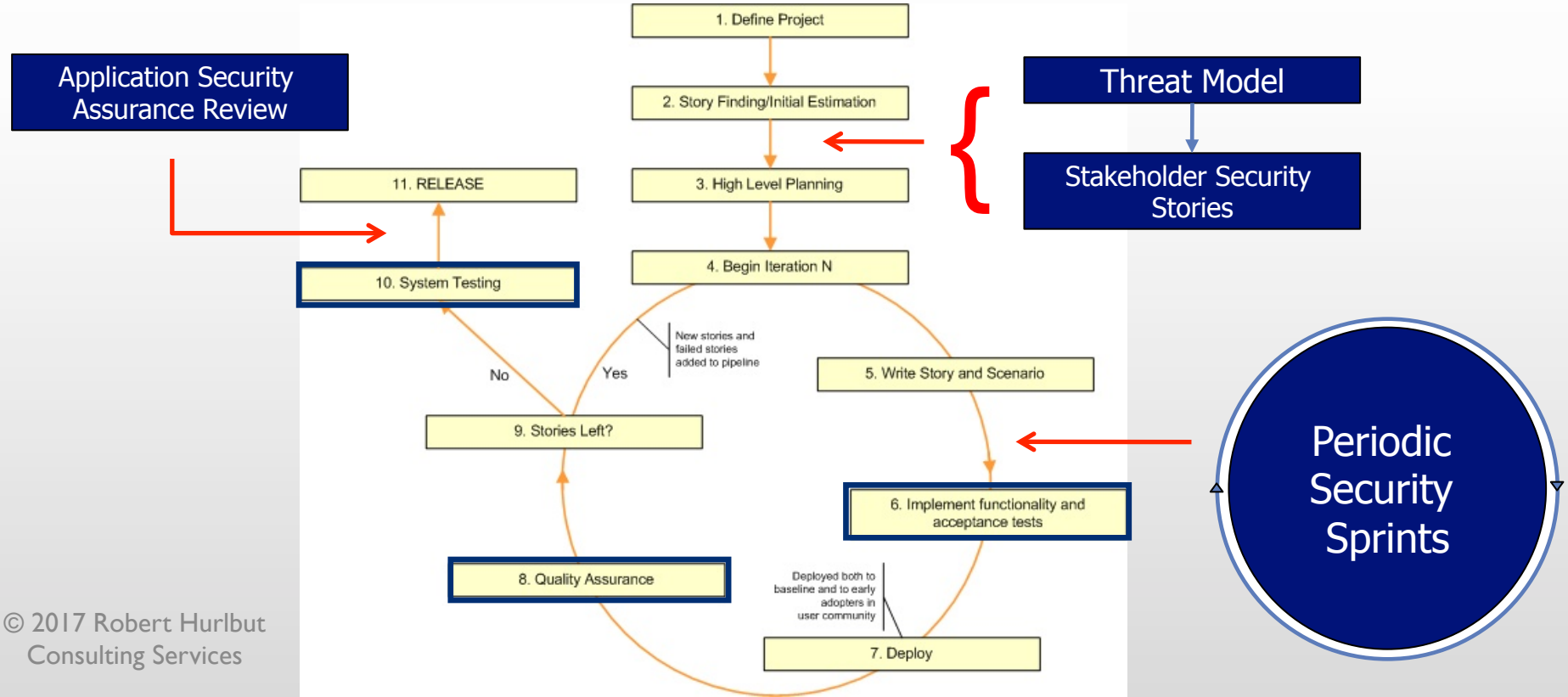


Threat modeling uncovers new requirements

© 2017 Robert Hurlbut Consulting Services

When? Make threat modeling first priority

Agile Sprint Planning - User Stories, Attacker Stories



© 2017 Robert Hurlbut Consulting Services

Simple Tools

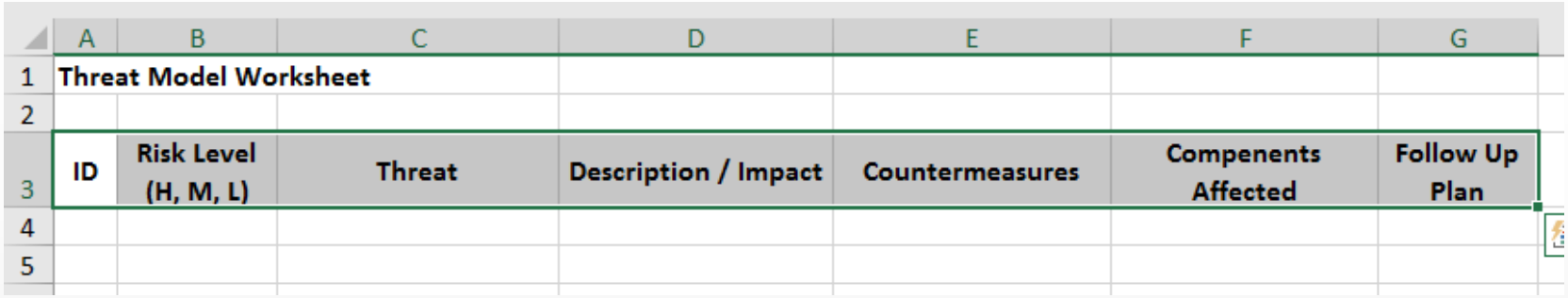
Whiteboard

Visio (or equivalent) for diagraming

Word (or equivalent) or Excel (or equivalent) for documenting

© 2017 Robert Hurlbut Consulting Services

Threat Model Sample Worksheet



	A	B	C	D	E	F	G
1	**Threat Model Worksheet**						
2							
