



Cybersecurity Tools for Connected Lighting

Aaron L. Temin, PhD, CISSP-ISSAP

Connected Lighting Systems Workshop

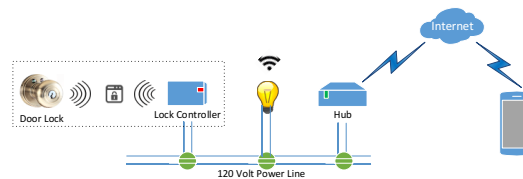
Santa Clara, CA

8 June 2017

Introduction



National Cybersecurity FFRDC

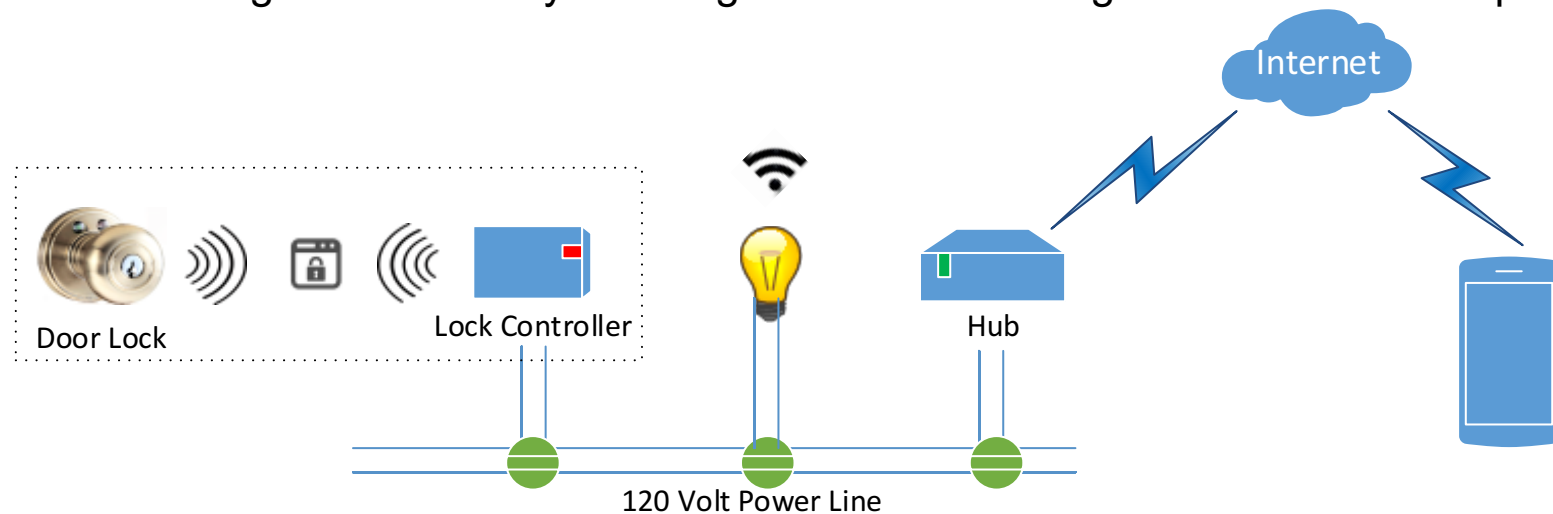


IoT Device Cybersecurity Challenges

- **Device Constraints**
 - Size, weight, power, and storage
- **Lack of Market Incentives**
 - Low cost
 - Increased functionality
 - Short time to market
- **Lack of a Cybersecurity Culture**
- **Lack of Standards**
 - Including interoperability
- **Monoculture of Subsystems**
- **Missing Cybersecurity Functions**
 - Audit
 - Weak or non-existent cryptography
 - Patching
 - Security testing
- **Poor Practices**
 - Lack of certificate pinning, validation, and revocation status checks
 - Hardcoded passwords & keys
 - Security through obscurity

Example: Replay in a System of Systems

- **Defeating replay resistance in a smart door lock +**
 - Multiple vendors products involved in smart home system
- **Setup**
 - Record radio signals emitted by smart lightbulb while locking/unlock door via cellphone



Risk Management

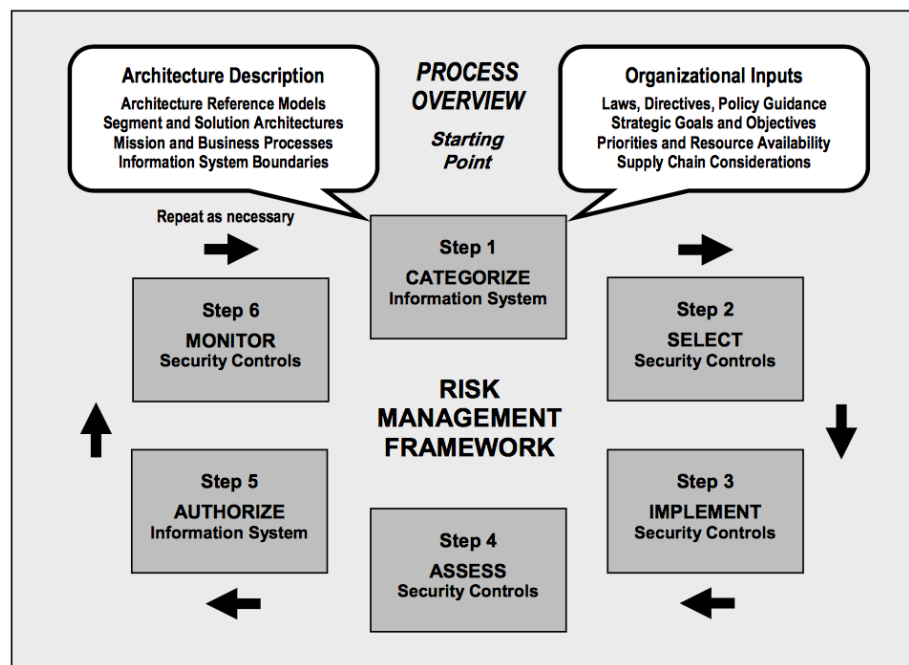


FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

Source: NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems"

