INTRO TO THREAT MODELING

Designing for Security

By Avi Douglen

Bounce SECURITY

About… Avi Douglen

- Email: AviD@BounceSecurity.com
- Twitter: @sec_tigger
- He / Him

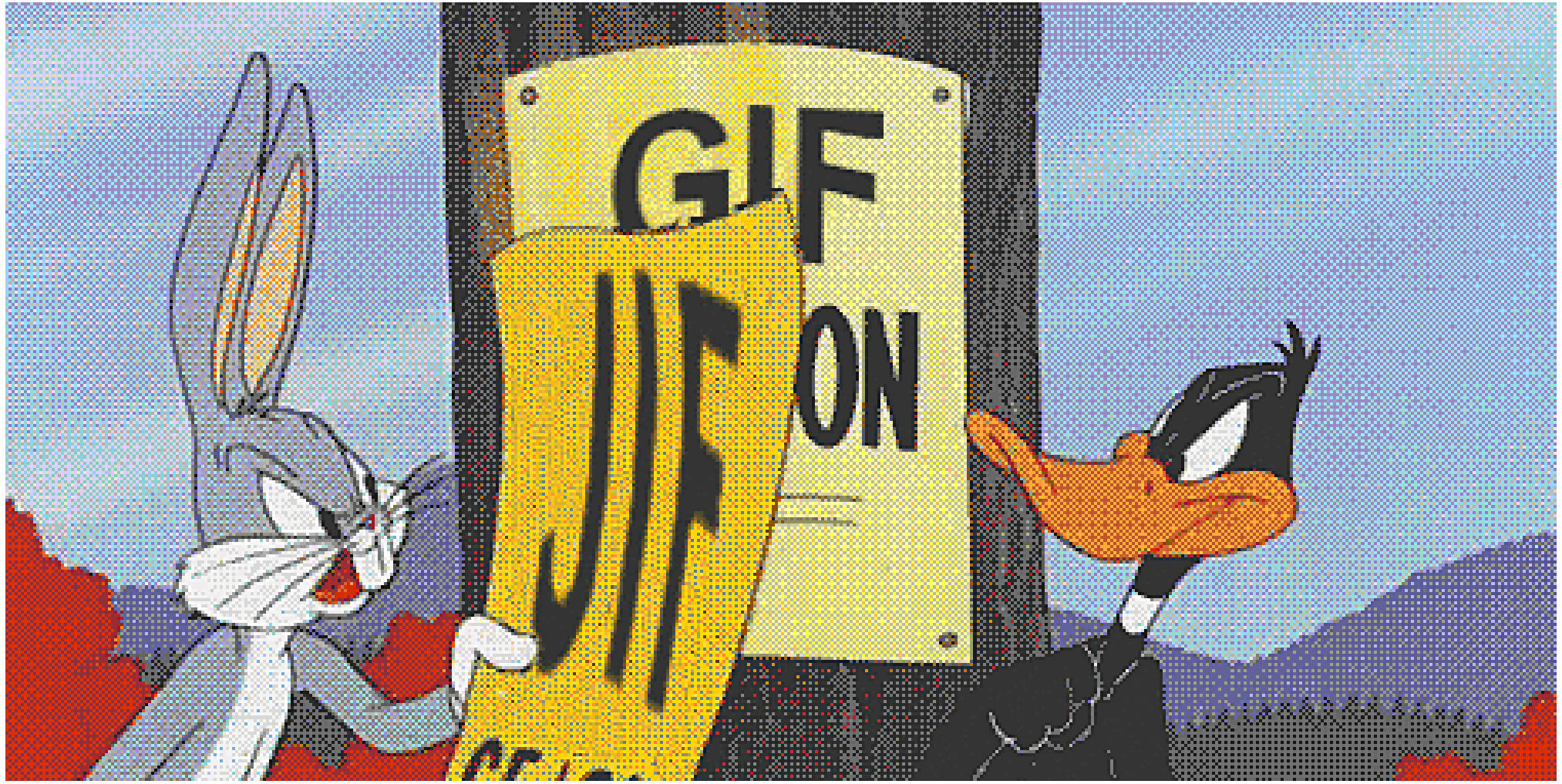
- The important things:
  - *Whisky: smokey*
  - *Beer: stout*
  - *Coffee: black*

- Software Security @ Bounce SECURITY
- Researcher / Developer / Architect
- Advisor at OurCrowd Labs/02
- OWASP Israel Leader
- Threat Model Project Leader
- Moderator Security.StackExchange

Agenda

- Why Threat Modeling
- What Threat Modeling
- How Threat Modeling
- Who Threat Modeling
- When Threat Modeling

