Guiding Principles

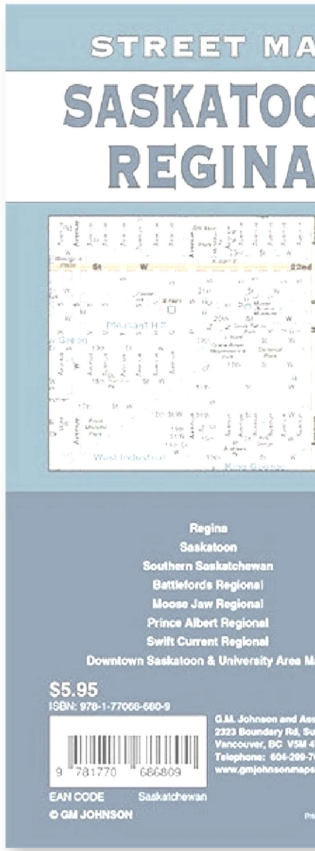
Develop Intelligence

Goals

1. Discuss the merits of security theater
2. List 2 of the basicest rules

Roadmap

1. Scary Stories
2. Mindset
3. Basicist Rules for Web Apps



Develop
Intelligence

Scary Stories

Develop Intelligence

Biggest Data Breaches

Victim	Year	Users Affected (M)
Adobe	2013	152
7-Eleven	2013	160
Marriott	2018	500
Facebook	2019	540
First American	2019	885

Worldwide Cybercrime Damag

- Cost $3 trillion in 2015
- $6 trillion in 2021
- US Federal Revenue in 2019: $3.46 trillion

Develop
Intelligence

Mindset

Develop Intelligence

Overview

1. Not Binary
2. Relative
3. Process

Security is Not Binary

Gene Spafford:

> *The only truly secure system is one that is powered of*
> *a block of concrete and sealed in a lead-lined room wi*
> *armed guards - and even then I have my doubts.*

Security is relative

- There's no door that the NSA can't get in, but that d
  matter.
- (Hereafter referred to as a skilled and determined h
- But even with those resources, it's not worth the mo

Bear Joke

Security is a Feature

- It's just for a long time, no one was very articulate
- They just say, it should 'be secure'
- Think about your risk profile and risk tolerance

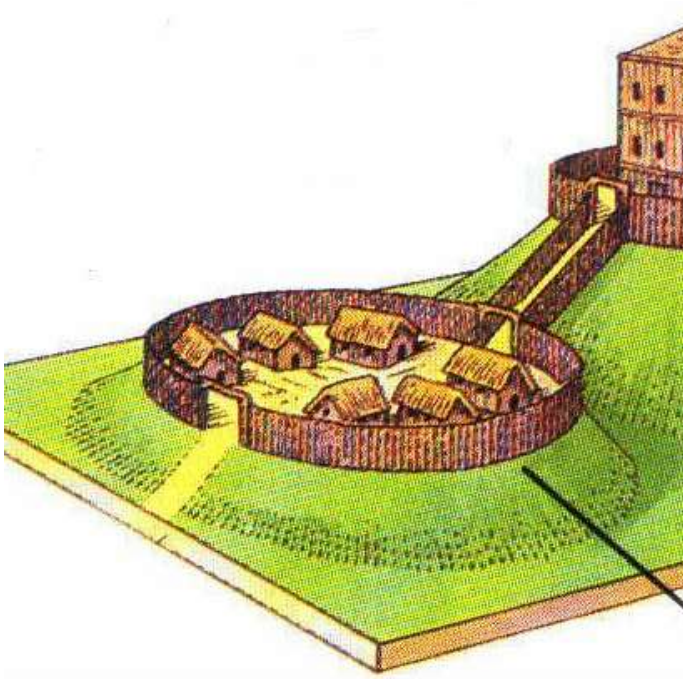
Alignment is Hard

Mark Magliocco:

> *Agreement is easy... alignment is hard. When I ask my*
> *she wants dinner, she quickly says okay-- the trouble s*
> *when I ask where we should go.*

Security Should be Redundant

- Defence in depth
- Like a Motte-and-bailey castle
- Example:
  - Secure your identity database
  - Hash and salt passwords



Stand on the shoulders of gian

- Don't roll your own stuff
- Think hard before adopting non-mainstream stuff (e
  Choose Vue over Elm (or whatever))
- Avoid dependencies. If you don't need dancing bun
  whatever, maybe roll your own.
- Follow best-practices

Think Like a Practitioner

- The one time I got fired
- Hippocratic oath
- Responsibility to users

Develop
Intelligence

Basicist Rules for Web App

Develop Intelligence

Think about **Trust**

- Can you trust the integrity an HTTP request?
- Answer: No
- What about internally-facing services?
- Also: No

Validate Input

Input validation *is the process of ensuring input data*
consistent with application expectations. Data that falls
of an expected set of values can cause our application
unexpected results, for example violating business log
triggering faults, and even allowing an attacker to take
of resources or the application itself.

Never Trust Input

- When building a client, assume the server is compr
- Building an API, assume you're talking to a hacker
- Validate Everything

Bad Input Validation Enables

- Cross Site Scripting
- SQL Injection

Encode HTML

- HTML is a very, very permissive format
- Browsers try their best to render the content, even i
  malformed

Bind Parameters for Database Queries

- **Don't** concatenate strings
- Use a prepared statement e.g. SqlCommand
- Better yet EF Core

Protect Data in Transit

- SSL Everywhere

Follow Checklists

- Look it up
- cheatsheetseries.owasp.org

Security Theater

- Lots of security practices don't help
  - Password expiration
  - PIN complexity
- Do it anyway
- Tall poppy syndrome

Resources

- Sites
  - Schneier on Security
  - OWASP Cheat Sheet Series
  - Krebs on Security
- Books
  - Kevin Mitnick
  - The Gift of Fear
  - Facing Violence

Develop
Intelligence

Review

1. Discuss the merits of security theater
2. List 2 of the basicest rules