Hands-On Threat Modeling Workshop

Tue, 1/14/2025 8:00 am – Sandusky, Ohio, United States

Robert Hurlbut

CodeMash 2025

Labs

ROBERT HURLBUT

JANUARY 14, 2025

Who am I?

X (*Twitter*): @RobertHurlbut
BlueSky: roberthurlbut.bsky.social
LinkedIn: roberthurlbut

Robert Hurlbut

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

- Microsoft MVP – Dev Sec / Dev Tech
- (ISC2) CSSLP
- Boston Code Camp – Co-Organizer
- Boston .NET Architecture Group – Founder / Leader
- Amherst Security Group – Leader
- Application Security Podcast – Co-Host
- "Threat Modeling Manifesto" – Co-Author
- "Threat Modeling Capabilities" – Co-Author
- Threat Modeling Connect – Co-Founding Member
- Expert Witness (Threat Modeling, Cybersecurity)
- Ph.D. Student – Space Cybersecurity

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 an 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 are not likely to happen right away

Rare Books R Us

Fictitious mail-order bookseller specializing in rare and old book titles

Launching website: **Rare Books R Us**

Security is essential, but they need help in determining where it is needed

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

The company is also looking to move most of the data and operations to the cloud and may add a mobile app

Rare Books R Us

Business Goals:

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

Technical Goals:

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

Rare Books R Us

Data Stores:

Customers DB

Orders DB

Invoices DB

Users:

Customers (external)

Warehouse Staff (internal)

Processes:

Orders API

Billing API

Payments API

Data Flows:

Save Orders

Add Billing

Process Payments

Etc.

Data Flow Diagram (DFD)

DFD Elements

External Entity	The external entity shape is used to represent any entity outside the application that interacts with the application via an entry point
Process	Represents a task that handles data within the application. The task may process the data or perform an action based on the
Multiple Process	Used to present a collection of subprocesses. The multiple process can be broken down into its subprocesses in another DFD.
Data Store	Represents locations where data is stored
Data Flow	Represents data movement within the application. The direction of the data movement is represented by the arrow.
Privilege Boundary	Represent the change of privilege levels as the data flows through the application.

Model the system

To model the system:

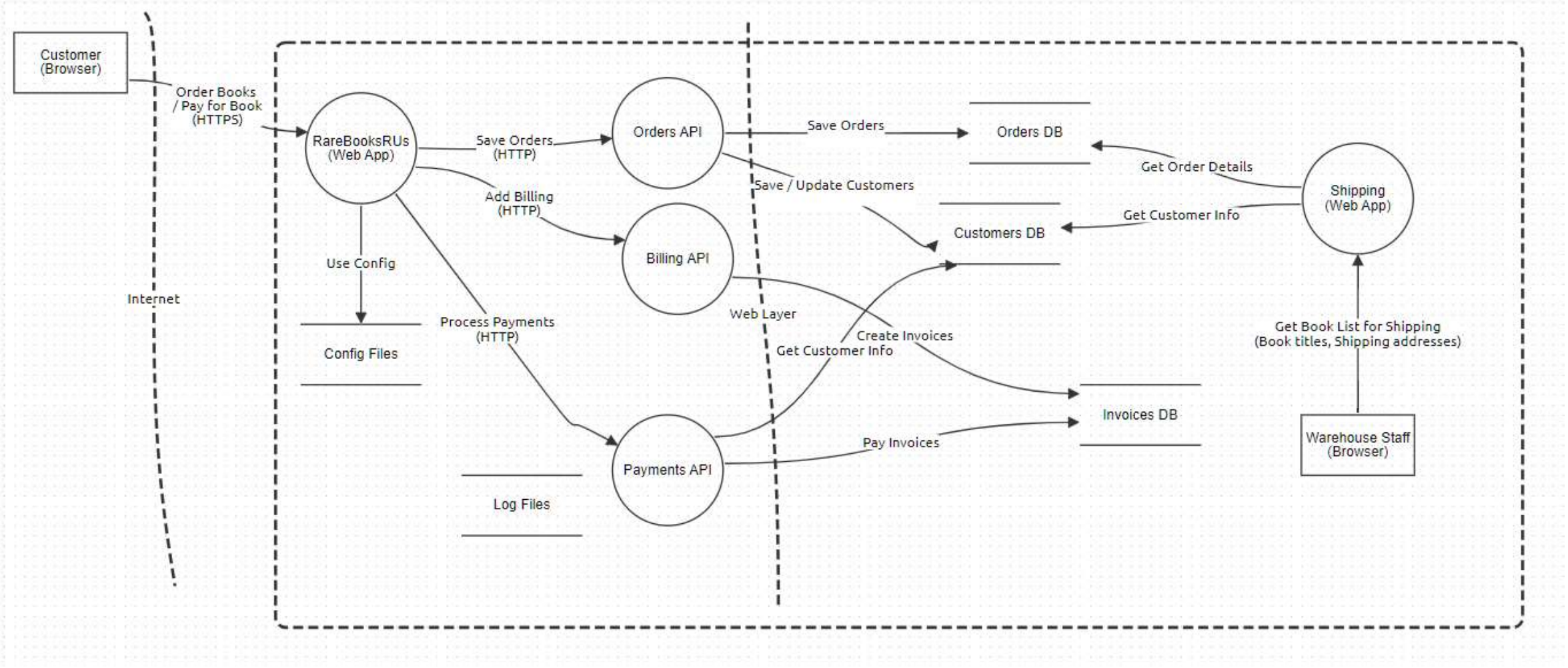
- Receive and review all artifacts
- Review the interview notes made by your colleagues