The Eternal Conundrum…

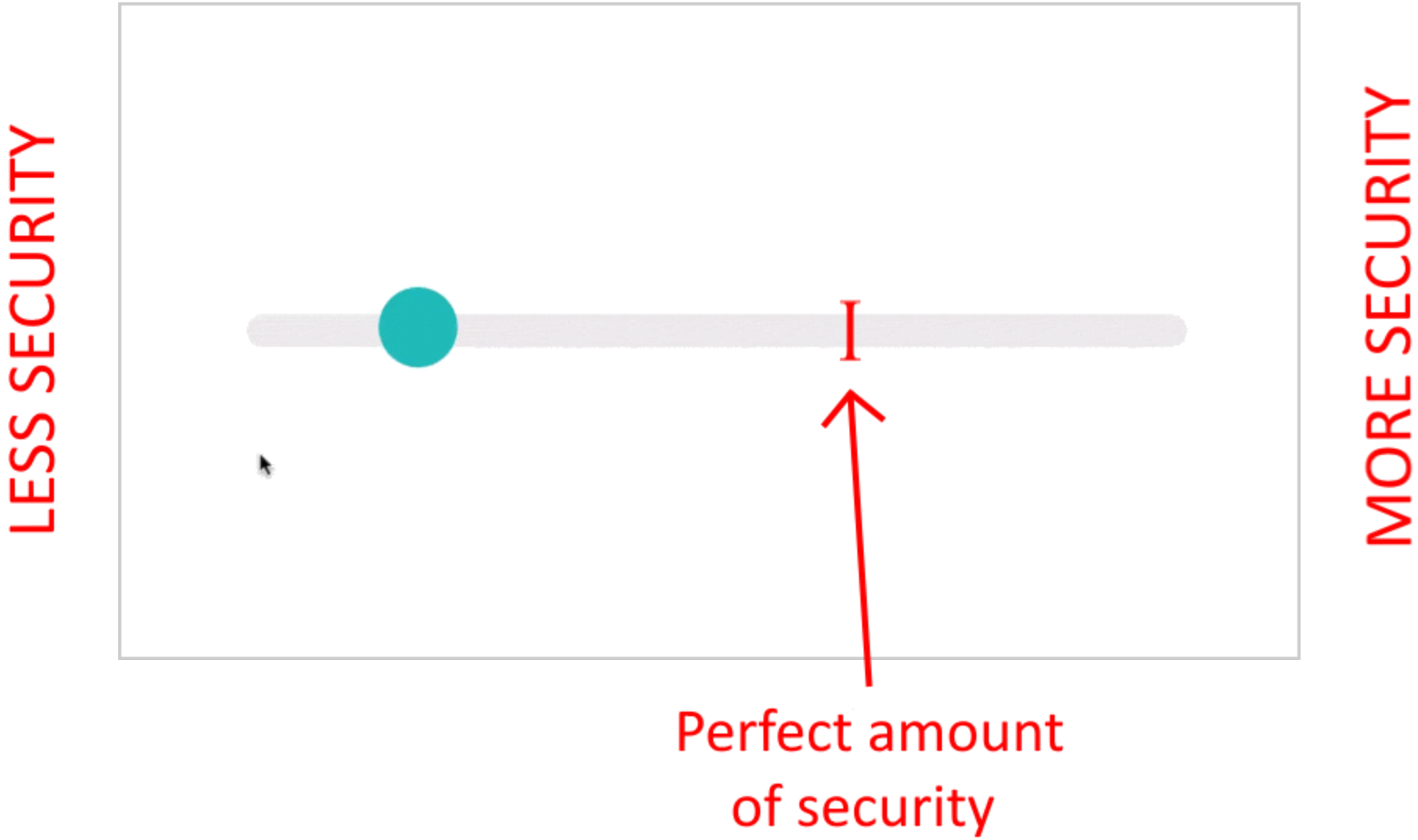


Bounce
SECURITY

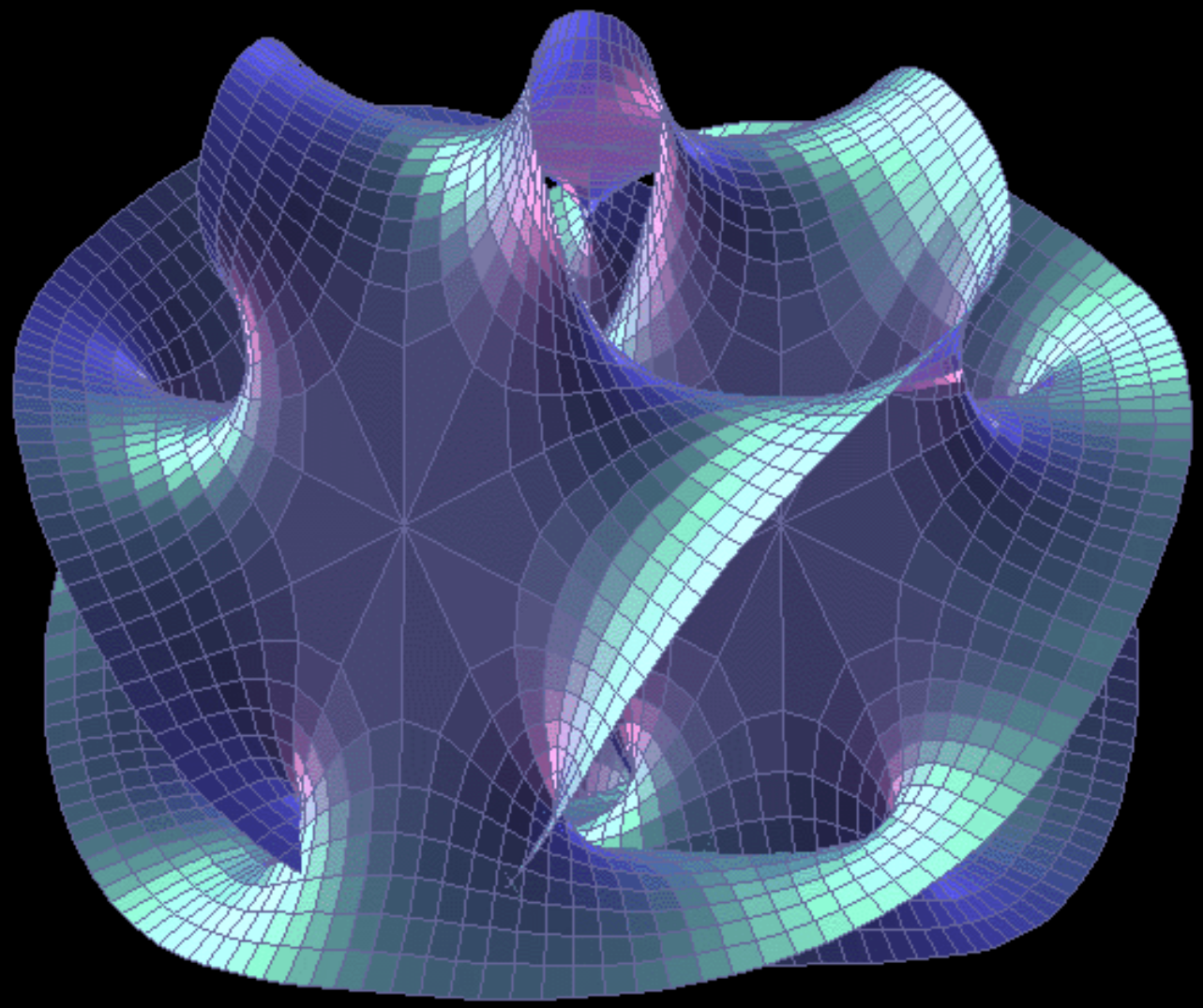
How Secure is Secure *Enough* ??

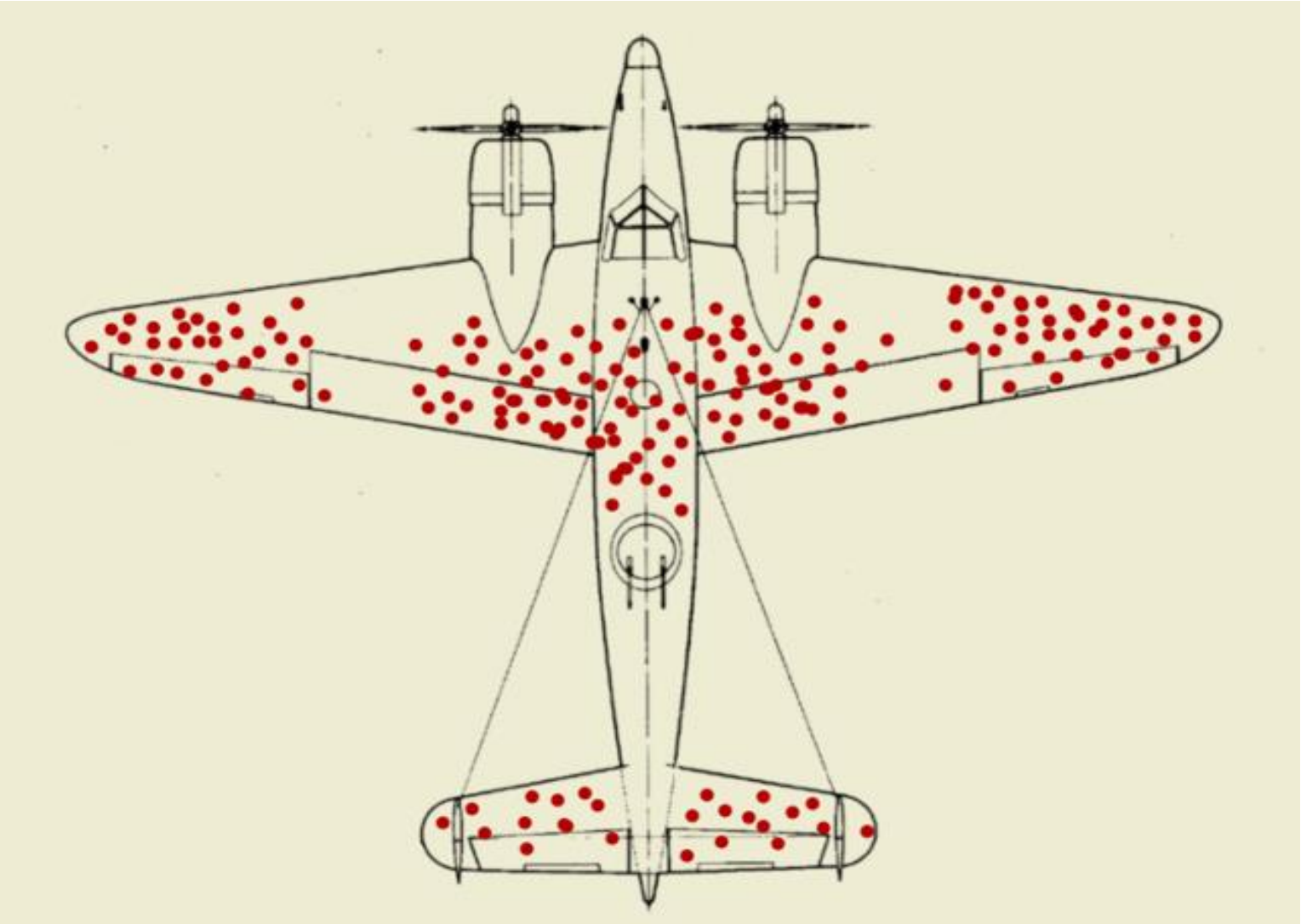
- How much time / resources to invest in security?
- Spend too much = WASTE
- Spend too little = BREACHED
  - *(or worse, fined)*
- … Or maybe it's both??
- The crutch of generic "Best Practices"

Bounce SECURITY



Bounce
SECURITY





Bounce
SECURITY

What does “secure” even mean?

