codestock

Security from Scratch: Building Secure Applications from the Ground Up

Jared M. Smith
@jaredthecoder
jaredmichaelsmith.com

About me

- Security Researcher and Software Engineer at ORNL in the Cyber Warfare Research Team
- Formerly Software Security Engineer at Cisco System's Advanced Security Initiatives Group
- Senior at UTK in Computer Science
  - Founded HackUTK and VolHacks
  - Published in ACM and IEEE journals
- Technical Consultant for several VC-backed startups (cybersecurity, media, and social spaces)

Storytime!

A (slightly satirical) life of a dev

Lead Developer: Boss, we've been building this application for weeks. We think we're finally at 1.0 and the client likes the preliminary results. Even all of our continuous integration tests are passing! Can we launch it?!

Manager: Let me check with the other managers, PM's, and the CTO and I'll get back to you ASAP.

[at all-hands meeting the following day]

CTO: We've been waiting for this day for a long time…blah blah blah buzz word blah blah blah…blah blah buzz word blah… LAUNCH IT NOW!

Lead Developer: […scurrying to keyboard…types `git push origin release`…anxious waiting…terminal returns `TESTS PASSED. V. 1.0 DEPLOYED TO RELEASE BRANCH`…]

Slack Bot: 🎉🎉🎉

6 MONTHS

LATER...

[…massive leak of credit card numbers and plaintext passwords…hackers breached internal systems as well]

Slack Bot: SEND 25 BITCOINS TO WALLET 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2 TO GET YOUR BOT BACK

Security from Scratch

1) Understand the problem

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 11th July 2016)

interesting story

YEAR | *BUBBLE COLOUR* YEAR | METHOD OF LEAK | *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER

latest

2015

2014

2013

2012

Anthem 80, 000, 000

Mossack Fonseca

Code.org

Hacking Team

MySpace 164, 000, 000

Philippines' Commission on Elections 55, 000, 000

Syrian government

Turkish citizenship database 49, 611, 709

National Childbirth Trust

Privatization Agency of the Republic of Serbia

Mutuelle Generale de la Police

World Check

uTorrent

Verizon

VK 100, 544, 934

AshleyMadison.com

Carefirst

Minecraft

MSpy

Premera

Wendy's

Adult Friend Finder

CarPhone Warehouse

Kromtech

Voter Database 191 million

US Office of Personnel Management (2nd Breach)

VTech

Australian Immigration Department

D&B, Altegrity

Dominios Pizzas (France)

Experian / T-mobile

Invest Bank

JP Morgan Chase 76, 000, 000

Uber

Community Health Services

British Airways

European Central Bank

IRS

Sanrio

TalkTalk

Twitch.tv

UPS

Mozilla

US Office of Personnel Management

Slack

AOL 2, 400, 000

Yahoo Japan

Korea Credit Bureau

Securus Technologies 70 million

Ebay 145, 000, 000

Home Depot 56, 000, 000

Target 70, 000, 000

Advocate Medical Group

Vodafone

Twitter

Washington State court system

Neiman Marcus

NASDAQ

New York Taxis

Staples

Sony Pictures

Nintendo

Scribd

NMBS

OVH

SnapChat

South Africa police

TerraCom & YourTel

Adobe 36, 000, 000

Apple

Drupal

Facebook

Japan Airlines

Kissinger Cables

Living Social 50, 000, 000

Central Hudson Gas & Electric

Evernote 50, 000, 000

Florida Department of Juvenile Justice

UbiSoft "unknown"

"Apple"

California Department of Child Support Services

Citigroup

Crescent Health Inc., Walgreens

Indiana University

Formspring

Kirkwood Community College

Tumblr 65, 000, 000

Ubuntu

Dropbox

Greek government

Florida Courts

Massive American

Source: informationisbeautiful.net


SSLv3

Compromise is inevitable

- We all mess up when writing code
- Non-public, unknown bugs are used against you
  - Zero-days
    - Example: Stuxnet, FBI and the iPhone, Kaspersky
- You probably won’t notice it for a non-trivial amount of time
  - Example: OPM

And it's a **hard** problem.

