RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-W13

Hacking IoT:
Why Security in IoT is Failing

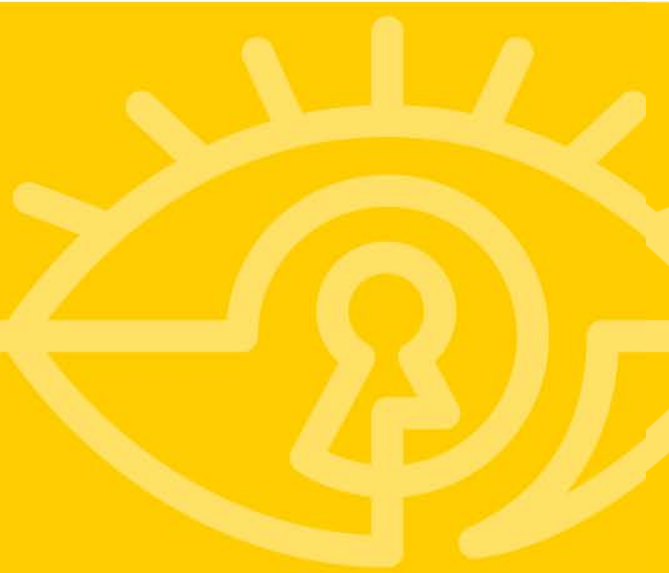
(and how to fix it!)

Ted Harrington
Executive Partner
Independent Security Evaluators (ISE)
Ted.Harrington@securityevaluators.com
@ISESecurity

#RSAC

Why is this important?

