SECURITY INNOVATION

IoT SOLUTIONS

IoT SECURITY ASSESSMENTS & TRAINING

On top of the usual threats inherent to IT networks, applications, and cloud services, IoT devices can create a massive, distributed attack surface.

Security Innovation can help you mitigate this risk by providing full-stack security analysis and support at the physical, communications, and software levels including:

- **Embedded systems** - devices that gather data and interact with the world
- **Firmware** - software that runs on embedded devices
- **Wired/wireless communications** - chipsets and protocols that connect devices and systems
- **Supporting infrastructure** - routers, switches, wireless bridges, and data aggregators
- **Cloud services** - remote servers and RESTful APIs that manage data and control devices
- **Applications** - end user applications that provide access to the data or control the devices

SECURITY ASSESSMENTS

Our assessments match expert skills and tools to the wide range of technologies and security choices for IoT devices. We determine if attackers can bypass authentication controls, provision or assign devices, program devices remotely, and tamper with data.

All of our technology assessments generate and leverage a Threat Model for precision inspection of the security risks, threats, and attack surfaces. Additionally, we provide reports that detail:

- Security and functional objectives
- Vulnerabilities that can compromise your system
- Steps to exploit vulnerabilities found
- Mitigation controls for problems discovered

SECURE SYSTEM DESIGN

Our embedded engineers can help you with early stage activities like capturing security requirements, usage models, and performance requirements. We can also help select the appropriate protocols and algorithms as well as provisioning components, firmware, hardware protections, and policies to ensure the secure operation of your system.

SECURE DESIGN REVIEW

The use of hardware security does not ensure a secure system. These security primitives must be deployed within a secure design to ensure your software is protected from intrusion. A design review will identify high-risk areas, architectural weaknesses, and damage potential in your architecture and offer defense recommendations to reduce the risk of a compromise.

FIRMWARE SECURITY ASSESSMENT

We can analyze the security of device firmware and its update distribution process to identify low-level vulnerabilities and ensure best practices like cryptographically signing updates and using authentication hardware to verify signatures are being implemented.

SECURITY CODE REVIEW

Leveraging static analysis (SAST) tools for breadth and "eyes on" techniques for depth, our engineers conduct a security code review to identify critical security issues before they propagate into numerous and costly to fix vulnerabilities.

PENETRATION TESTING

Organizations rely on our experts to conduct attacks with the same level of determination and sophisticated that an attacker would. Leveraging dozens of specialized tools and proprietary attacks, our engineers will focus on high-risk areas and provide platform- and technology- specific remediation guidance for each

TRAINING

Security Innovation offers general-purpose and IoT-specific courses for secure coding principles, secure design, and security testing. Training is available in self-paced or instructor-led formats.

IoT Embedded Systems Security courses include:

- IoT Security - Fundamentals of Secure Software Development
- IoT Security - Fundamentals of Secure Mobile Development
- IoT Security - Creating Secure Code – C/C++ Foundations
- IoT Security - Creating Secure C/C++ Code
- IoT Security - How to Create an AppSec Threat Model
- IoT Security - Attack Surface Analysis and Reduction
- IoT Security - How to Perform a Security Code Review
- IoT Security - Architecture Risk Analysis & Remediation
- IoT Security - Creating Secure Application Architecture
- IoT Security - Fundamentals of Security Testing
- IoT Security - Classes of Security Defects
- IoT Security - Advanced Software Security Testing

CLOUD EXPERTISE

Our experts have performed dozens of assessments on cloud-based applications as well as Azure and AWS directly.
We provide cloud-specific remediation recommendations to ensure their platforms and plug-ins are secure. This experience yields a deep understanding of how cloud components function and fail together with respect to security.

IoT CENTER OF EXCELLENCE (CoE)

Our IoT CoE conducts ongoing research and assessments on the various chipsets, RTOSs, protocols and deployment platforms. This yields continued methodology, skills and tools development to deliver specialized assessments, training and research including:

SECURITY ASSESSMENT:

- Tablet that interfaces with a power grid
- PLC firmware
- Cloud-based printer
- Breathalyzer
- Point of Sale (PoS) device
- Firmware driver in a popular mobile phone
- Thales Hardware Security Module (HSM)
- Wireless interfaces, CAN bus, and OBD port for connected-motorcycle platform

CONSULTING:

- Co-authored IEEE 1609.2 standard for secure vehicle communications for US DOT
- Security analysis and specifications for commercial automotive satellite radio system
- Customized training for industrial control system (ICS) manufacturer
- Secure coding training for the cloud, middleware, and chipset interfaces
- Researched hardware and wireless attacks on Bluetooth and touchscreen "smart locks"