- When you don’t get hacked?
- What are you protecting?
- How are you being attacked?
- Who is attacking you?
- Why are they targeting you?

Bounce SECURITY

Why it is Important

- Most systems have exploitable vulnerabilities
- Customers are demanding secure systems
- Best to build on a secure design
- Find security issues without a line of code
- Shared understanding of system security
- How much time is wasted:
  - *building unneeded security features*
  - *patching critically broken security*

Security is YOUR Responsibility

- Essential non-functional requirements
- Less work now vs. more work later
- Which “security” to work on?
- Own your products security
- Threat modeling helps focus efficient work

Bounce SECURITY

The Threat Modeling Approach

Bounce SECURITY

Enter Threat Modeling

- Structured security-based analysis
- Framework to understand threats
- Review of design elements
- Prioritize mitigations by risk

Bounce SECURITY

Common Approaches

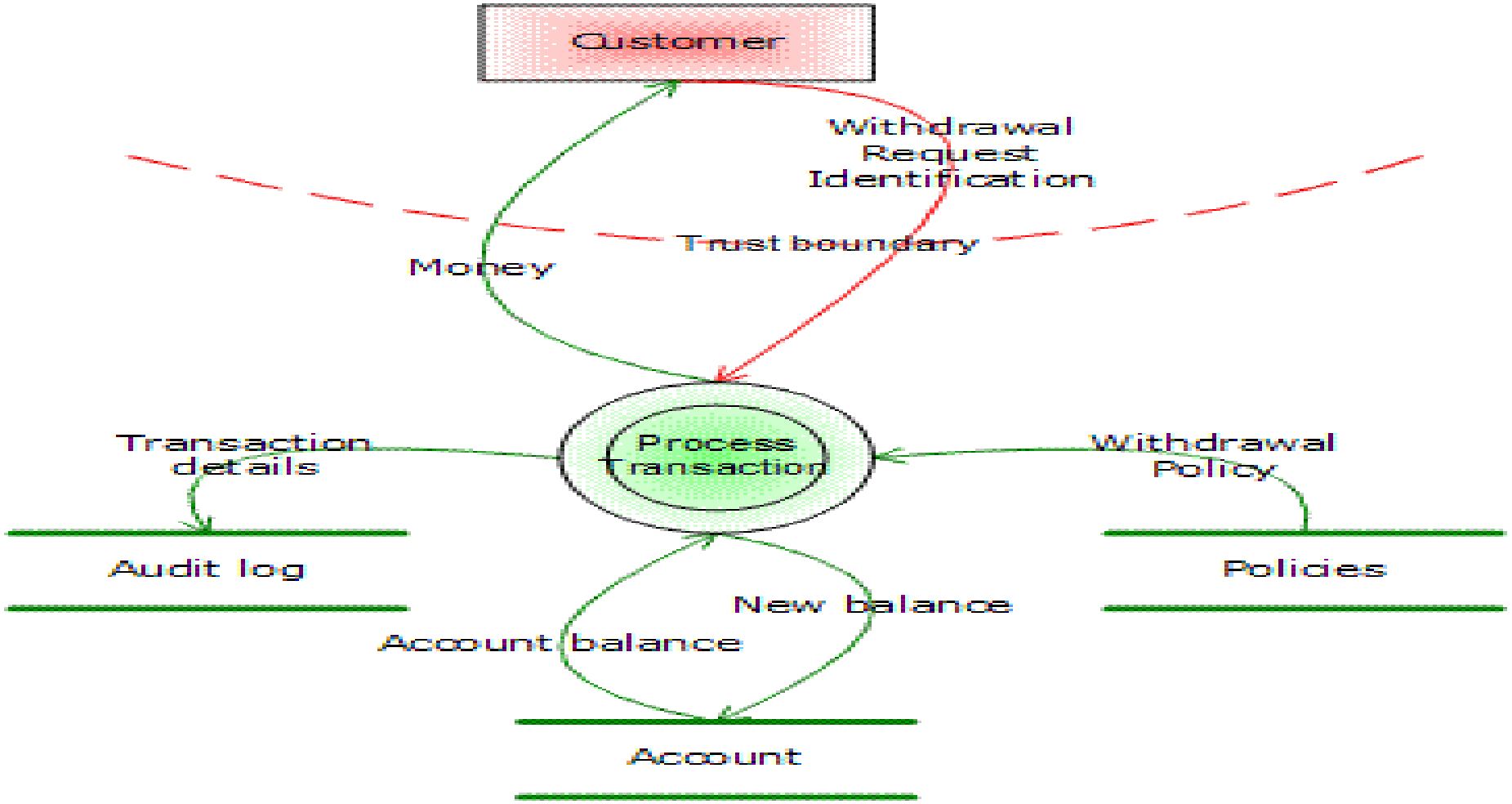
- Software centric
- Asset centric
- Attacker centric
- Risk based
- Value driven