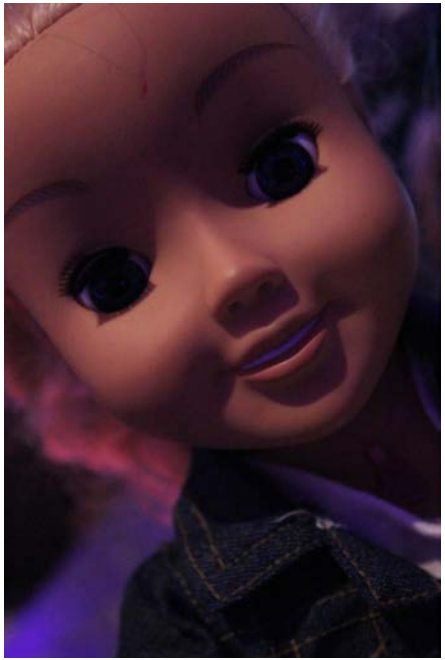
independent security evaluators



IoT Village


VILLAGE

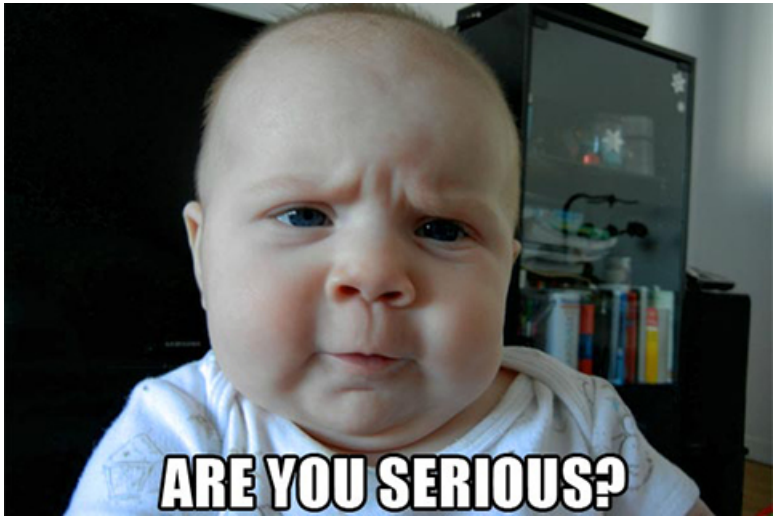

DANGER LIVE RAILS
DEFCON
23




VILLAGE
SECURITY OF WIRELESS
HOME AUTOMATION
SYSTEMS – A WORLD
BESIDE TCP/IP
cognosec
HAC
VILLAGE

IoT Village: Results

- **66** zero-days
- **27** device types
- **18** manufacturers



IoT Village: Results

SAMSUNG

PHILIPS

fitbit

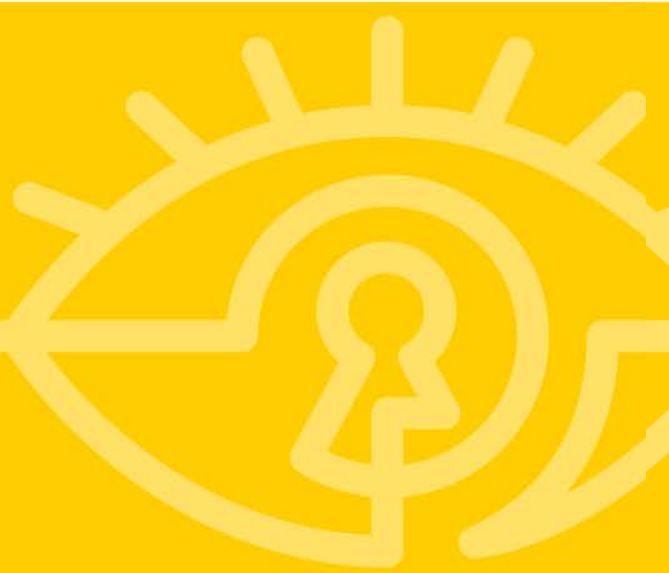
BOSE

D-Link®

ISE
independent security evaluators

IoT Village: Results

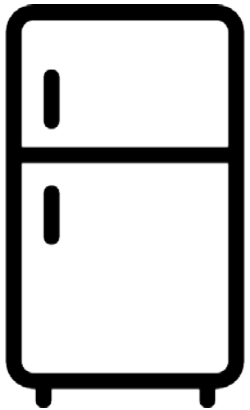
- Privilege Escalation
- Remote Code Execution
- Backdoors
- Runs as Root
- Lack of Encryption
- Key Exposure
- Denial of Service
- Etc, etc, etc



