Threat Modeling Workshop Labs

NERD Summit 2023
March 19, 2023

Robert Hurlbut
@RobertHurlbut

Who am I?

Robert Hurlbut

Principal Application Security Architect / Threat Modeling Lead @ Aquia, Inc. (https://aquia.us)

- **Microsoft MVP – Dev Sec / Dev Tech (2005 – 2009, 2015 -)**
- **(ISC2) CSSLP 2014-2023**
- **Founder / Leader two groups: Boston .NET Architecture Group (2004 -) and Amherst Security Group (2016 -)**
- **Co-host Application Security Podcast with Chris Romeo (2016 -)**

- **Co-author of "Threat Modeling Manifesto" (2020)**
- **Co-founder of Threat Modeling Connect (2022)**

Threat Modeling Lab 1:
Review case study
Draw a Data Flow Diagram (DFD)

Objectives

Reinforce what you just learned

Build a complete threat model with optional diagram for a fictitious system

Work in independent groups
- Even with a defined process, people come up with different threat models
- The models converge over time but is not likely to happen right away

Rare Books R Us

Fictitious mail-order bookseller specializing in rare and old book titles
Launching web-site: **Rare Books R Us**

Security is important but need help in determining where it is needed

Variety of data stores (Oracle, SQL Server, mySQL)

At some point, the company looks to move most of the data and operations to the cloud

Rare Books R Us

Business Goals:

- Provide online inventory of rare and old books
- Make searching and buying easy
- Security is important, but not sure how / where to apply it

Technical Goals:

- System written with React front end, Java backend interacting with several DB inventories and systems