Threat Modeling Framework

- Thanks to Adam Shostack

- What are we building?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

Data Flow Diagram



Bounce
SECURITY

The Process

Phase #0 – Scope the model

Phase #1 – Decompose the application

Phase #2 – Identify the threats

Phase #3 – Determine countermeasures

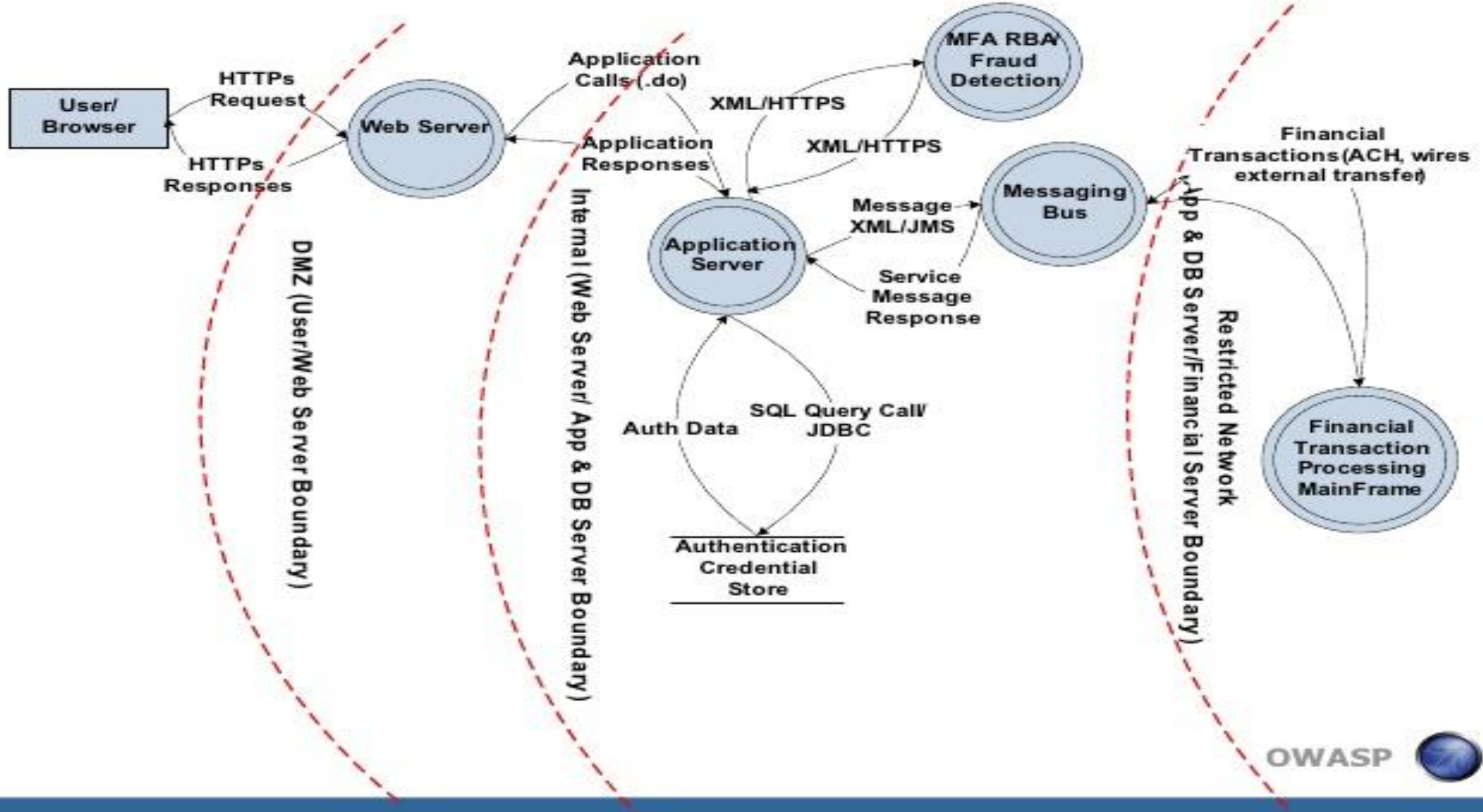
Phase #4 – Analyze result

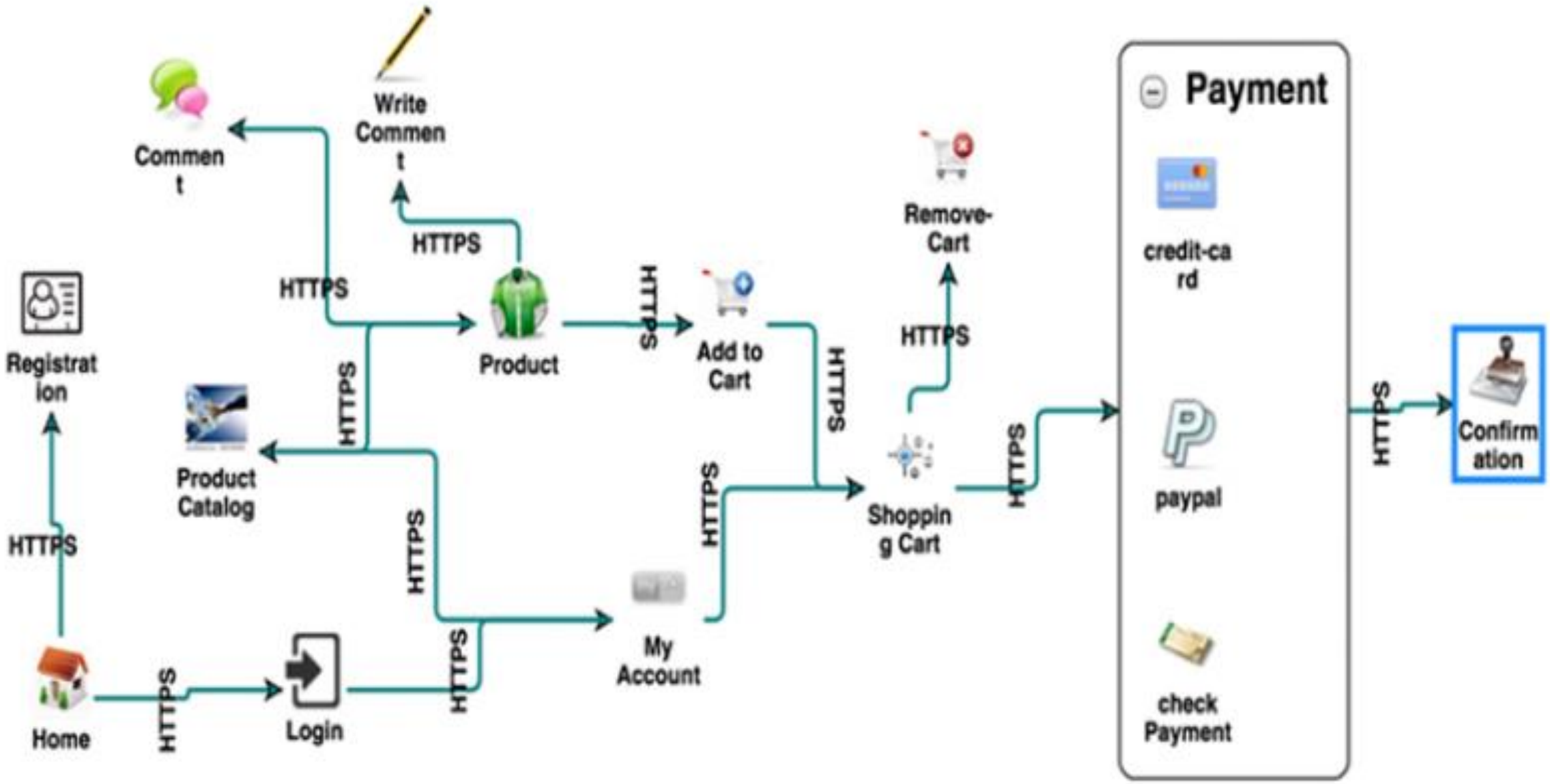
STRIDE Per-Element

Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privileges

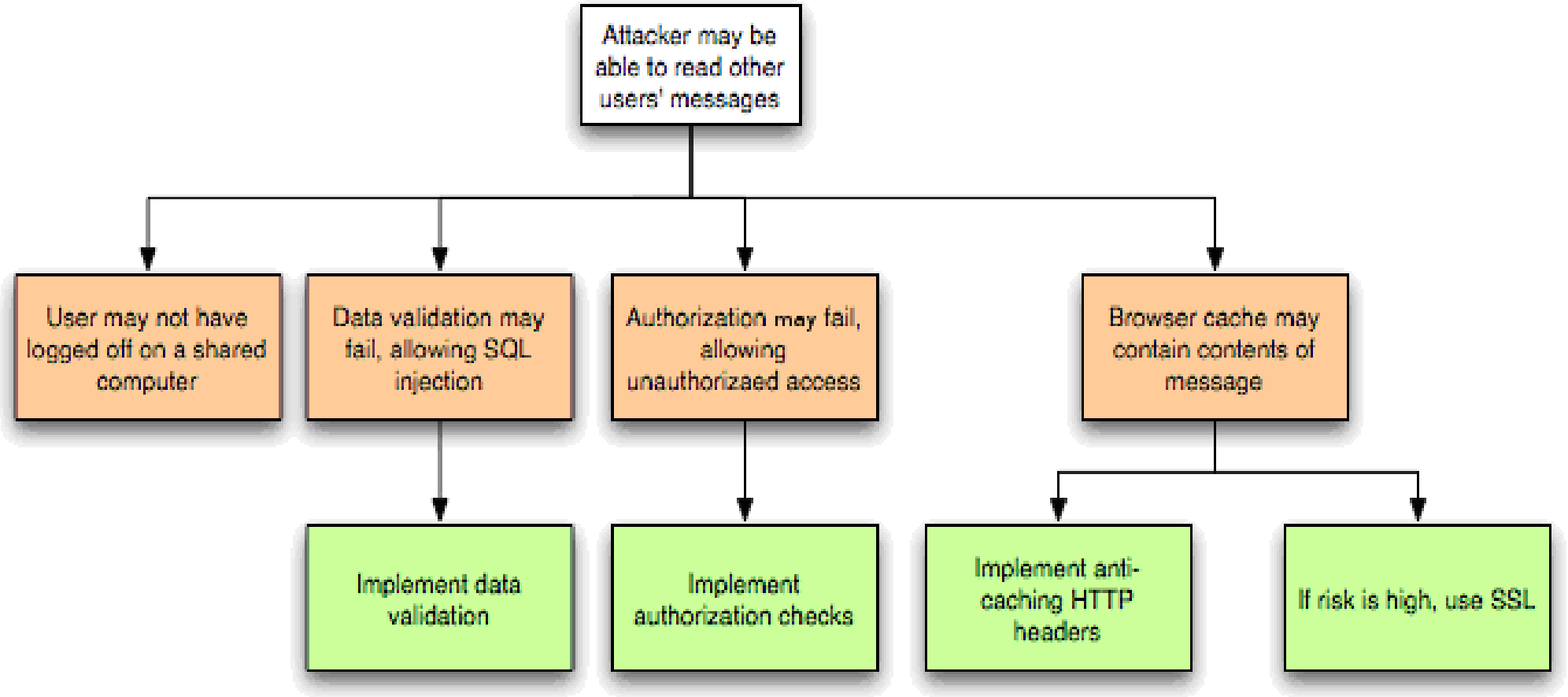
Bounce SECURITY

Data flow diagram-Online Banking Application




Commen
t
Write
Commen
t
HTTPS
HTTPS
Registrat
ion
Product
HTTPS
Add to
Cart
HTTPS
Remove-
Cart
HTTPS
Payment
credit-ca
rd
Product
Catalog
HTTPS
HTTPS
Shoppin
g Cart
HTTPS
paypal
HTTPS
Confirm
ation
HTTPS
HTTPS
My
Account
HTTPS
Home
HTTPS
Login
HTTPS
check
Payment

Attack Trees



Bounce SECURITY

P.A.S.T.A

- **P**rocess for **A**ttack **S**imulation and **T**hreat **A**nalysis
- Risk-Based Methodology for higher assurance

- Seven stage process:

1. Define Objectives

- Identify Business Objectives
- Identify Security & Compliance Requirements
- Business Impact Analysis