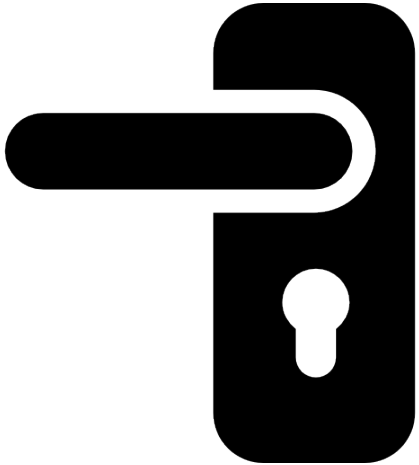
Attack Anatomies

Baby Monitors

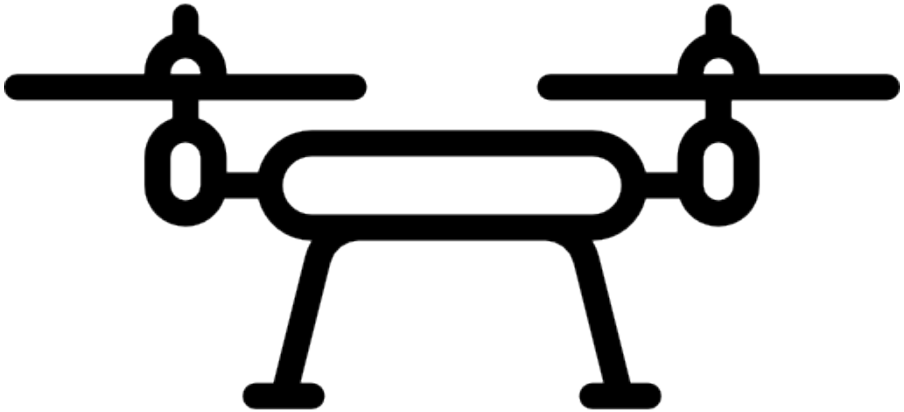
Refrigerator



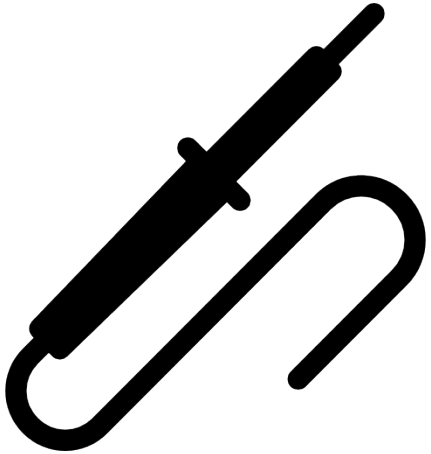
Lock

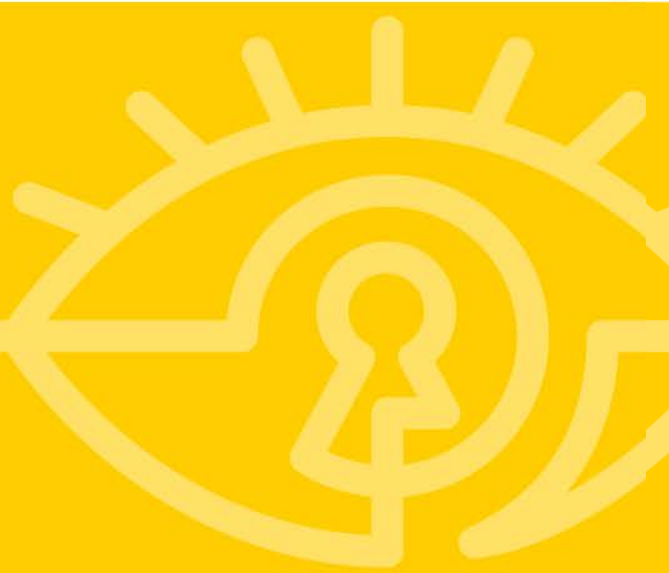


Drone



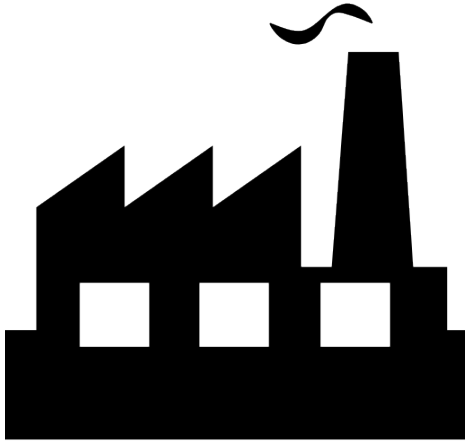
Hardware Hacking

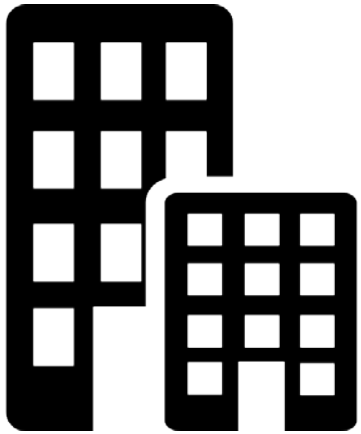




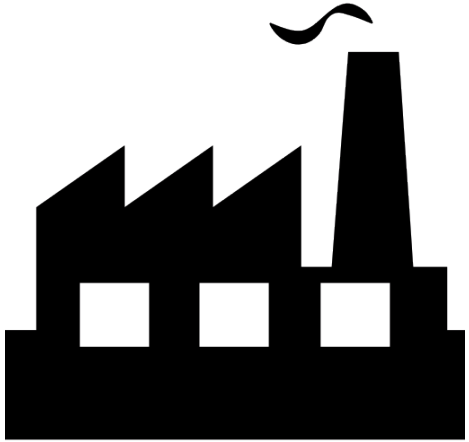
Solutions

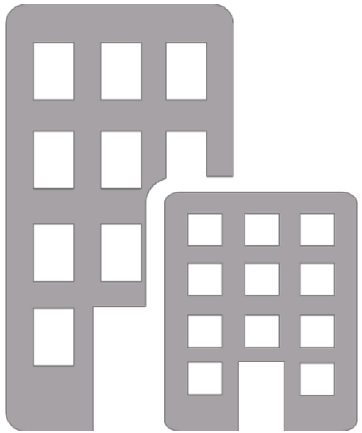
What Can Be Done?