Rare Books R Us

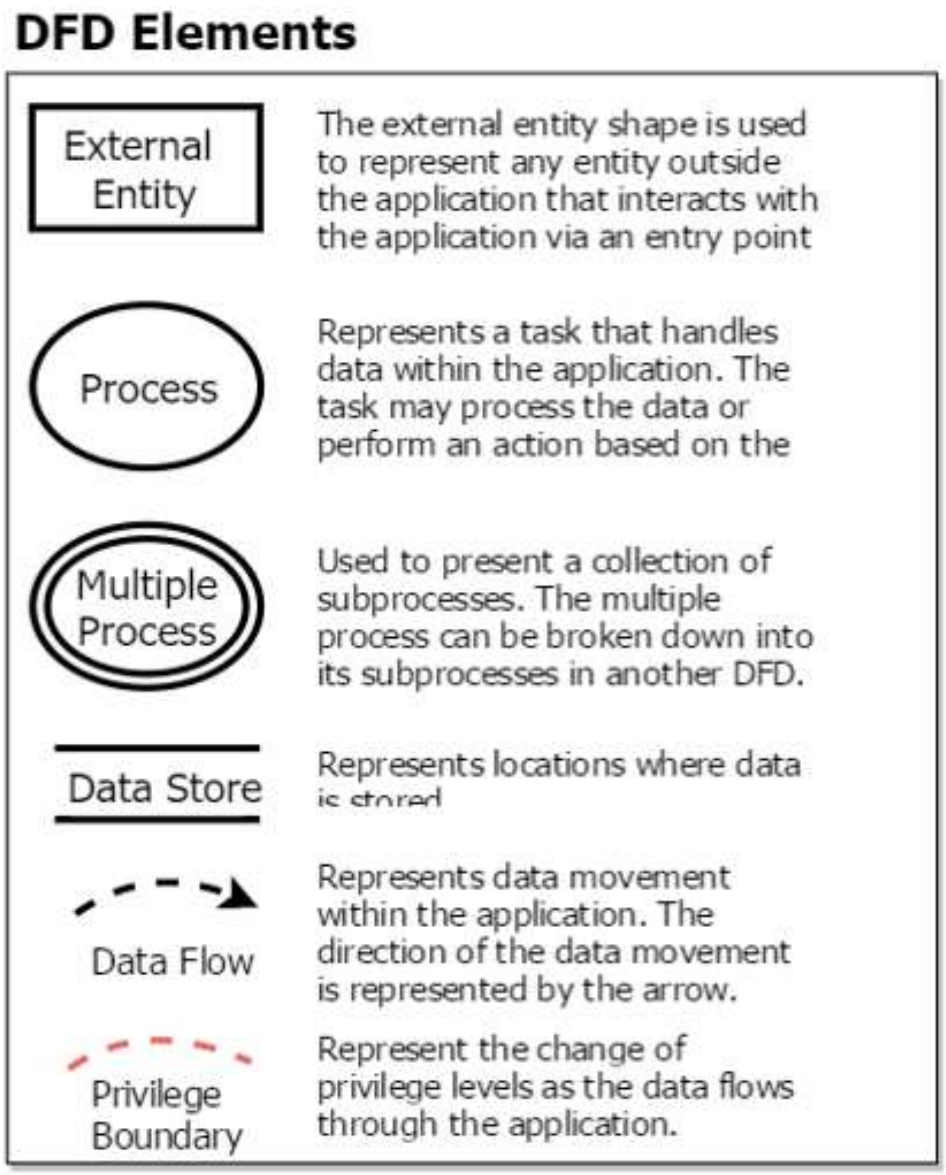
Data Stores:
Customers
Orders
Invoices

Users:
Customers (external)
Warehouse (internal)

Processes:
Receive Order
Collect Payments
Ship Books

Data Flows:
Orders
Billing information
Order details / shipping details
Etc.

Data Flow Diagram (DFD)



Model the system

To model the system:

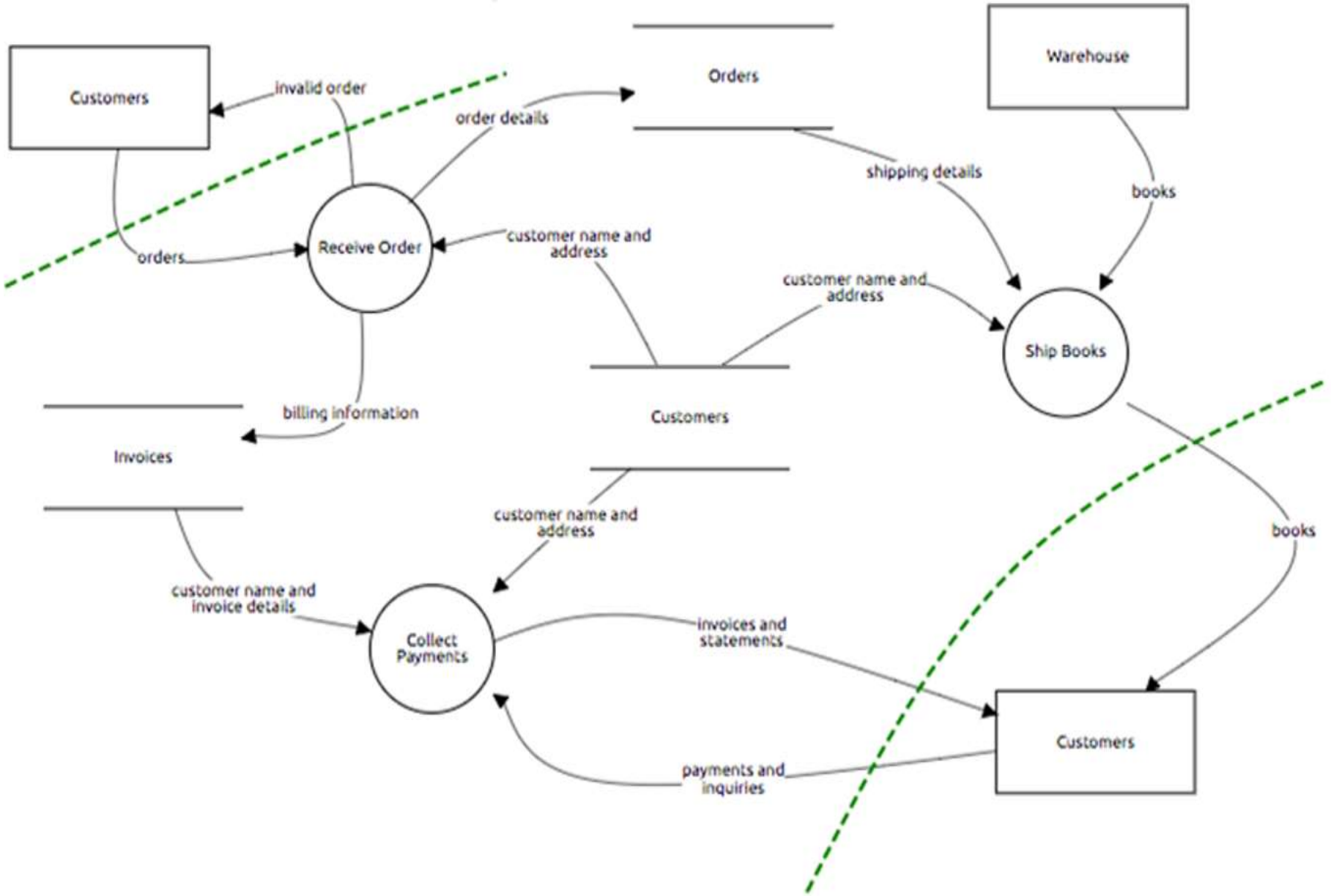
- Receive and review all artifacts
- Review the interview notes made by your colleagues