Create a component diagram

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

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

RareBooksRUs DFD Web-Onlv v1.0



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

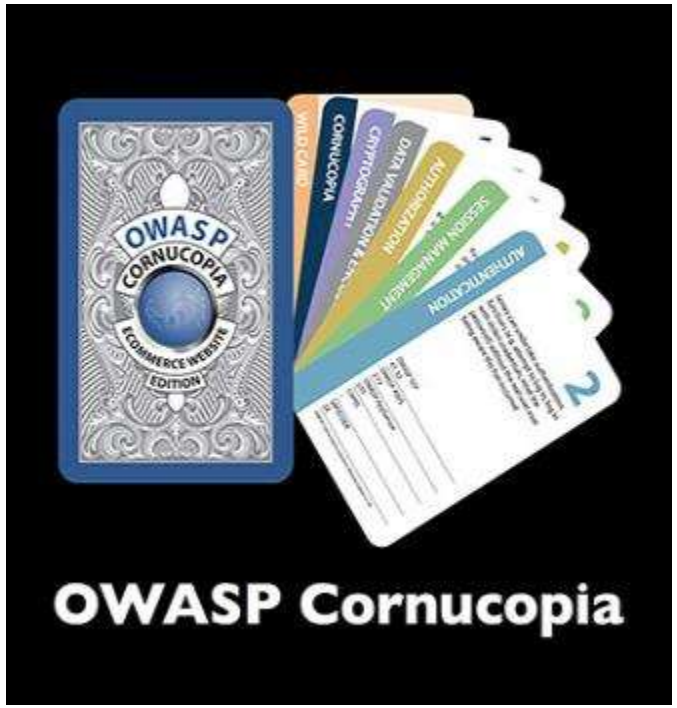
Authorization

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:

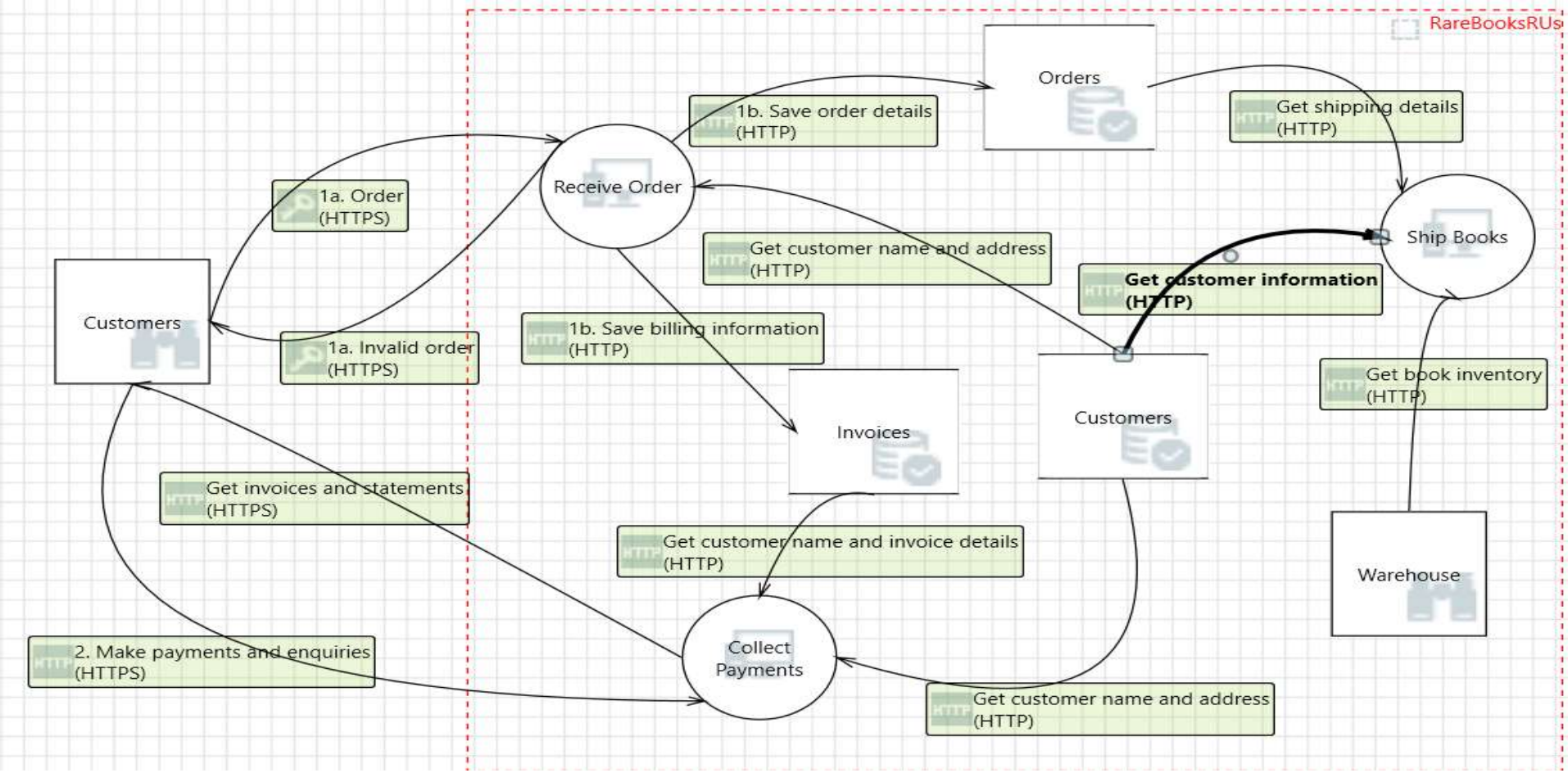
- Using STRIDE or other methods

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

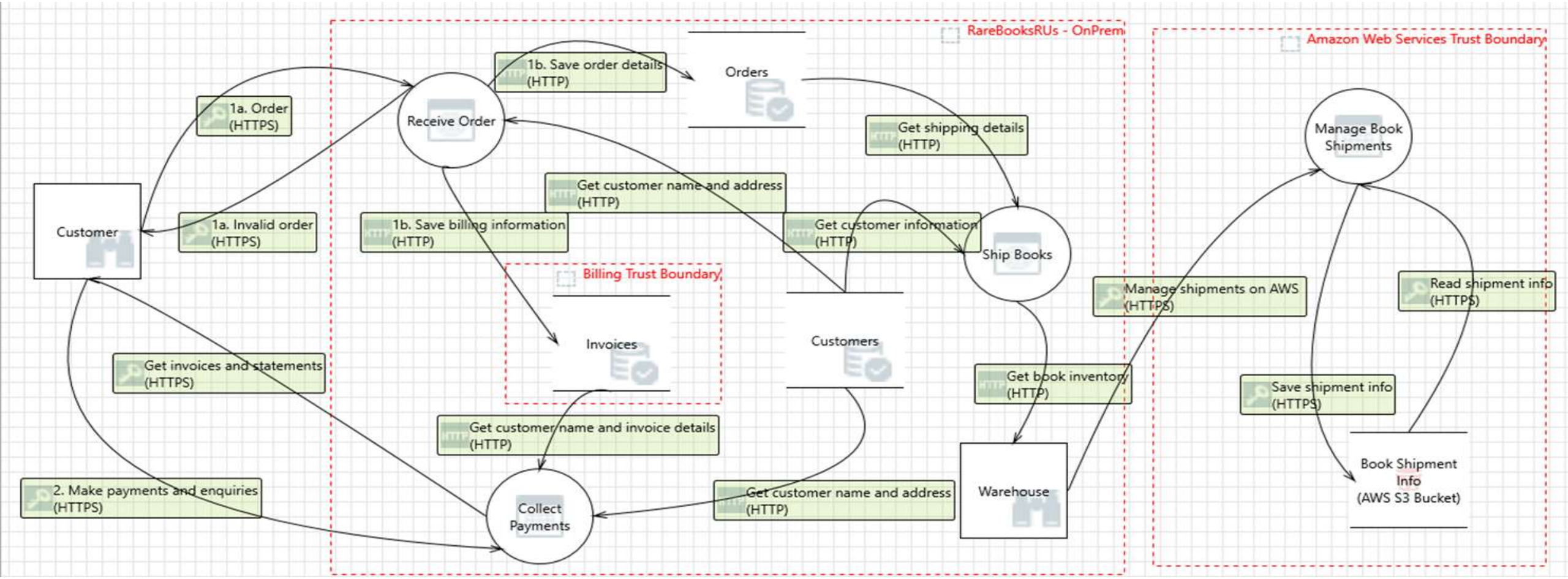
Threat Table

Threat	STRIDE	Mitigation / Risk	Review / Action Items

MS Threat Modeling Tool – RareBooksRUs DFD