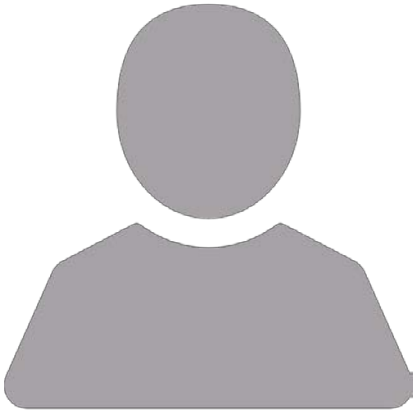




What Can Be Done?







Back to Basics

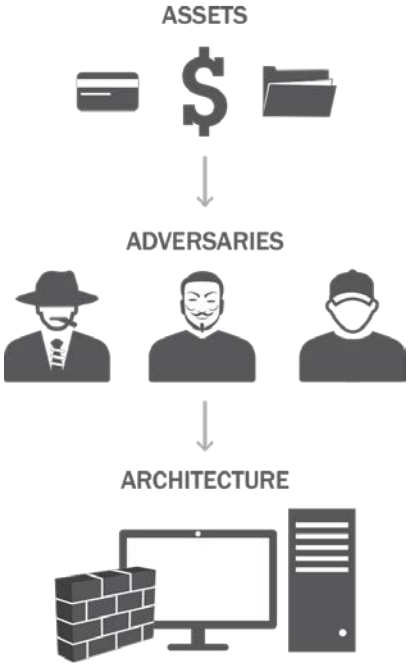
- Secure Design Principles
- Threat Model
- IoT is no different, from a security perspective

Threat Model

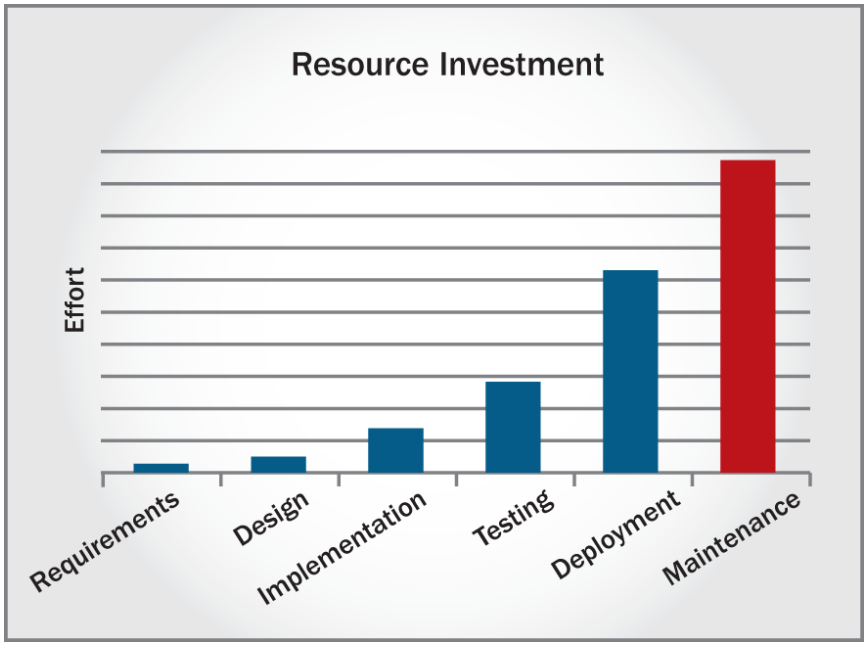
"If you don't know where you are going…

… any road will take you there."

Threat Model



Build It In!