2. Define Technical Scope

- Capture the boundaries of the technical environment
- Capture Infrastructure | Application | Software Dependencies

3. Application Decomposition

- Identify Use Cases | Define App Entry Points & Trust levels
- Identify Actors | Assets| Services | Roles| Data Sources
- Data Flow Diagramming (DFDs) | Trust Boundaries

4. Threat Analysis

- Probabilistic Attack Scenarios Analysis
- Regression Analysis on Security Events
- Threat Intelligence Correlation & Analytics

5. Vulnerability & Weakness Analysis

- Queries of Existing Vulnerability Reports & Issues Tracking
- Threat to Existing Vulnerability Mapping Using Threat Trees
- Design Flaw Analysis Using Use & Abuse Cases
- Scorings (CVSS/ CWSS) | Enumerations (CWE/CVE)

6. Attack Modeling

- Attack Surface Analysis
- Attack Tree Development | Attack Library Mgt
- Attack to Vulnerability & Exploit Analysis using Attack Trees

7. Risk & Impact Analysis

- Qualify & quantify business impact
- Countermeasure Identification & Residual Risk
- ID risk mitigation strategies

Bounce SECURITY

From a Developer's Perspective

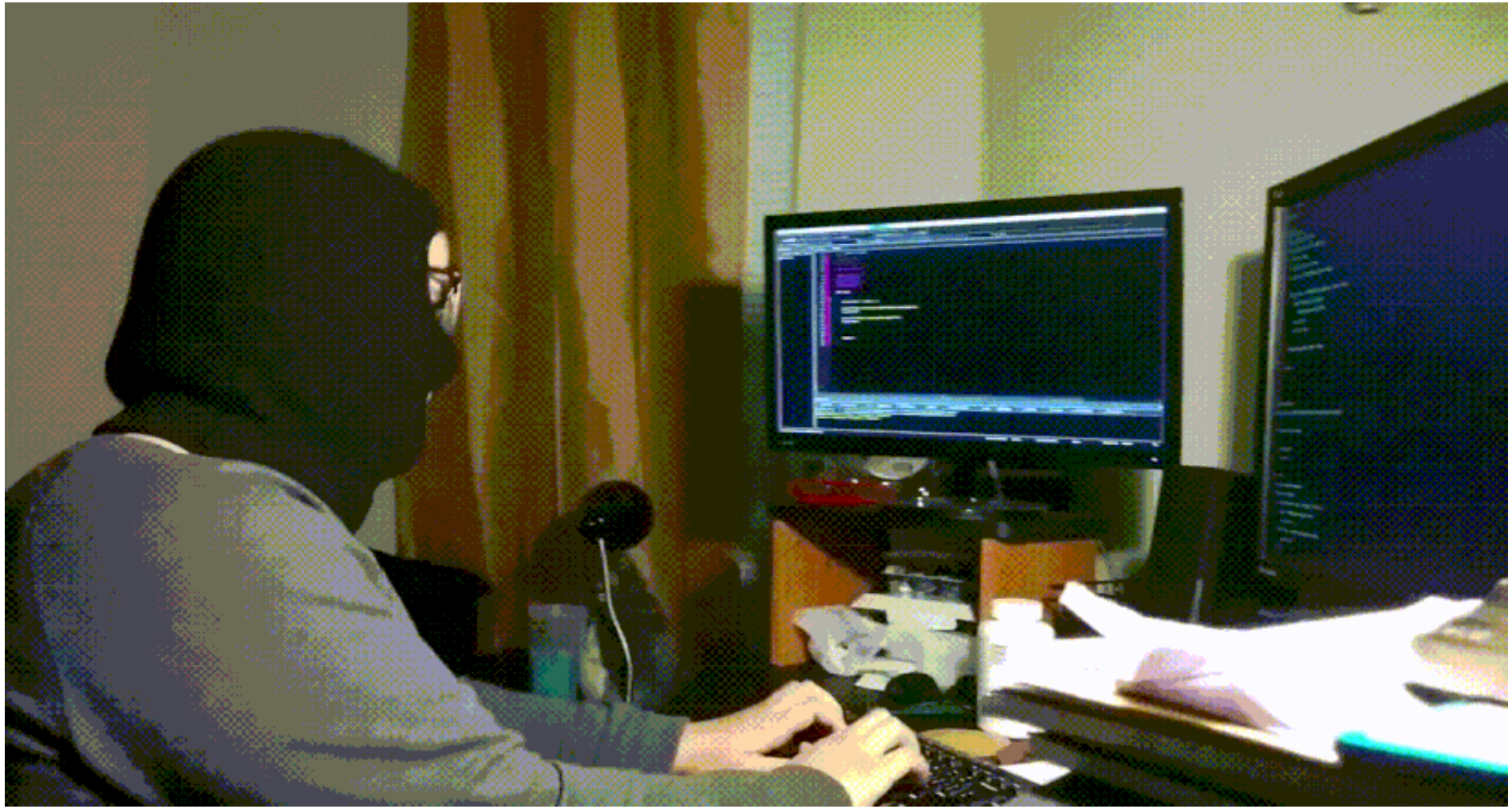
Bounce SECURITY

Takes too much time!