Create a component diagram

- OK to "flag" assets, controls, etc.
- **Only draw a component / DFD diagram now!!**

Duration: 20 minutes (includes 10 min. to review)

RareBooksRUs DFD



Threat Modeling Lab 2: Identify threats

Identify threats - STRIDE

STRIDE

Threat	Description	Breaks
Spoofing	Pretending to be somebody else	Authentication
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 supposed to do	Authorization

Identity threats - Games

OWASP Cornucopia

Suits:

Data validation and encoding

Authentication

Session Management

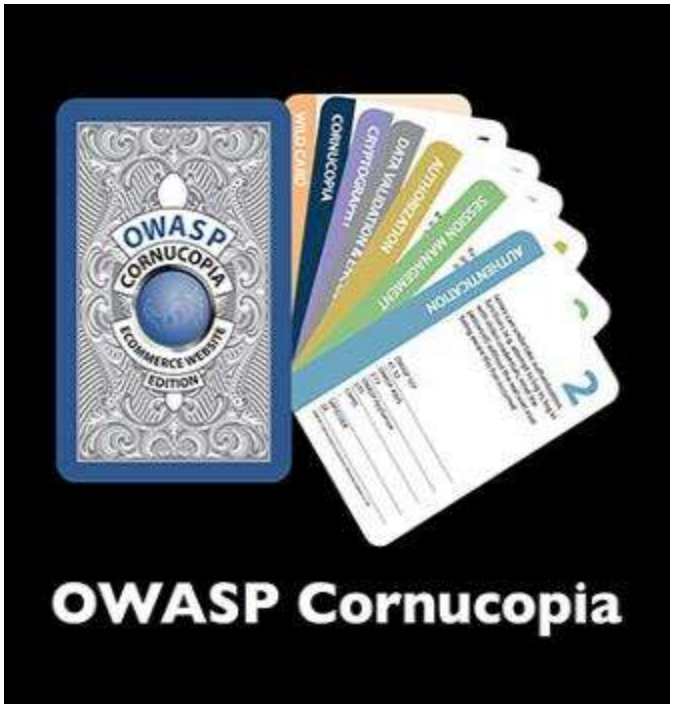
Authorization

Cryptography

Cornucopia

13 cards per suit, 2 Jokers

Play a round, highest value wins



Identity threats - Games

Elevation of Privilege (EoP)

The EoP game focuses on the following threats (STRIDE):

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Identify threats

Base your work on **ONLY** the provided system model diagram!

Add threat possibilities to the model:

- Using STRIDE or other methods

Duration: 20 minutes (includes 10 min. to review)

Threat Modeling Lab 3: Determine mitigations

Determine mitigations

Base your work on **ONLY** the provided system model diagram!

Add mitigations to the model:

- Security controls

Duration: 20 minutes (includes 10 min. to review)