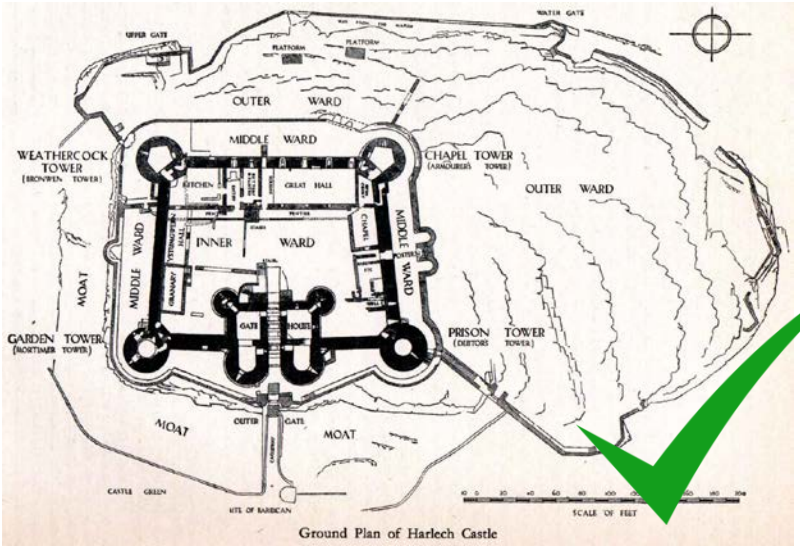
independent security evaluators

Reduce Asset Handling

independent security evaluators

Complete Mediation

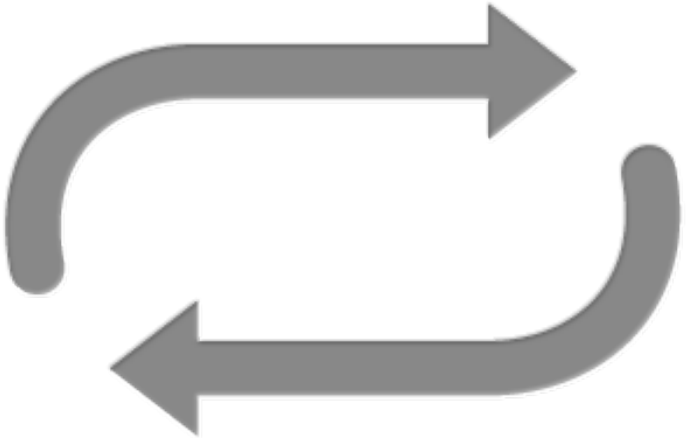
Security Assessment



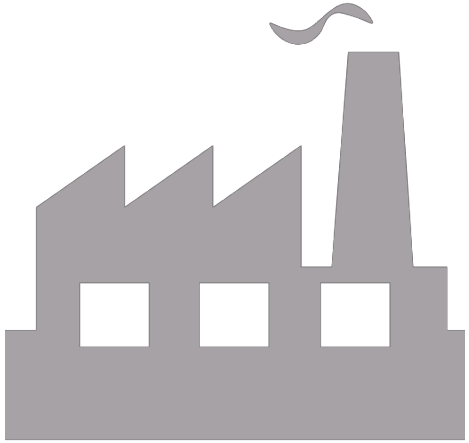
Ground Plan of Harlech Castle

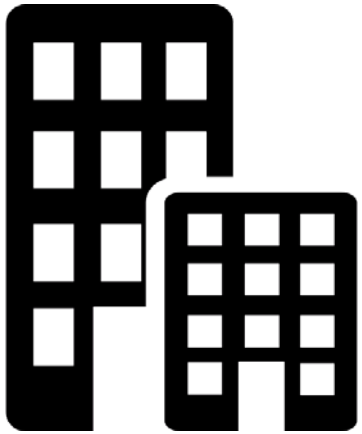
independent security evaluators

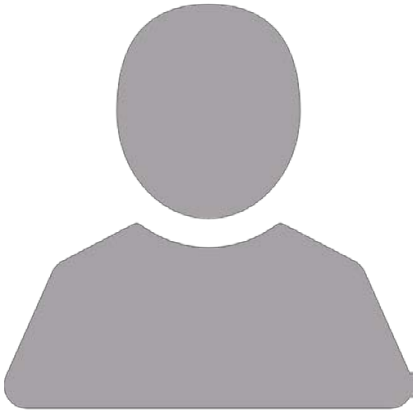
Ongoing Reassessment



What Can Be Done?