Bounce SECURITY

“Security is everybody’s job”

Bounce SECURITY



“Think like an attacker”

Bounce SECURITY

Threats are obvious

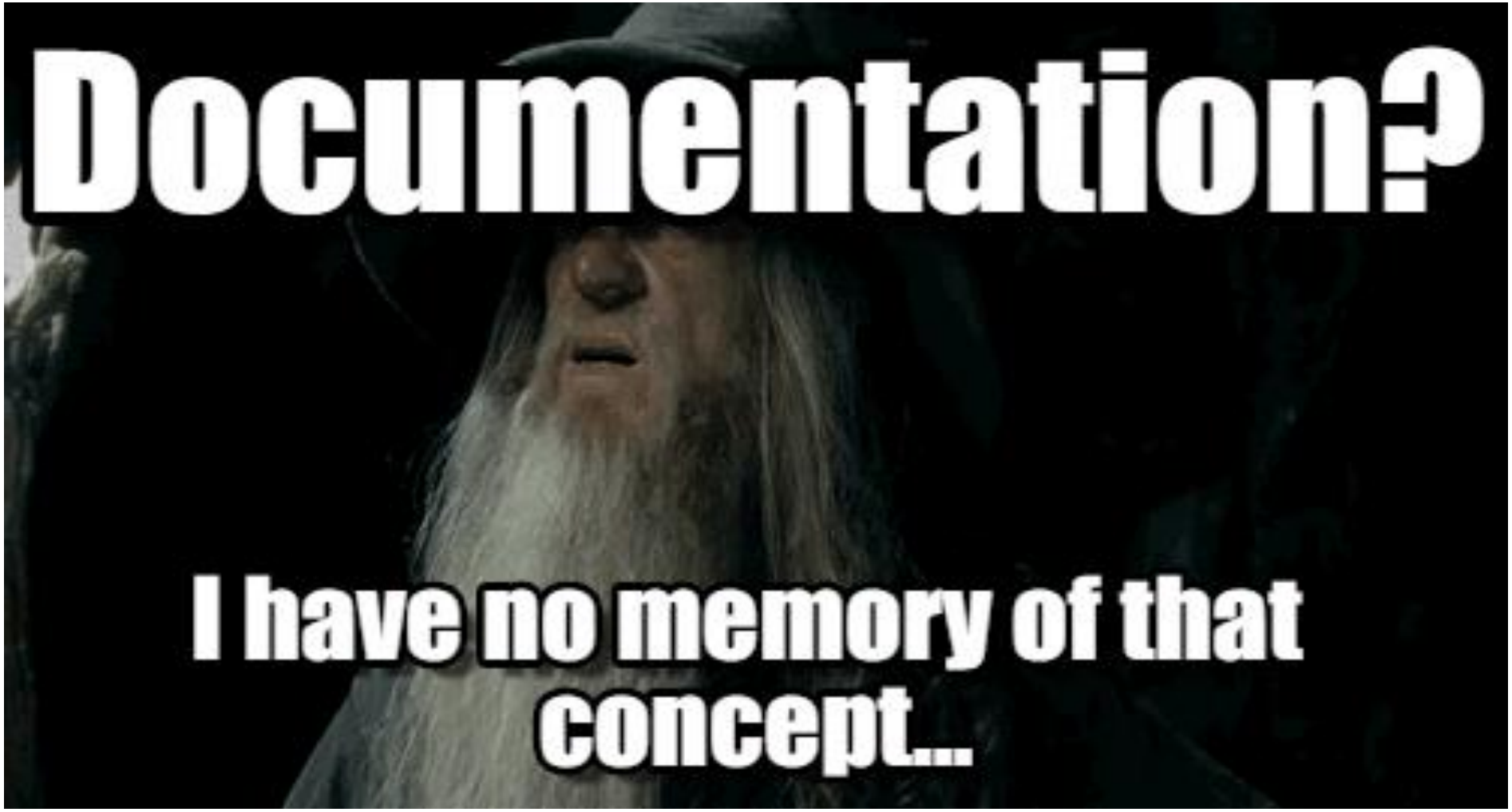
Bounce SECURITY

Use case approach to user story development

Bounce SECURITY

Big Model Up Front

Bounce SECURITY



Threat model separate from design

Bounce SECURITY

Usually out of date before completed

Bounce SECURITY

You want me to do WHAT with this?

Bounce SECURITY

Wasted time on unrealistic threats

Bounce SECURITY

Dependent on Security

Bounce SECURITY

Security team drops in and out

Bounce
SECURITY

Security team doesn’t scale

Bounce
SECURITY

Bounce
SECURITY

Bounce
SECURITY

Bounce
SECURITY

Bounce
SECURITY

Value Driven Process

Value Driven Approach

"All Threat Models are wrong,
some are useful"

Accept that it's wrong,
focus on the usefulness

Bounce
SECURITY

Prioritize by Value Chain

- Why are we building this?
- How do we get the value from this?
- What do we do to ensure that happens?

Bounce SECURITY

Find the Value

Follow the money!

How do people die?

Bounce SECURITY

Lightweight Threat Modeling

- Prioritize by value chain
- Focus on building useful controls
- Goal driven mitigation
- Threat patterns library
- Assumption-less design