Domains of Security

- Web
- Networks
- Vehicles
- Mobile
- Internet of Things (IoT)
- Embedded
- SCADA (Industrial Systems)
- and more…

Vulnerabilities Can Be Everywhere

TCP/IP Model	Protocols and Services	OSI Model
Application	HTTP, FTP, Telnet, NTP, DHCP, PING, DNS, BGP, JSON-RPC, SOAP, Exchange ActiveSync, IMAP, LDAP, POP, RTP, SIP, VOIP, SMTP, SSH, TLS/SSL, WebSockets, DDP, Tor, STOMP, RDP, NFS, MQTT, IRC BitTorrent, Bitcoin, SOCKS, SPDY, ASCII, UTF-8, MIME, AFP, PFIF, XML-RPC	Application
		Presentation
		Session
Transport	TCP, UDP, PPTP	Transport
Network	IPv4, IPv6, ICMP, IGMP, IPSEC	Network
Network Interface	MAC (Ethernet, DSL, ISDN, FDDI), 802.11 (Wi-Fi), ARP, ATM, LLDP, NDP, PPP, OSPF, L2TP	Data Link
		Physical

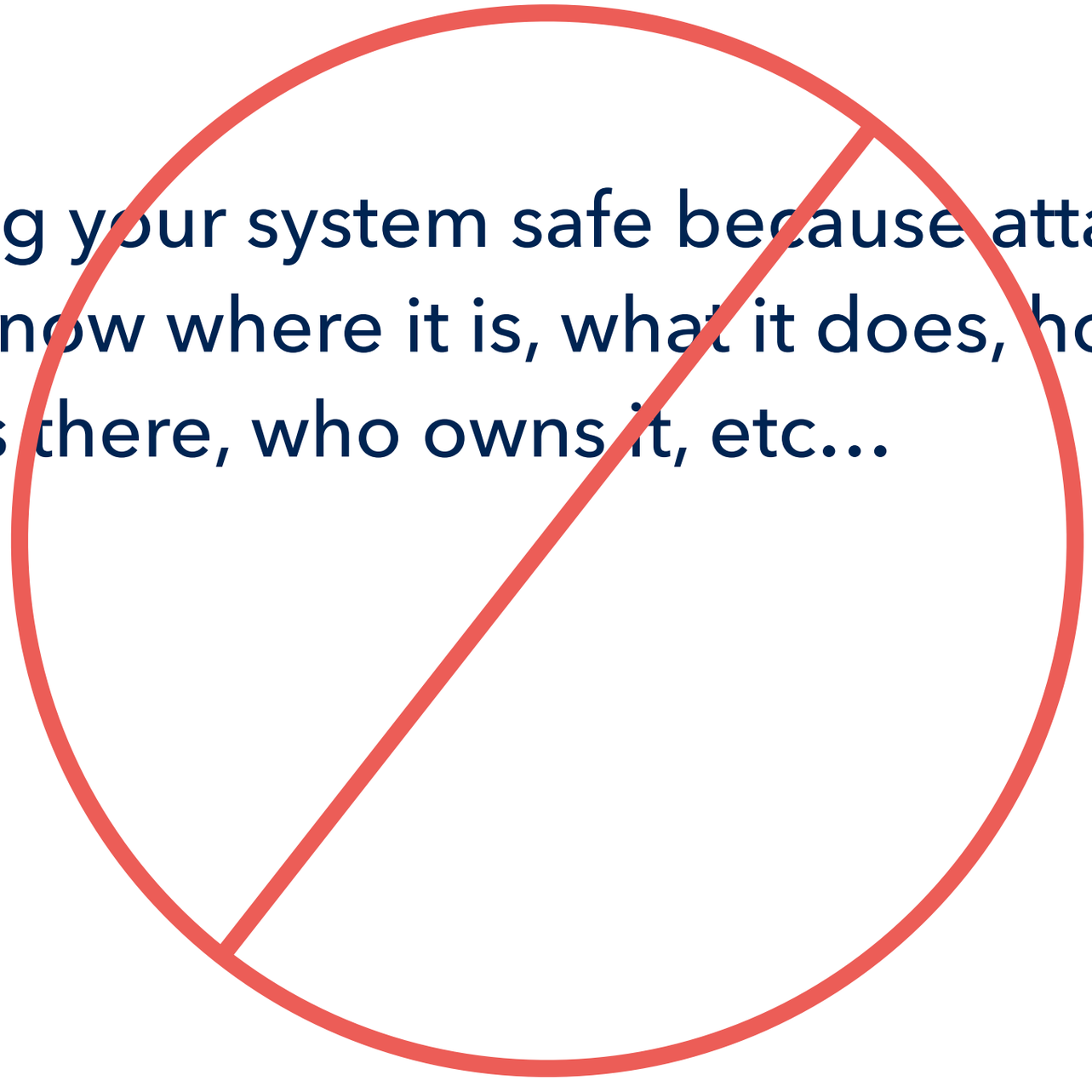
But there is hope.

Cue epic Star Wars music...