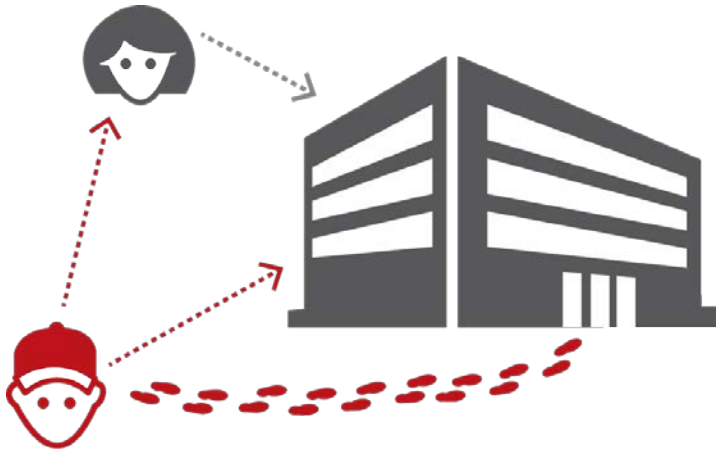




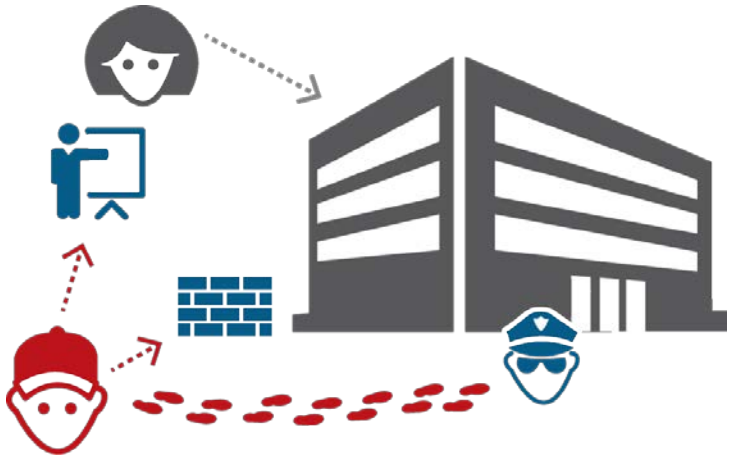


Understand Threat Landscape

Traditional Attacks



Traditional Defenses



independent security evaluators

Understand Threat Landscape