Cybersecurity Lifecycle

Cybersecurity Lifecycle

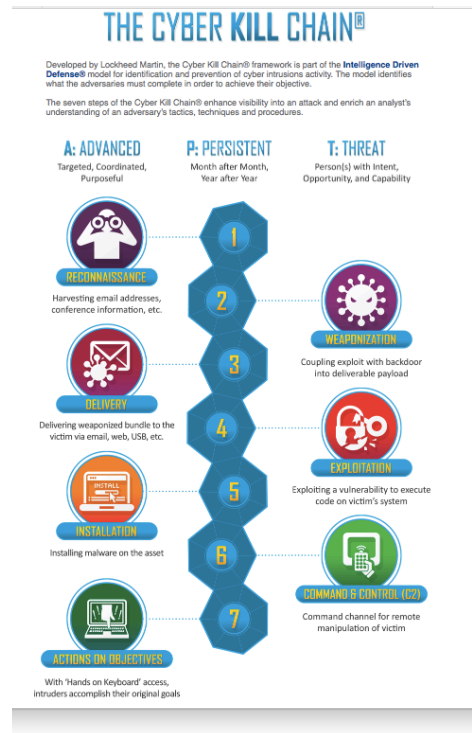
Cybersecurity Lifecycle

Cybersecurity Lifecycle

Figure 1: Framework Core Structure

Source: NIST, “Framework for Improving Critical Infrastructure Cybersecurity”

Adversary (Threat) Modeling



C

Intercept

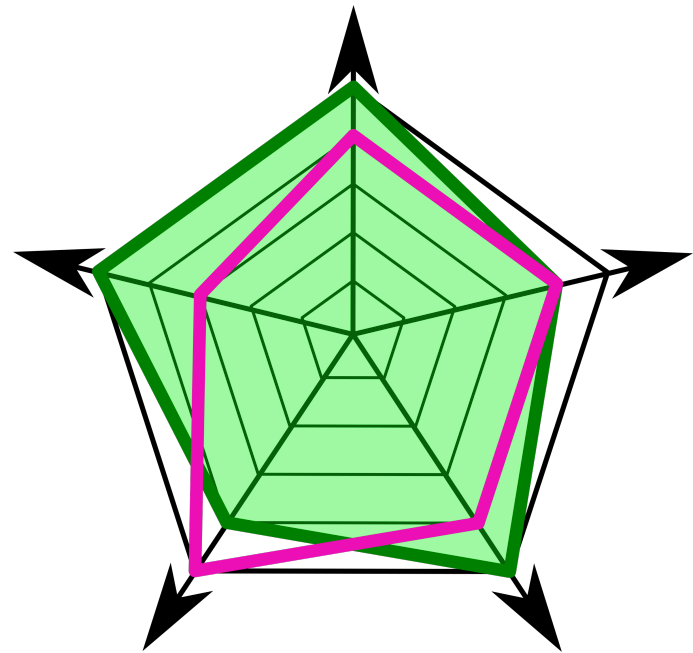
I

Fabricate
Modify

A

Interrupt
Degrade

Measures and Metrics



Final Notes

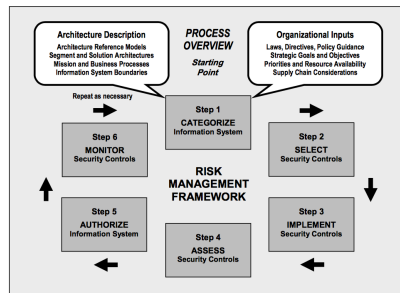
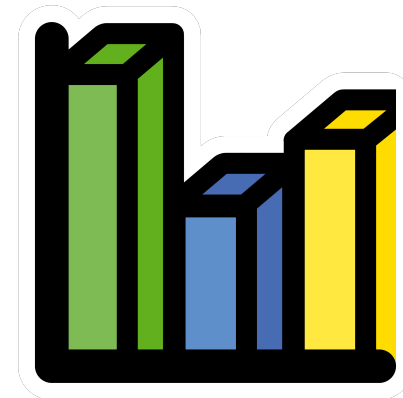
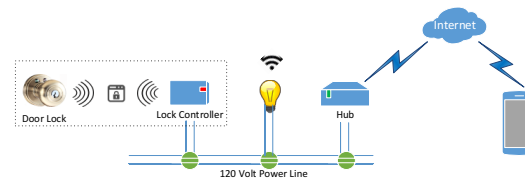


FIGURE 2-2: RISK MANAGEMENT FRAMEWORK



Resources

- **NIST Risk Management Framework,**
<http://csrc.nist.gov/groups/SMA/fisma/framework.html>
- **NIST Cybersecurity Framework,** <https://www.nist.gov/cyberframework>
- **NIST National Cybersecurity Center of Excellence,** <https://nccoe.nist.gov>
- **Adversarial Tactics, Techniques & Common Knowledge,**
https://attack.mitre.org/wiki/Main_Page
- **Common Attack Pattern Classification and Enumeration,**
<https://capec.mitre.org>
- **Scott Musman et. al., Evaluating the Impact of Cyber Attacks on Missions,**
<https://www.mitre.org/publications/technical-papers/evaluating-the-impact-of-cyber-attacks-on-missions>
- **Deborah Bodeau et. al., Cyber Resiliency Engineering Aid,**
<https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-aid-the-updated-cyber-resiliency>