2) Understand the right way

Security through Obscurity

- Keeping your system safe because attackers don’t know where it is, what it does, how it works, why it’s there, who owns it, etc…



Security through Ignorance

- Keeping your system safe by completely ignoring the fact that computer security exists, bad guys aren't real and don't care about your company, and vulnerabilities are a myth

Security by Default / Security by Design

- Keeping your system safe by designing it to be secure from the ground up
- Acknowledging vulnerabilities can occur in code
- Maintaining and prioritizing a security team (even if it’s just one person)
- Thinking about how attackers will try to hurt you

3) Understand the basics

The Rundown

The Rundown

Basic things you should never do

- Missing authentication and authorization for the checkout page
- Hard-coded credentials, pushing credentials to version control like a pro
- Sensitive data is not encrypted from end-to-end
- Sudo first and ask questions later
- Using ROT13 for your encryption algorithm
- No rate-limiting because you don’t believe in DoS

Basic things you should never do

- Example: Early internet visitor counters
- Downloading files without checking the checksum
- Upload whatever files you want, including .php
- Improper sanitization of user input because XSS isn’t real - Example: Zuckerberg account takeover
- Using `*os.system(request.data)*` in your Django app
- Malicious advertisements, drive-by downloads of malware

4) Understand your enemy and yourself

“If you know the enemy and know yourself, you need not fear the result of a hundred battles.”

–SUN TZU, THE ART OF WAR

Hats? What hats?

- Black hats, white hats, grey hats, etc…
- Used to classify “hackers” by their motivations, purpose, compensation, and **generalized** characteristics

Motivation, who cares?

- It is helpful to understand how different parties are motivated
- Money, power, destruction…
- Morality, responsibility, protection of users

White Hats

White Hats

- Security Researchers
- Practice “responsible disclosure”
- Bug Bounties

Black Hats

Black Hats

- Motivations usually include at least one of four of the following:
  - Money - LinkedIn data breach
  - Power - North Korea vs. Sony
  - Destruction - Ukrainian power grid
  - Revenge - “Hacktivists”, Anonymous group

What's a vulnerability?

- When you make the application do something that it's not supposed to do
- To find vulnerabilities, you have to understand the application
- That's **GREAT** for us developers!

Know the application

- What's the intended functionality?
- What's the intended behavior?
- What does the application use as input?
- What does the application produce as output?

Wikipedia vs. CNN

- You find that authenticated, regular users can edit page content
- Vulnerability?
  - wikipedia.com
  - cnn.com

Attacking is a process

- **Step 1**: Reconnaissance
- **Step 2**: Develop vulnerability hypothesis
- **Step 3**: Test vulnerability hypothesis
- **Step 4**: Develop exploit
- **Step 5**: Profit

Injection Vectors

- Understand **ALL** input to the application!
- Examples for Web Applications:
  - Query parameters
  - URL path
  - PUT/POST parameters
  - Cookies
  - Headers (Referer header)
  - File uploads
  - Functionality from other websites
  - Emails
  - Form fields
  - Web Sockets
  - …

