Was I supposed to Mix the Security in Before I Baked It?

Security Beyond the Cliché

W. Brandon Martin
Deconstructed Security, LLC

RVASEC
RICHMOND.VA

The Next 45 Minutes

01 - Introduction

02 - Background & Overview

03 - Security v. Business

04 - Security Balance

05 - Architectural Solutions

06 - Security Practitioners

07 - Questions

01 - Introduction

About Me

- Christian
- Dad (x3)
- Independent Security Consultant
- Raised in a barn
- Creds
  - OSCP, OSWP, GPEN
  - CISSP, CRISC
  - 6 Sigma Black Belt
- *Disclaimer: My statements today do not necessarily represent anyone else's view or actionable security advice.*

02 - Background & Overview

Problem Statement

- Good security requires planning and preparation.
- Security requirements delay projects.
- Businesses need projects to stay in business.
- Business and security goals collide.

Goals

- Explore the security / business tension.
- Review real-world balance failures.
- Review architectures that worked and failed.
- Re-define the security practitioner's role.

03 - Security v. Business

Reality

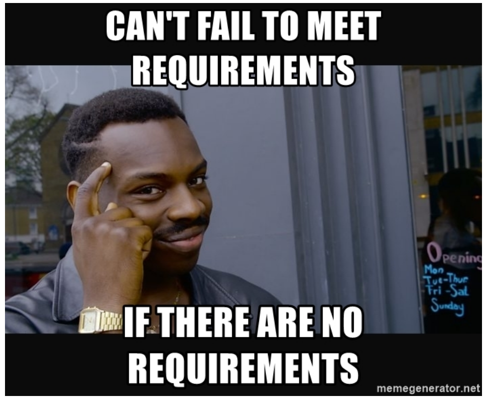
- Business people struggle with security.
- Technical people struggle with security.
- Security people struggle with both sides.

Security Requirements

- Keep the hackers out.
- Maintain compliance and/or regulator satisfaction.
- Train developers on secure coding practices.
- Keep penetration testers out.
- Sanitize untrusted input.
- Implement CIS benchmarks.
- No High or Critical findings

Business Requirements

- Calculate interest on a loan.
- Send a purchase order electronically.
- Automate the disbursement process.
- Complete the first sprint by Feb 28.



Technical Requirements

- Response latency < 2 seconds.
- Application must be testable.
- Application must run on Microsoft Windows, Android, iOS.
- Network throughput SLA must be 2Mb/s.

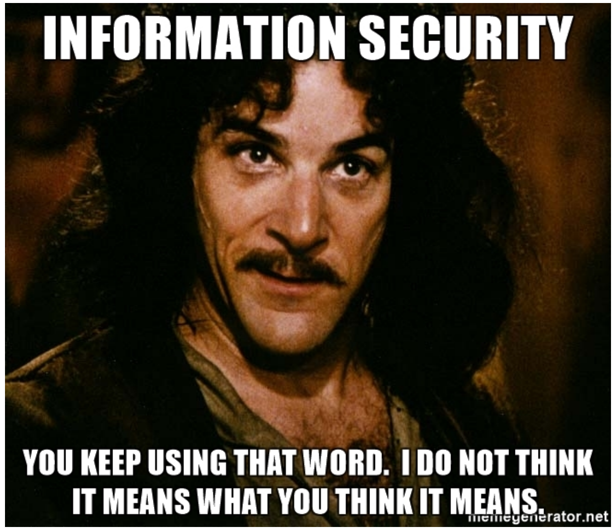
The Result

- CFO wants results yesterday.
- CTO wants to be meet the SLA.
- CISO wants to dot the "i" and cross the "t."