3	**ID**	**Risk Level (H, M, L)**	**Threat**	**Description / Impact**	**Countermeasures**	**Compenents Affected**	**Follow Up Plan**
4							
5							

© 2017 Robert Hurlbut Consulting Services

Other Tools

Microsoft Threat Modeling Tool 2016

ThreatModeler – Web Based (in-house) Tool

ThreadFix

IriusRisk Software Risk Manager

© 2017 Robert Hurlbut Consulting Services

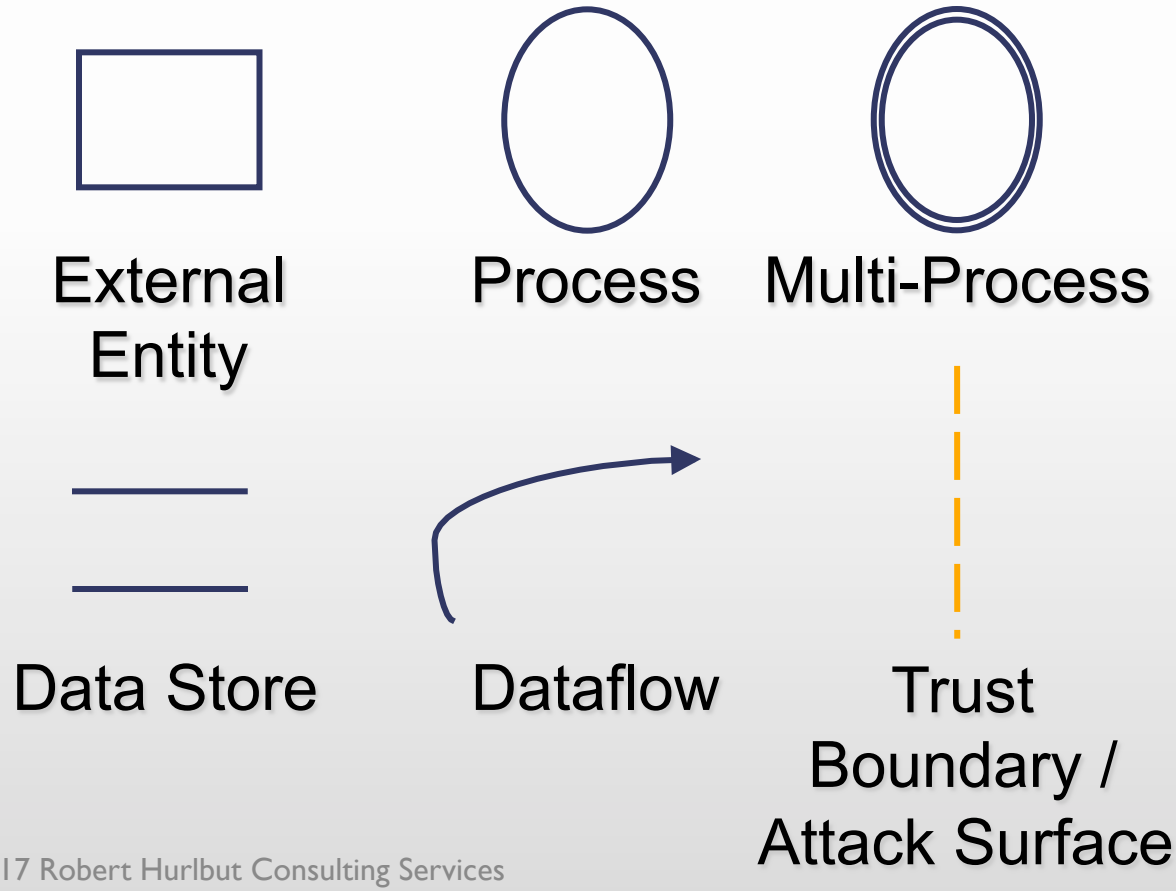
Threat Modeling Process

1. Draw your picture – understand the system and the data flows
2. Identify threats through answers to questions
3. Determine mitigations and risks
4. Follow through