MS Threat Modeling Tool – RareBooksRUs DFD – w/ AWS



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

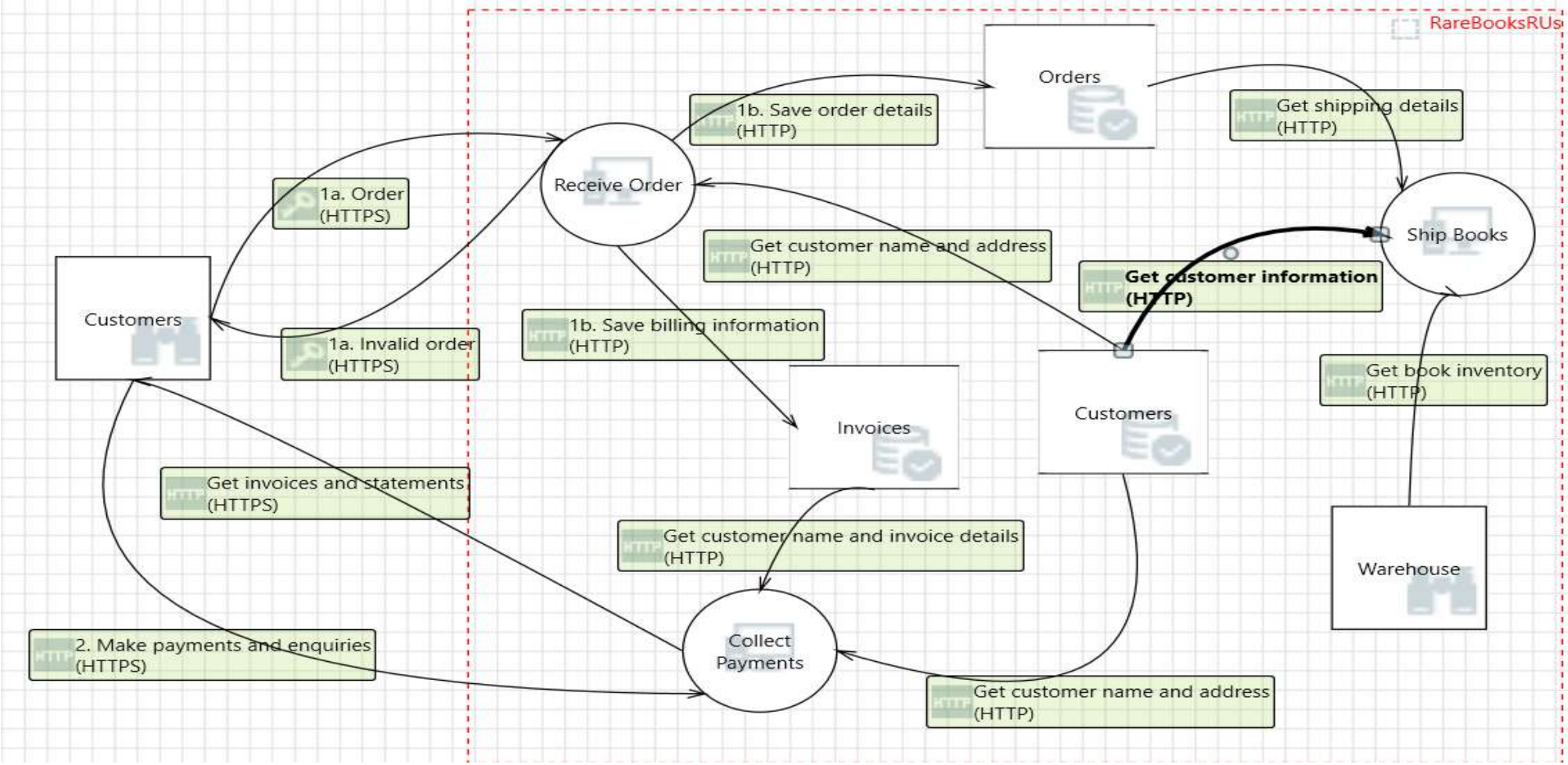
Duration: 20 minutes (includes 10 min. to review)

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



MS Threat Modeling Tool – RareBooksRUs DFD – w/ AWS