04 - Security Balance

Security Overpowers Business

- A German pro basketball team was relegated to a lower division due to a Windows update (2015)
- User can't create a valid password at change time (2019)
- GrooveShark (2015)
- Countless failed startups you never heard mentioned

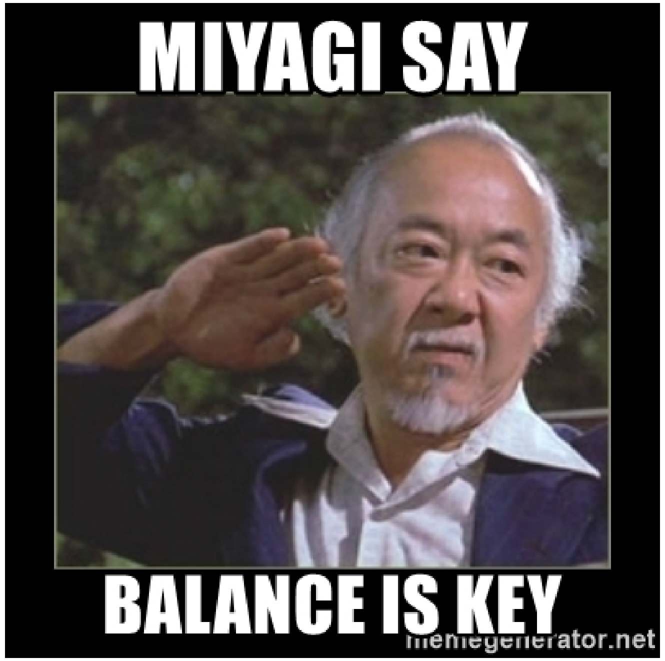

INFORMATION SECURITY
YOU KEEP USING THAT WORD. I DO NOT THINK IT MEANS WHAT YOU THINK IT MEANS.
memegenerator.net

Business Overpowers Security

- Mirai Botnet
- Target's Heating and Cooling System Breach (~$202M)
- Yahoo lost 500M Passwords; Linkedin 117M
- Hillary Clinton's Email Server

Balance is Key

- Risk perspective is missing.
- Context is under-appreciated.
- Healthy discourse is difficult.

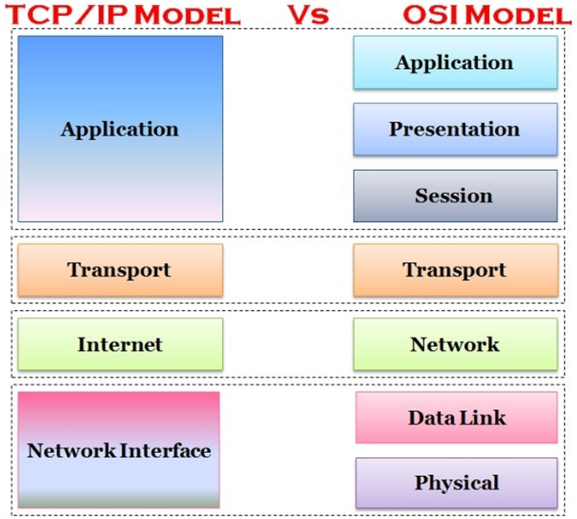


05 - Architectural Solutions

Architecting the Internet - TCP/IP

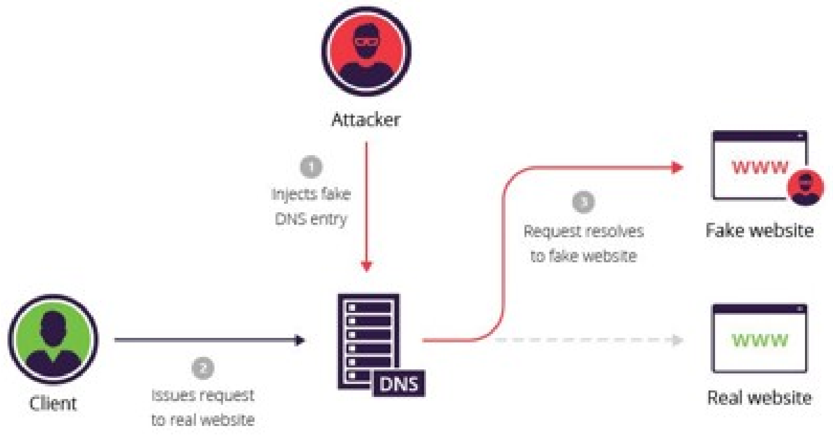
- Designed in the 1970's
- Adopted in the 1980's
- Secured in the 1990's