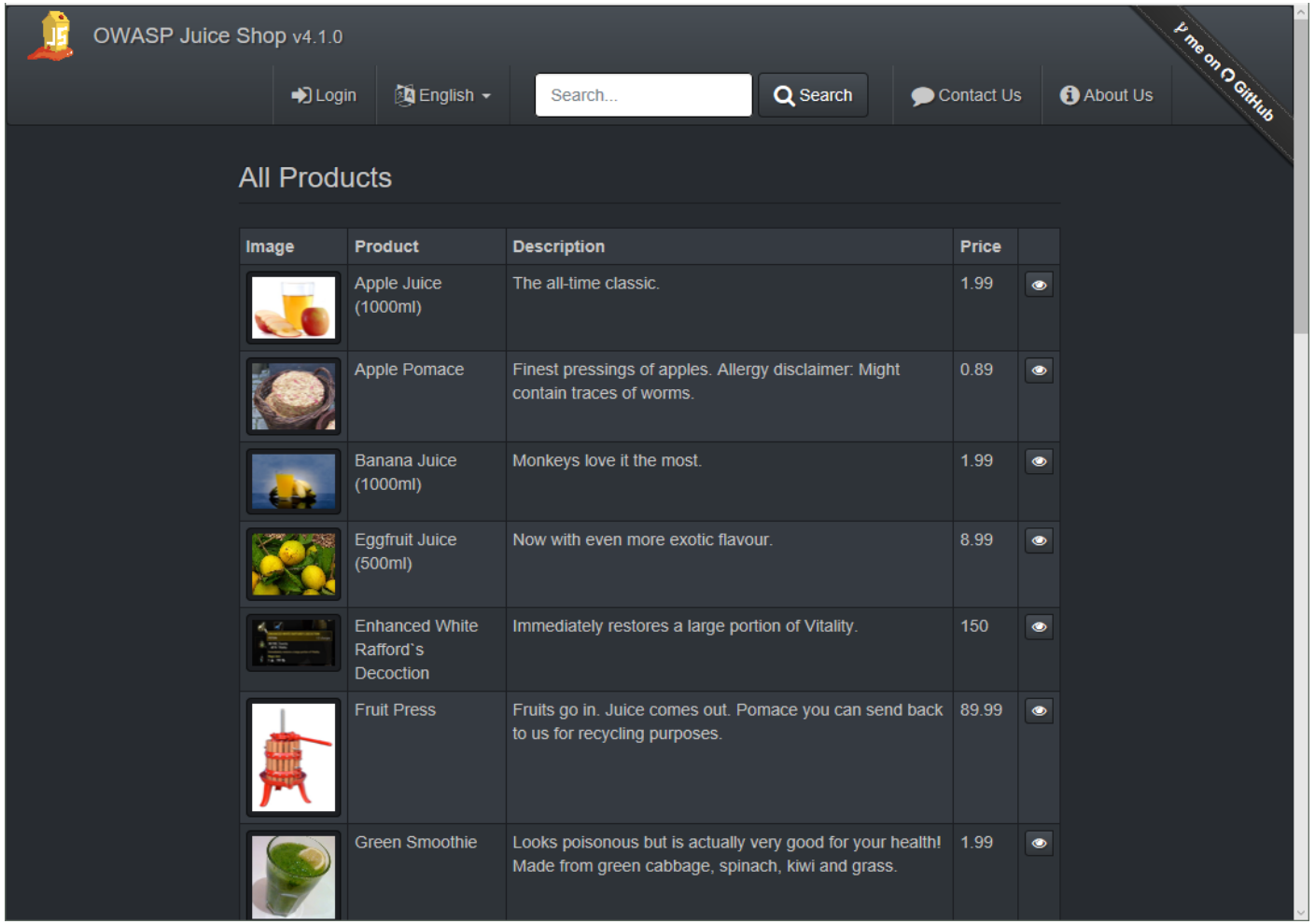
Scope

- For each User Story / Epic / Feature
  - *During “Discovery” or Sprint Planning*
  - *Agile approach of “just enough”*
  - *Threat model goes into the User Story*

Workflow – Stories & Epics

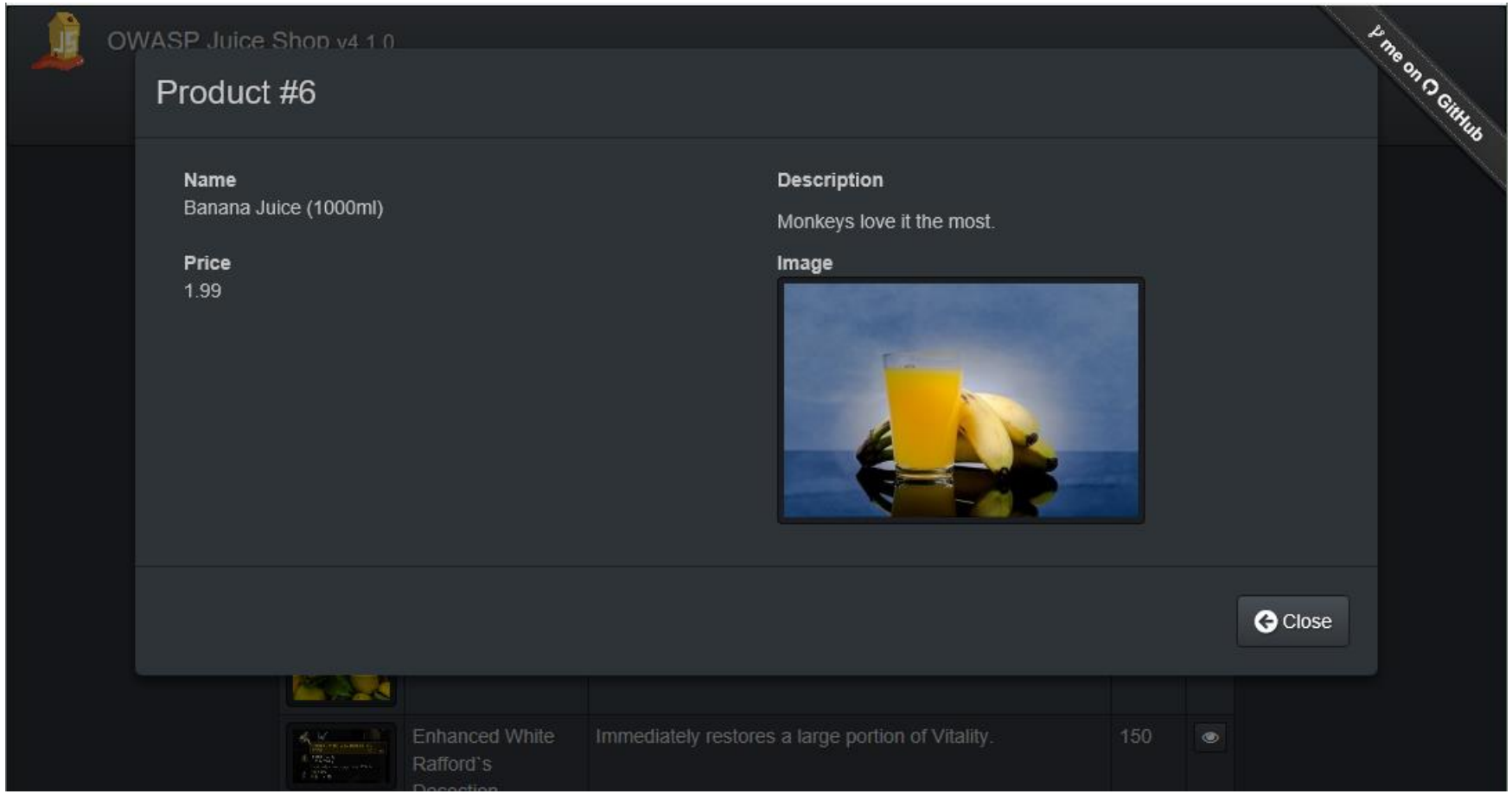
1. State story goals and value chain
2. Describe expected flow and failure states
3. Discover assumptions and conditions
4. Validate assumptions and enforce conditions
5. Explicitly handle failure states

OWASP Juice Shop



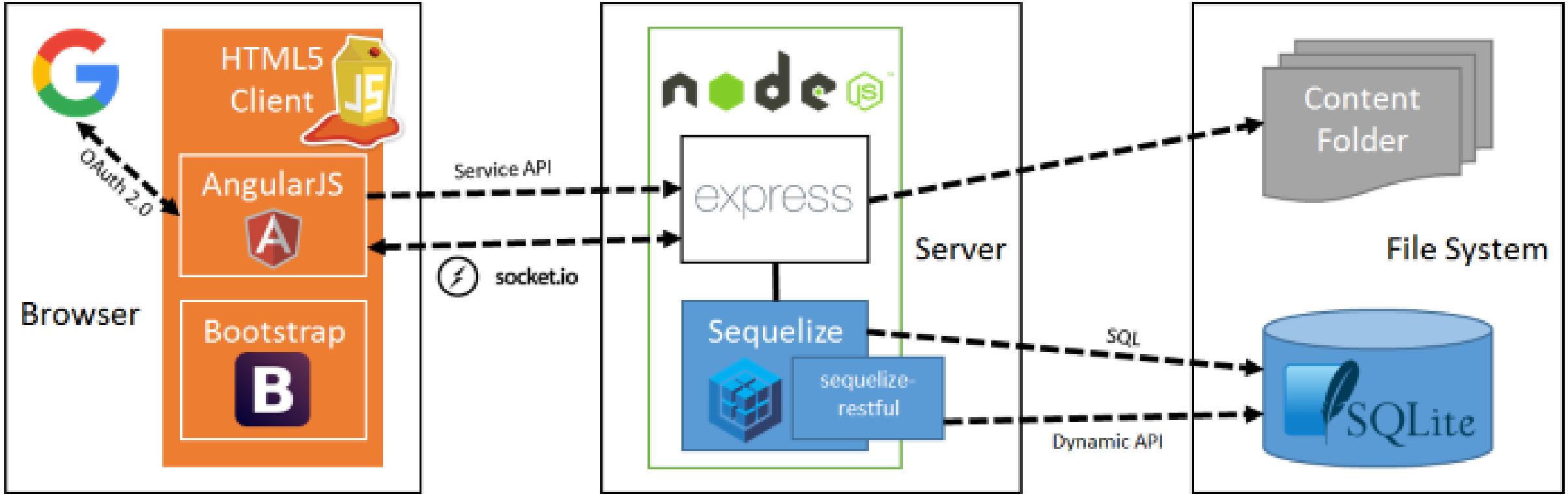
Bounce SECURITY

OWASP Juice Shop - Selection



Bounce SECURITY

OWASP Juice Shop Architecture



OWASP Juice Shop - Checkout

OWASP Juice Shop v4.1.0

Logout | English | Search... | Search | Your Basket | Change Password | Contact Us | Recycle | Complain? | About Us