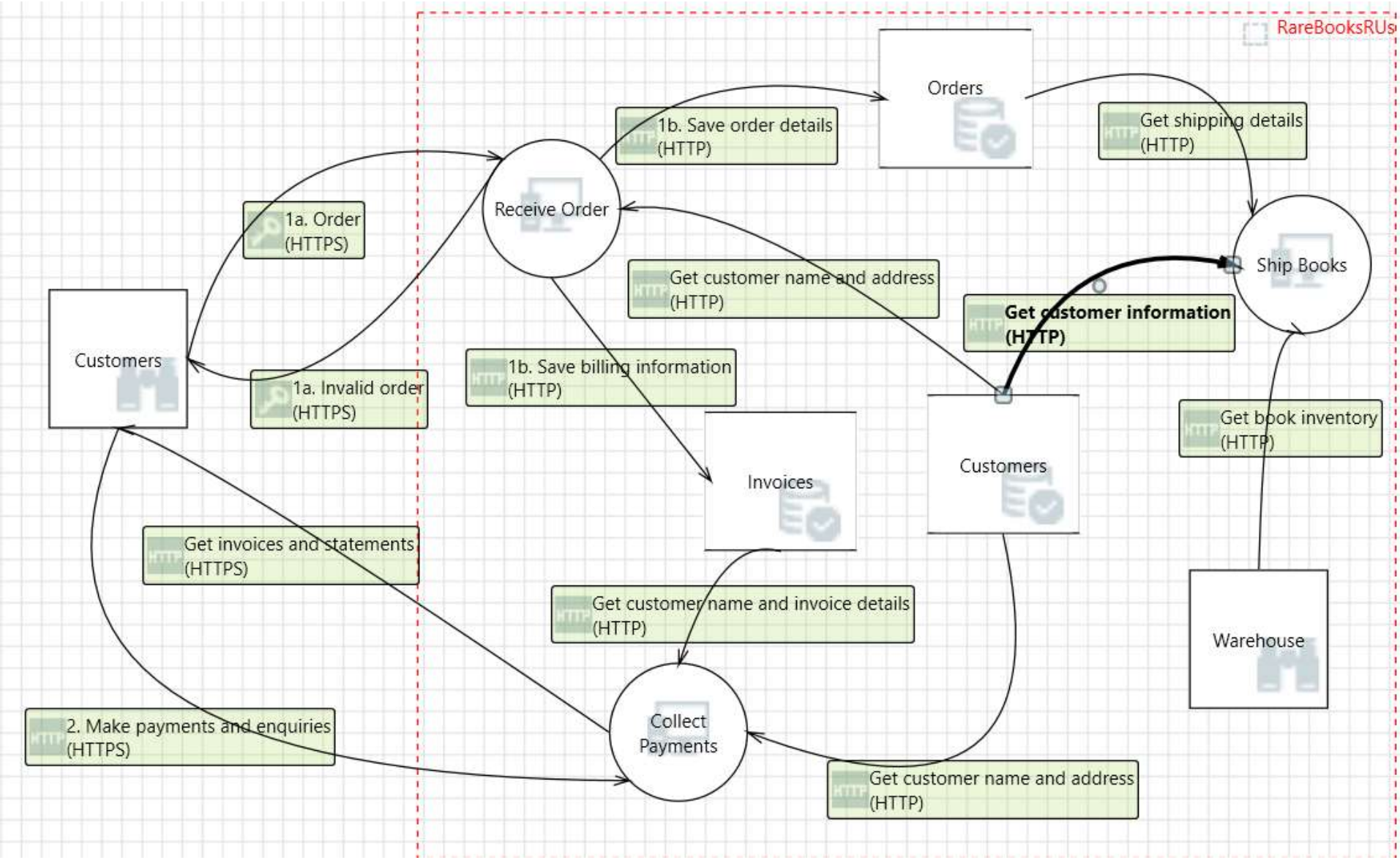
Review

Let’s review the threat models:

How different was each group’s interpretation of the system?

What areas were identified where you need to get additional information?

MS Threat Modeling Tool – RareBooksRUs DFD



Resources – Threat Modeling Manifesto

"Threat Modeling Manifesto" (2020)

https://threatmodelingmanifesto.org/

- Definition
- Values
- Principles
- Anti-Patterns

Resources – Threat Modeling Connect

Threat Modeling Connect (started Fall, 2022)

https://www.threatmodelingconnect.com/

- Support and insights from other Threat Modelers
- Monthly Community Meetups
- Threat Modeling Hackathons
- Threat Modeling Open Forum
- First Threat Modeling Conference – November, 2023

Resources - Books

Threat Modeling as a Practice:

Threat Modeling: A Practical Guide for Development Teams (2020)
Izar Tarandach and Matthew Coles

Threat Modeling: Designing for Security (2014)
and
Threats: What Every Engineer Should Learn from Star Wars (2023)
Adam Shostack

Securing Systems: Applied Architecture and Threat Models (2015)
Brook S.E. Schoenfield

Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis (2015)
Marco Morana and Tony UcedaVelez

Resources - Books

Applied Threat Modeling:

Hacking Kubernetes: Threat-Driven Analysis and Defense (2021)
Andrew Martin, Michael Hausenblas

Playbook for Threat Modeling Medical Devices (2021)
MITRE: https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf

Resources - Tools

Microsoft Threat Modeling Tool

https://aka.ms/threatmodelingtool

ThreatModeler – Web Based (in-house) Tool

https://threatmodeler.com

IriusRisk Software Risk Manager

https://iriusrisk.com

OWASP Threat Dragon

https://owasp.org/www-project-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

Questions?

@RobertHurlbut

Thank you!