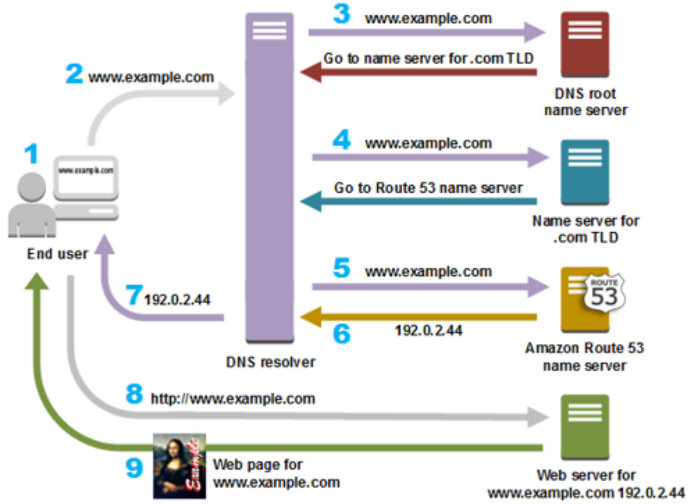
- Online Banking and Paris Hilton widely adopted in the 2000's



Architecting the Internet - DNS

- Proposed in 1983; essential since 1985
- Designed for 50M addresses, currently 271M
- DNSSEC introduced in 1997
- Dan Kaminsky's bug 2008
- DNSpionage 2019: 25% US Adoption of DNSSEC





Lessons Learned

- Some controls are difficult to "bolt on" after rollout.
- Forecasting unexpected use cases is hard.
- The architecture must leave "bolt holes" for security.
- Consumers don't always prioritize security.
- Security can take years.

Improving Security

- Containers
  - Don't patch, rebuild
  - Infrastructure as code (i.e. version tracking)

- DevSecOps - Integrating Security Testing In Development
  - Static Application Security Testing
  - Dynamic Application Security Tes

- Software Frameworks
  - Solve common problems

YO DAWG, I HEARD YOU LIKE CONTAINERS
SO I PUT A CONTAINER IN YOUR CONTAINER
memegenerator.net

06 - Security Practitioners

Partner Perceptions

- Just say no.
- Abuse fear, uncertainty, & doubt (FUD).
- Overstate risk.
- Don't understand the technology's built-in controls.
- Slow down and delay projects.
- Only understand [Insert Background]

Ideals

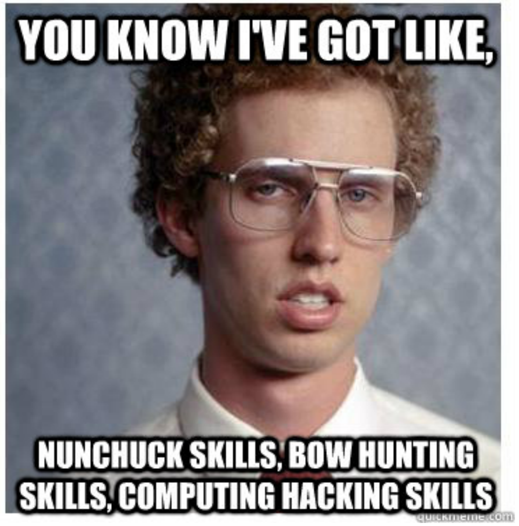
- "Yes, and..."
- Trust, Assurance & Confidence (TAC).
- Understand enough background to be helpful.
- Paint accurate risk pictures.
- Understand technical controls.
- Connect silos and accelerate projects.
- Don't accept risk.

Hard to find good help

- We can't all be the best.
- Can't educate a practitioner to full competence.
- Industry trend - full stacking
- Information Security
- Risk Analysis
- Networking, Servers, Clients, Mobile, Users

Addressing the Talent Gap

- Security Associate Programs (OJT)
- Job rotation
- Certification
- Mentoring
- Cybersecurity Education Reform
- Sales and Presentation Skills


YOU KNOW I'VE GOT LIKE,
NUNCHUCK SKILLS, BOW HUNTING SKILLS, COMPUTING HACKING SKILLS
quickmeme.com

07 - Questions