Understand data flow

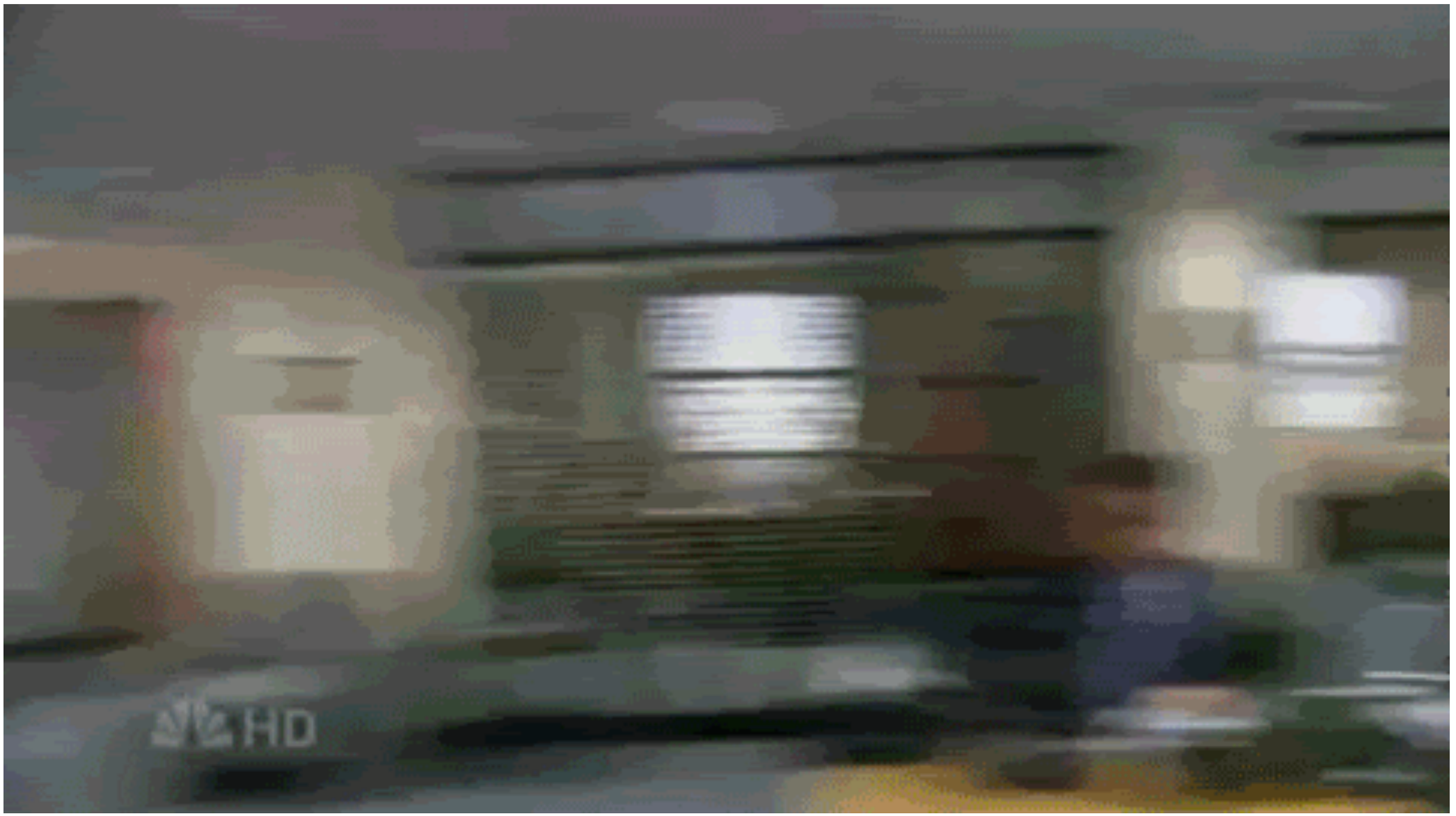
- How does the input data flow through the program?
  - Example: Data on page X is displayed on page Y and used to calculate the result of page Z
- How does the output of a page flow through the program?
  - Example: the result of a calculation used as part of a tweet

Takeaway

“If you spend more on coffee than on IT security you will be hacked. What’s more, you deserve to be hacked.”

–RICHARD CLARKE

FORMER NATIONAL COORDINATOR FOR SECURITY, INFRASTRUCTURE PROTECTION AND COUNTER-TERRORISM FOR THE UNITED STATES


HD

Sites to check out

- https://haveibeenpwned.com/ - check if your account has been compromised
- https://www.shodan.io/ - search devices on the internet (computers, connected TV's, cars, IoT devices, etc.)
- https://www.eff.org/https-everywhere - Encrypt all the data!
- https://panopticlick.eff.org/ - See how well your browser stands up to fingerprinting
- https://www.schneier.com/ - Bruce Schneier's blog, prolific cryptographer

Sites to check out

- https://github.com/sbilly/awesome-security
- https://github.com/PaulSec/awesome-sec-talks
- https://github.com/meirwah/awesome-incident-response
- https://github.com/enaqx/awesome-pentest

Podcasts you should check out

- http://securityweekly.com/ - Weekly Interview with security expert, security news of the week, and usually a technical segment
- http://softwareengineeringdaily.com/ - Interviews with people like Jeff Atwood (creator of Stack Exchange), creators of Spark and Hadoop, creators of ReactJS and Redux, lead engineers at well-known software companies, etc.

Podcasts you should check out

- https://talkpython.fm/ - Podcast all about Python focused on interviews with prolific Python community members, contributors, and companies
- http://www.newrustacean.com/ - Short weekly podcast on Rust, the language, Rust news of the week, a technical segment focused on it's semantics, and occasional interviews

Further Reading

- Black Hat Python: Python Programming for Hackers and Pentesters - Amazon
- Penetration Testing: A Hands-On Introduction to Hacking - Amazon
- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software - Amazon
- Hacking: The Art of Exploitation - Amazon
- So Good They Can't Ignore You - Amazon
- Deep Work - Amazon

Questions?

Jared M. Smith

jaredmichaelsmith.com

jared@jaredsmith.io

jaredmichaelsmith

jaredthecoder

jaredmichaelsmith