Threat Modeling Workshop

Threat Modeling Using OWASP Threat Dragon

AppSecUSA 2017 – Developer Summit

Robert Hurlbut

OWASP
The Open Web Application Security Project

OWASP
AppSec USA
ORLANDO
2017

Robert Hurlbut

Software Security Consultant, Architect, and Trainer

Microsoft MVP – Developer Security 2005-2010, 2015-2018

(ISC)2 CSSLP 2014-2017

Co-host Application Security Podcast (@appsecpodcast)

Contacts

Web Site: https://roberthurlbut.com

LinkedIn: RobertHurlbut

Twitter: @RobertHurlbut

OWASP
AppSec USA
ORLANDO
2017

RH ROBERT HURLBUT
CONSULTING SERVICES

OWASP Threat Dragon

OWASP Incubator Project – early 2017

Project Leader: Mike Goodwin (@theblacklabguy)

OWASP Threat Dragon

- https://www.owasp.org/index.php/OWASP_Threat_Dragon

Links – Source, Threat Dragon Live, Docs

- https://github.com/mike-goodwin/owasp-threat-dragon
- https://threatdragon.org/
- http://docs.threatdragon.org

Featured on AppSecPodcast (S02E06) 6/27/2017

- https://www.appsecpodcast.org/2017/06/27/the-girl-with-the-owasp-threat-dragon-tattoo-s02e06/

OWASP Threat Dragon

OWASP
The Open Web Application Security Project

Free, open-source, threat modelling web application for teams implementing the STRIDE approach

Key Areas:

- **Great UX** - using Threat Dragon should be simple, engaging and fun
- **A powerful threat/mitigation rule engine** - lowers barrier to entry for teams and allows non-specialists to contribute
- **Integration points with other development lifecycle tools** - ensures models slot easily into development lifecycle and remain relevant as the project evolves

OWASP Threat Dragon

Uses Angular JS, Node JS

Web-based app integrates with GitHub account – saves models to GitHub

Desktop Installation (Using Electron - Windows / Mac versions) – saves models to file system

It is still in the “alpha” stage, so still “rough”

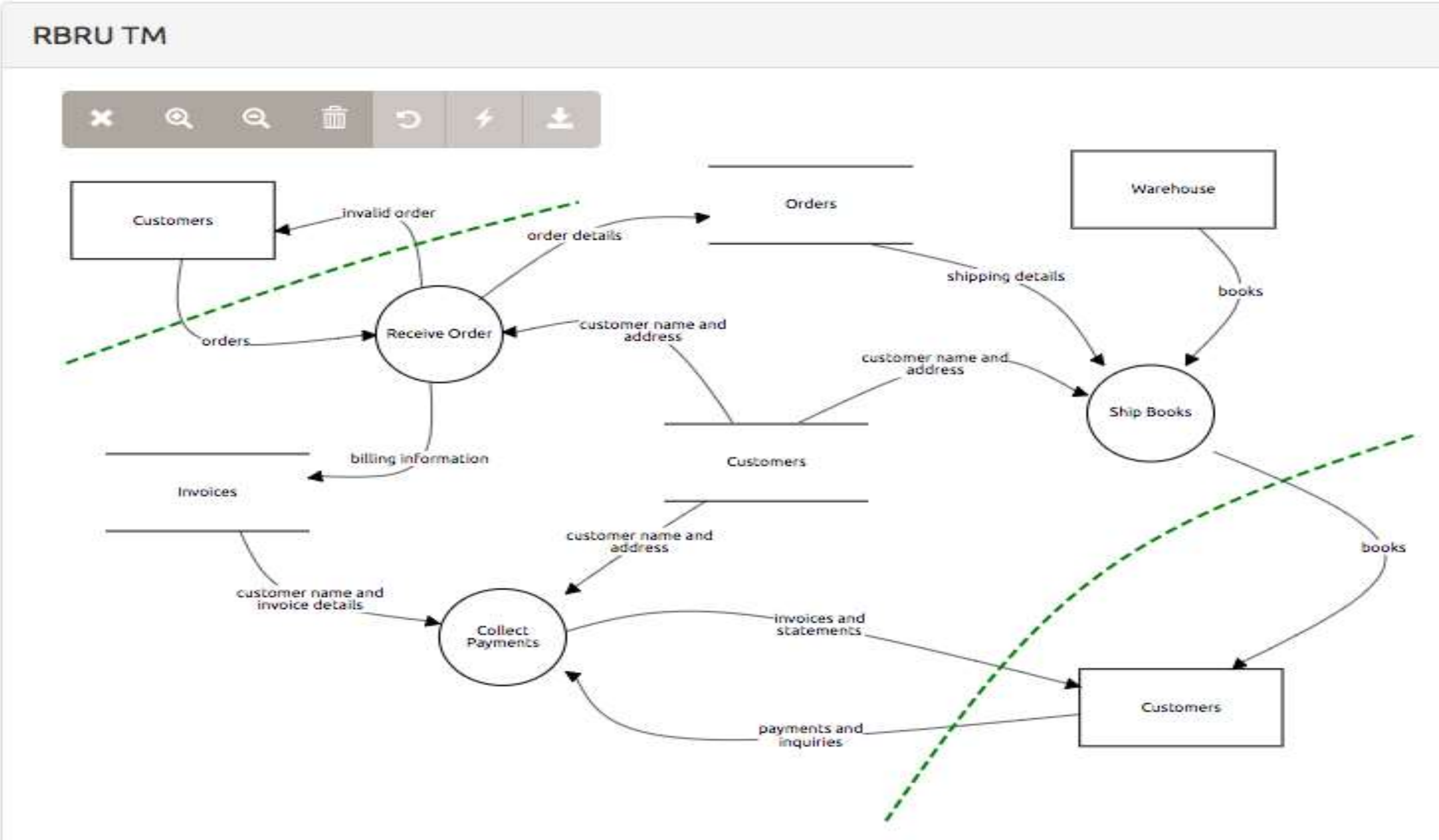
Take if for a spin – give feedback

Needs:

> Threat Modeling practitioners use it / test it / give feedback
>
> Developers help / join dev team

Threat Dragon – RBRU TM

OWASP
The Open Web Application Security Project



RBRU TM

Resources - Tools

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 Proactive Controls 2016

https://www.owasp.org/index.php/OWASP_Proactive_Controls

Questions?

OWASP
The Open Web Application Security Project

Slides at:

https://bit.ly/RHTMwTD

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut

ROBERT HURLBUT
CONSULTING SERVICES