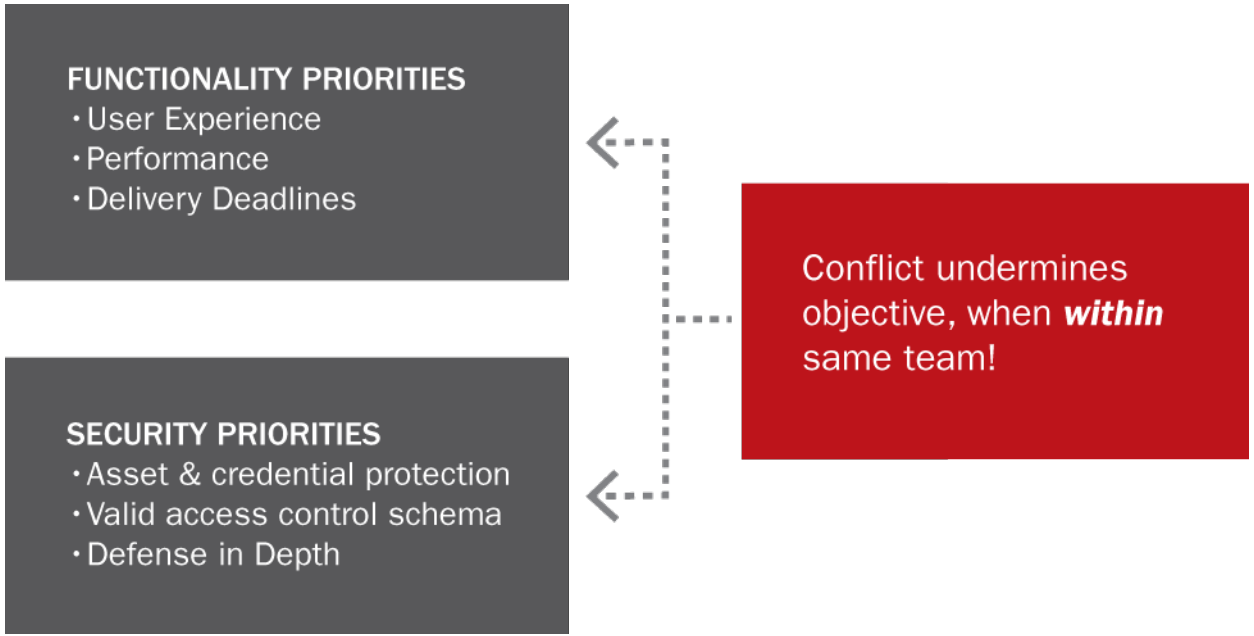
Defense in Depth

Priorities Affect Outcomes

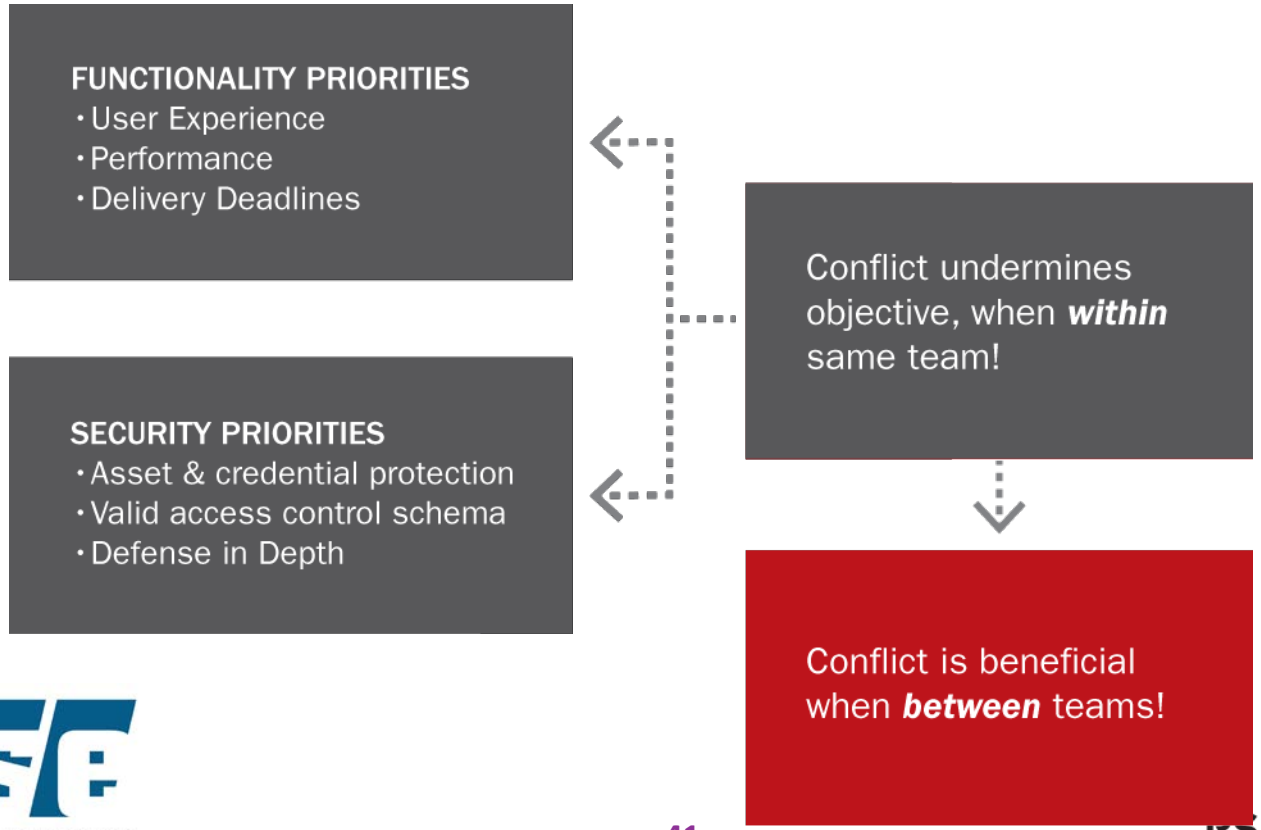
FUNCTIONALITY PRIORITIES
- User Experience
- Performance
- Delivery Deadlines

