OWASP

The Open Web Application Security Project

OWASP Threat Dragon

An OWASP *thumbs-up* incubator project

Jon Gadsden

- ForgeRock: Identity and Access Management
- Embedded software and security engineer
- Contributor to OWASP Threat Dragon project

OWASP Threat Dragon project

- Context in the SDLC
- What is threat modeling
- Modeling with Threat Dragon
- Short demo

OWASP secure software development lifecycle

- Training: secure coding and security training
- Requirements: risk evaluation and requirements
- Design: security reviews and threat modeling
- Implement : secure coding and testing
- Validation : penetration and security testing
- Release/maintenance : vulnerability management and incident response

- Vulnerability

  an exploitable weakness in a system or its design

- Asset

  anything that is valuable to an organization

- Threat

  potential danger to an asset

- Vector

  method to realise an exploit

- Trust boundary
- *change in level of trust for information or execution*

STRIDE and DREAD

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**levation of privilages

- **D**amage
- **R**eproducibility
- **E**xploitability
- **A**ffected users
- **-D**iscoverability

Some threats can never be modeled

- Government agencies
- Service provider
- Back doors
- Wet ware (the human)

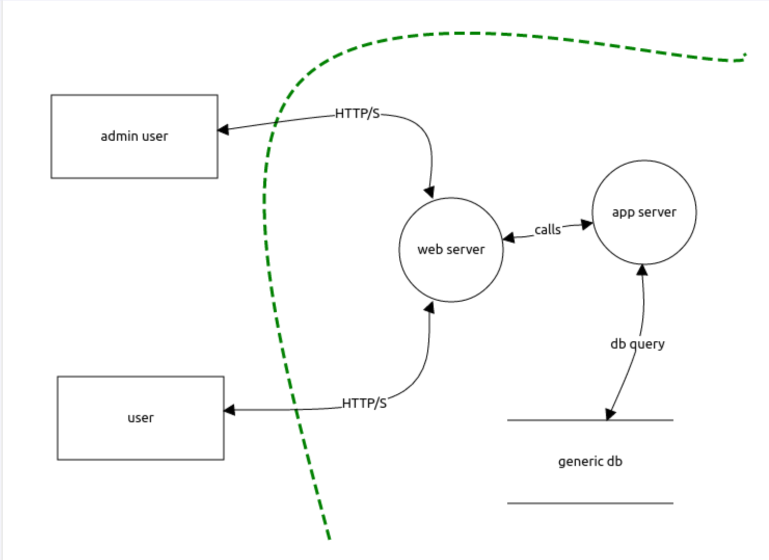
- Microsoft Threat Modeling Tool (TMT)
- OWASP Threat Dragon
- PyTM
- *Mozilla Sea Sponge*
- *Trike* – Tryke!

- Proprietary (IriusRisk, cisco Threat Builder, etc)

Threat Dragon (0.1.26)

- Free, open source threat modeling tool
- OWASP incubator project
- Web application
- Desktop application for local use
- Mike Goodwin

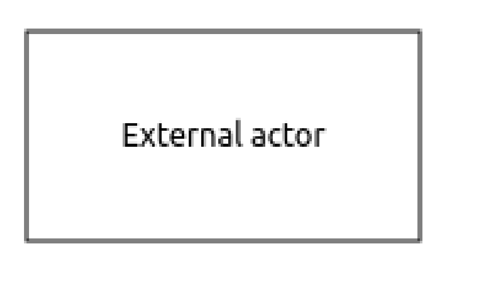
Threat model is a data flow diagram that



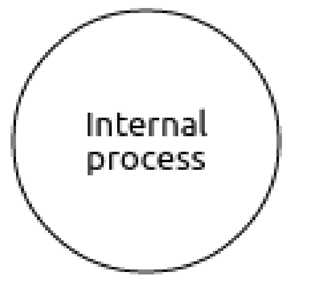
- Analyses security requirements
- Reduces attack surface

Threat Model components

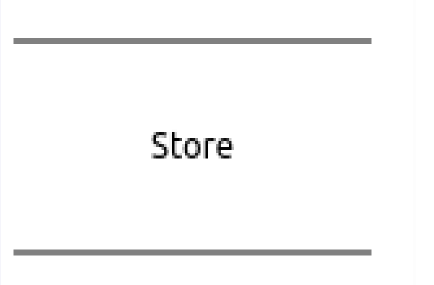
Actor



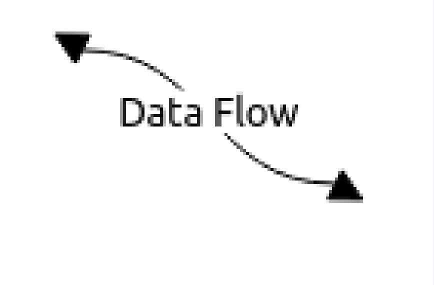
Process



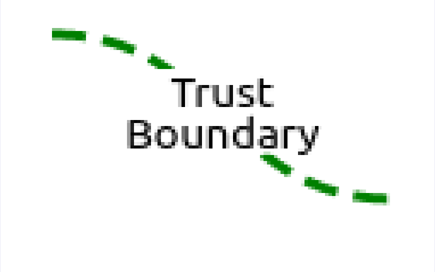
Storage

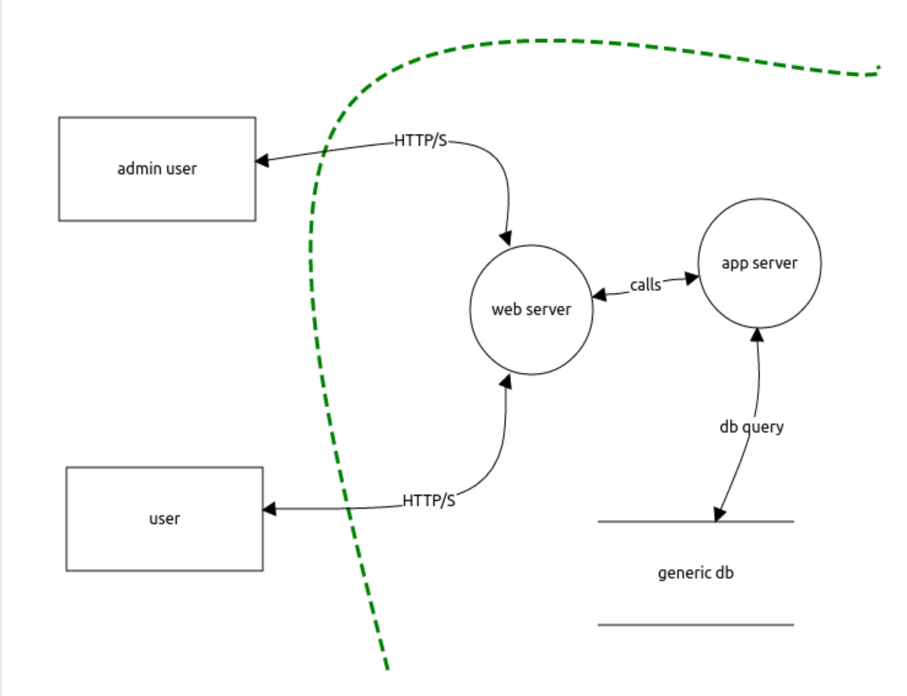


Data flow



Trust boundary





- It is not a system diagram
- Keep it simple
- Think hard before modeling existing systems
- Incremental threat modeling
- It is not a system diagram

- Contribute
- Have a github account?
- Node.js
- Angular
- Electron
- MongoDB (well, not yet)

Demo time!