© 2017 Robert Hurlbut Consulting Services

Understand the system

DFD – Data Flow Diagrams (MS SDL)



© 2017 Robert Hurlbut Consulting Services

Identify threats

Most important part of threat modeling (and most difficult)

Many ways – determine what works best for your team

© 2017 Robert Hurlbut Consulting Services

STRIDE Framework – Data Flow

Threat	Property we want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

© 2017 Robert Hurlbut Consulting Services

Mapping STRIDE to OWASP TOP 10

OWASP Top Ten 2013	STRIDE
A1 - Injection	Tampering, Spoofing
A2 – Broken Auth. & Session Management	Elevation of Privileges, Spoofing, Information Disclosure
A3 – Cross-Site Scripting (XSS)	Tampering, Spoofing
A4 – Insecure Object References	Privilege Escalation, Information Disclosure
A5- Security Misconfiguration	Information Disclosure (and others)
A6 – Sensitive Data Exposure	Information Disclosure
A7 – Missing Function Level Access Control	Privilege Escalation, Information Disclosure
A8 - Cross Site Request Forgery (CSRF)	Tampering, Spoofing, Elevation of Privileges
A9 - Using Components with Known Vuln.	All
A10 – Unvalidated Redirects and Forwards	Spoofing, Tampering

Microsoft Threat Modeling Tool 2016

Free ☺

Windows only ☹

Version History

- 2004, 2005: Threat Analysis & Modeling Tool (TAM) v1,v2: Windows GUI
- 2011: SDL Threat Modeling Tool 3: Visio Plugin
- …
- 2014: Microsoft Threat Modeling Tool 2014: Windows GUI
- **2015: Microsoft Threat Modeling Tool 2016: Windows GUI**

Download: http://aka.ms/tmt2016

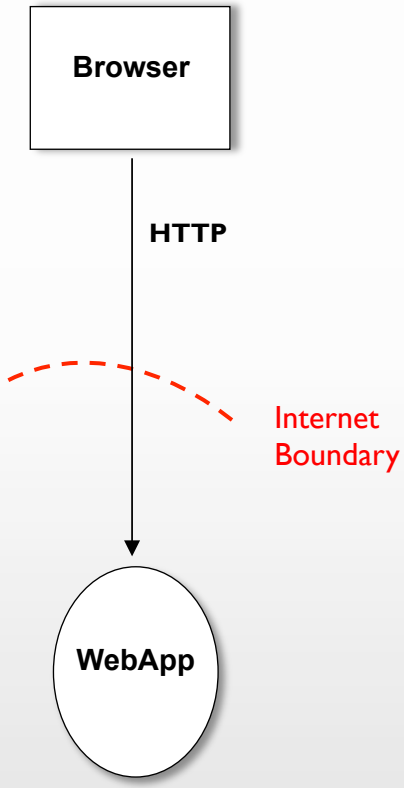
DFD Threat Modeling Logic

1. A **SOURCE**
   has a type („Browser“) and attributes
   has a parent („Generic External Interactor“) with attributes

2. Sends data via a **DATA FLOW**
   with a type („HTTP“) and attributes

3. That may crosses a **TRUST BOUNDARY**
   with a type („Internet Boundary“) and attributes

4. To a **TARGET**
   has a type („WebApp“) and attributes
   has a parent („Generic Process“) with attributes



DEMO

Microsoft Threat Modeling Tool 2016

© 2017 Robert Hurlbut Consulting Services

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

© 2017 Robert Hurlbut Consulting Services

Resources - Tools

Microsoft Threat Modeling Tool 2016

http://www.microsoft.com/en-us/download/details.aspx?id=49168

Open Threat Modeling Template

https://github.com/matthiasrohr/OTMT

Threat Model SDK (Java library)

https://github.com/stevespringett/threatmodel-sdk

© 2017 Robert Hurlbut Consulting Services

Questions?

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut, @AppSecPodcast

Email: robert at roberthurlbut.com

© 2017 Robert Hurlbut Consulting Services

ROBERT HURLBUT CONSULTING SERVICES

securedevelop.NET