SECURITY PRIORITIES
- Asset & credential protection
- Valid access control schema
- Defense in Depth

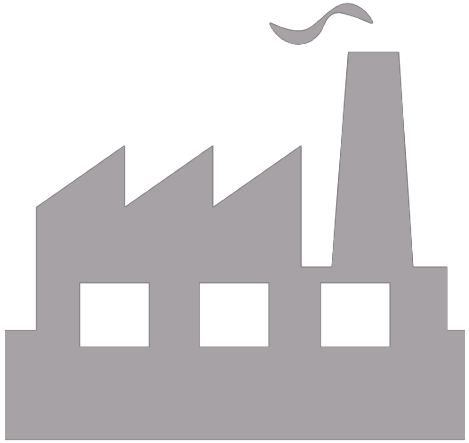
Priorities Affect Outcomes

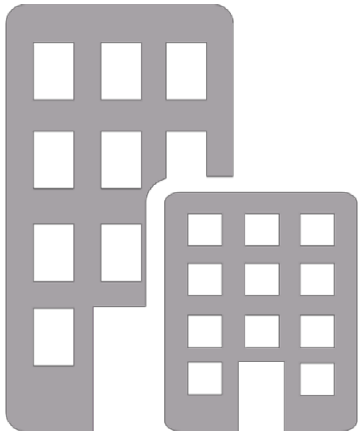


Priorities Affect Outcomes

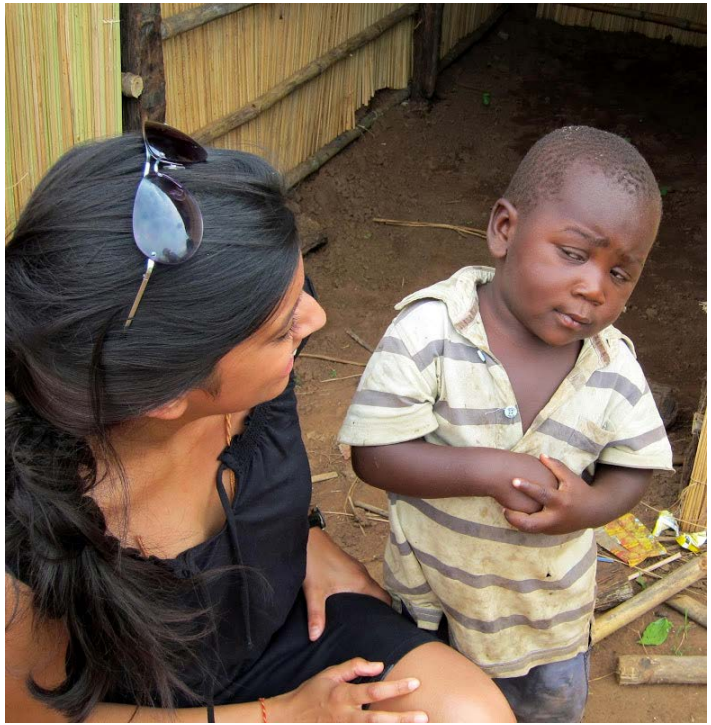


What Can Be Done?





Trust Reluctance



Sniff out the B******t

- “bank-level security”
- “military-grade encryption”
- Unsupported claims
- Lack of security features

Vote With Your Wallet!

Apply

Manufacturers

- Adhere to Secure Design Principles
- Establish Threat Model
- Perform security assessment… before the bad guys do!

Apply

Businesses

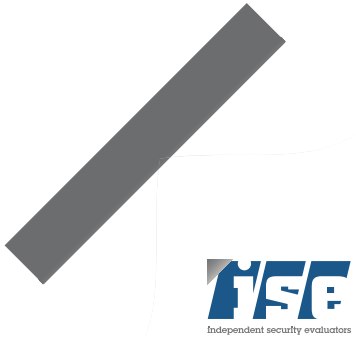
- Define Assets
- Consider Adversaries
- Identify and Reduce Risk

Apply

Users

- Understand the risk you are adopting
- Be an informed consumer
- Speak up!

Questions?



Ted.Harrington@securityevaluators.com