SafeLogic

# Security Strategies for Wearables

Ray Potter

IEEE – Wearable Technology Exposition

August 20, 2014

SafeLogic

# Agenda

- Use cases
- Technical constraints
- Risks
- Similarities to other mobile devices
- Techniques and best practices for security

# SafeLogic

- Provides cryptographic modules with emphasis on compliance
- Rooted in mobile and server-side implementations
- Focused on the future by developing and testing for wearables and IoT

# InfoSec Pillars

- Confidentiality
- Integrity
- Availability

# Use Cases (Think Security)

- Health
- Corporate
- Retail
- Transportation
- Utilities
- Education
- Consumer

# Constraints

- Space
- Performance
- Proliferation
- Churn
  - Devices
  - Firmware

# What's at Stake

- Pattern recognition
- Identity Theft
- Corporate espionage
- Life

# Mobility

- Wearables are a natural progression
- More mature security model
- Don’t make same mistakes twice

# Lessons Learned

- Threats
- Vulnerabilities
- Focus on data, not device
- Build security in
- Validation is important

# FIPS 140

- *Federal Information Processing Standard 140*
- Specifies requirements for CRYPTOGRAPHIC hardware and software modules
- Published by US (NIST) and Canadian Governments
- Offers 4 levels of validation

SafeLogic

# Why FIPS 140 Validation?

- Required for Federal and industry procurement
- FIPS Compliant
  - Embedding a module that already has a FIPS validation
  - Uses proven crypto functions
- FIPS Validated
  - Getting your own certificate
  - Reassures buyers

# Dev Effort Required

- Perform CAVP algorithm testing
  - Build tools / harnesses to accept input vectors from lab and properly format responses
- Guide testing laboratory through source code to demonstrate compliance to functions specified in FIPS 140
- Develop functional test harnesses

# Let's Connect

- @SafeLogic
- www.safelogic.com