Fork me on GitHub

Your Basket

Product	Description	Price	Quantity	Total Price	
Banana Juice (1000ml)	Monkeys love it the most.	1.99	5	9.95	
Raspberry Juice (1000ml)	Made from blended Raspberry Pi, water and sugar.	4.99	1	4.99	
Woodruff Syrup "Forest Master X-Treme"	Harvested and manufactured in the Black Forest, Germany. Can cause hyperactive behavior in children. Can cause permanent green tongue when consumed undiluted.	6.99	1	6.99	

Checkout

Coupon (Need a coupon code? Follow us on **Twitter** or **Facebook** for monthly coupons and other spam!)

Redeem

Bounce SECURITY

OWASP Juice Shop - Coupon

Bounce SECURITY

Agile Techniques

Bounce SECURITY

Advantages of Agile

Attributes:

- Cross functional teams
- Focus on usable software
- Developer independence

Activities:

- Definition of Done
- Acceptance Criteria
- TDD / Unit tests

Updated User Story Format

“As a … I want … so that … WITHOUT …”

As a customer,
I want to purchase juice
so that my kids let me sleep in
<u>WITHOUT my credit card being stolen</u>

Bounce SECURITY

Acceptance Criteria

When I login with a wrong password,
I should be locked out after X times.

Security Unit Tests

Test that accounts are locked after X attempts

Test locked accounts are unlocked after Y time

Abuser Stories

As an attacker,
I want to impersonate another user
so that I can steal their juicebox

Bounce SECURITY

Sorry Points

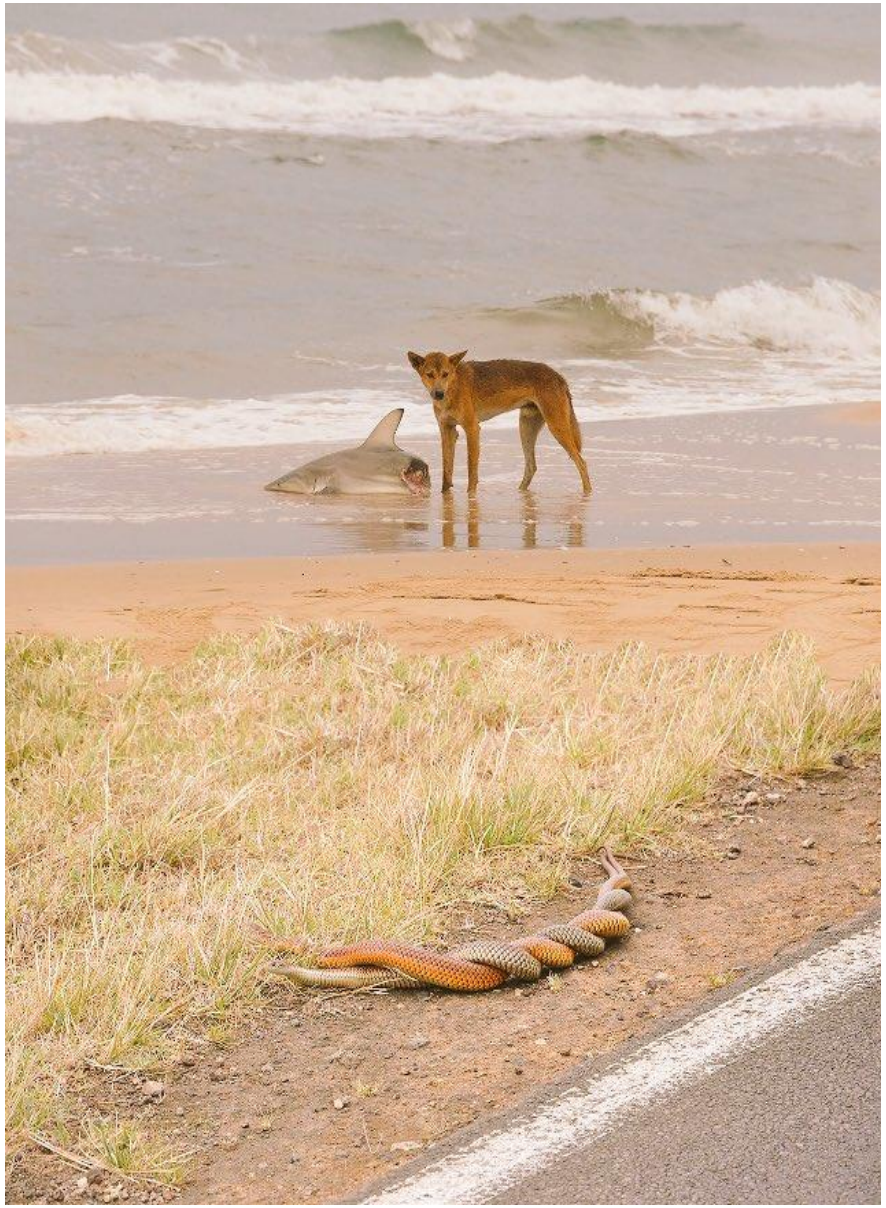
- Similar to Story Points
  - *Rough estimate relative to other stories*
- Measured in the same way
  - *Tshirt sizes, Fibonacci values, etc*
- “How sorry will you be if this breaks?”
  - *Value*
  - *Visibility*
  - *Side effects*

Story Points

Relative estimate of effort

Sorry Points

Relative estimate of impact



"What if it goes horribly wrong?"

Bounce SECURITY

Definition of Done

User stories will include a threat model and security tests.

Bounce SECURITY

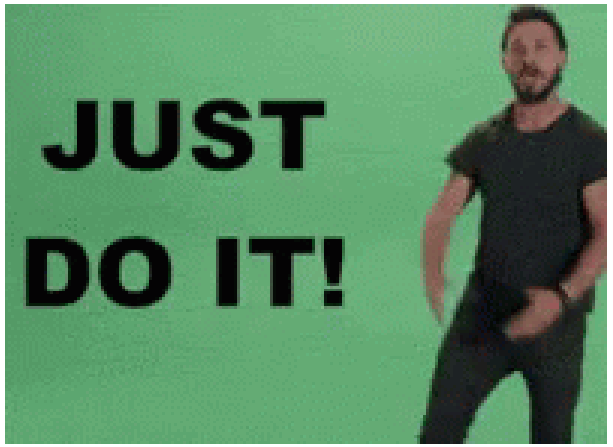
Communication

x Cross Site Request Forgery (CSRF)	<->	✓ Unauthenticated Access to Cash Transfer
x Stored XSS	<->	✓ Admin Takeover
x AuthZ Bypass	<->	✓ Change Delivery Address
x Denial of Service	<->	✓ Loss of Revenue/Market

Bounce SECURITY

Takeaways

- Design for security by threat modeling
- Everything should be threat modeled
- Everyone should be threat modeling
- Focus on business value
- Prioritize usefulness



Bounce SECURITY

THANKS FOR LISTENING!

Avi Douglen
Bounce Security
@sec_tigger

Bounce SECURITY