Foundstone Embedded Systems Assessment

Reducing risk by discovering security vulnerabilities in your embedded systems

The Internet of Things (IoT) is no longer a futuristic concept. It has become a reality—representing the interconnection of specific embedded computing devices within the internet infrastructure. Offering advanced connectivity of devices, systems, and services, IoT goes beyond machine-to-machine communications. Embedded systems include smart thermostats, TVs, smart appliances, printers, routers, car "infotainment" systems, and more. With Gartner predicting nearly 26 billion embedded IoT devices by 2020,[1] there is a critical need to assess and protect these systems from breaches and attacks.

Analyzing Your Critical Components

The Foundstone® Embedded Systems Assessment is based on a proven methodology followed by skilled consultants trained to analyze the critical components of any embedded system. These embedded systems include the underlying operating system (for example, RTLinux or VXworks), firmware, communication protocols (for example, CAN bus, ZigBee, Z-wave, Bluetooth, Wi-Fi), hardware interfaces (for example, USB, HDMI, Serial, 802.11 Ethernet), administrative interfaces, network services (for example, Open SSH, Telnet), embedded web browsers, back-end services, persistent data storage, cryptography, authentication framework, etc. Using manual techniques, proprietary and commercial tools, and custom programs created uniquely for each system being assessed, our consultants can pinpoint specific vulnerabilities and identify underlying threats.

Foundstone Consulting Experts

Foundstone consultants have skills in both application and network security, which are required when performing complex embedded systems assessments. Our consultants are trained in reverse engineering, debugging, and fuzzing, but can also develop custom scripts onsite during the engagement. Our rigorous embedded systems assessment methodology is developed based on our breadth of experience testing embedded systems ranging anywhere from smart TVs and medical devices to avionics systems and kiosks. Our security experts make our engagements unique because of the following:

- Our proprietary and up-to-date testing process consists of more than 100 manual checks.
- We ensure exceptional accuracy by relying almost entirely on proven manual testing rather than on automated systems.

Benefits

- Feel confident that your system is secure through expert vulnerability testing and investigation.
- Gain the most from IoT knowing you have secure systems.
- Employ a proactive approach to security assurance before moving systems into production.
- Know that our team will analyze your risk and the potential impact to your business—incorporating that into our risk calculations.
- Gain knowledge of testing techniques, issues, and remediation for future strategic planning or issues.

- Our strong emphasis on manual testing allows us to discover critical business-logic bypass and authorization issues that automated scanners overlook.
- Our training program, comprehensive methodology, and strict quality control ensure that customers experience virtually no false positives.
- We actively and consistently transfer knowledge of testing techniques, issues, and remediation to our customers.

Foundstone Services consultants are certified in their areas of expertise including CISSP, CEH, CISM, PCI QSA, and GIAC. They've undergone rigorous background investigations and interviews, and have passed comprehensive testing.

Penetration Testing Methodology

The Foundstone methodology is key to ensuring our customers are protected. Our detailed, methodical approach to penetration testing creates assessments that are effective, efficient, and repeatable. While the methodology followed by our consultants supports consistency, it also supports creative problem-solving and the ability to leverage white-hat hacking skills. The methodology includes:

- Discovery
- Configuration management
- Authentication
- Authorization
- User and session management
- Data validation
- Error handling and exception management
- Data protection

> **"When I was asked why I chose Foundstone Services, I thought, 'Would I want to hire a company that runs the tools and reads the books, or should I hire the company that writes the tools and writes the books?' The choice was simple."**
>
> —Foundstone client

Reporting and Recommendations

As our consultants complete their investigation and testing, the results and recommendations are captured and communicated throughout the engagement. Our quality reporting includes:

- Detailed description of the vulnerability
- Steps to reproduce the findings
- Affected functionality/parameter/URL/application
- List of tools used and download locations
- Exploit(s) to reproduce the findings
- Detailed descriptions of instances, samples, inclusive lists, and site-wide issues
- Technology-specific recommendations
- Risk calculations using models that incorporate application risk rating and business context:
  - Foundstone's Approach: Impact and Exploitability
  - CVSSv2 (Industry Standard)

Related Foundstone Services

- Web Application Assessment
- Web Services Security Assessment
- Thick Client Assessment
- Mobile Application Assessment
- Security Code Review Assessment
- Application Threat Modeling
- Software Security Maturity Assurance (SSMA) Assessment/ S-SDLC Gap Analysis
- Writing Secure Code Training (Java, .Net, C/C++)
- Secure Coding Policies and Standards

Final Report and Summary

Our team will deliver a comprehensive technical report in the format of your choice. After thorough review-board approval, we deliver the report broken into the following categories:

- Executive Summary
- Summary of Strengths
- Benchmark Data upon request
- Testing Notes
- Report Card
- Strategic Recommendations: People, Process, and Technical
- Findings and Recommendations

Discounted Retesting

At the conclusion of your engagement, Foundstone consultants will list all discovered vulnerabilities based upon a ranking of high, medium, and low. At a discounted rate, we will perform a retest of each of the discovered vulnerabilities within three months of the completion of your engagement. This will allow you to validate that your security remediation efforts resolved all vulnerabilities discovered by our services.

Why Foundstone Services

Enterprises should never feel like they are on their own when it comes to protecting critical corporate digital assets—especially in an emergency. Foundstone Services is your first responder, available to help you quickly identify a breach and remediate further damage.

We are seasoned security consulting experts skilled at identifying network and application vulnerabilities, providing remediation recommendations, and helping organizations design ironclad security programs and enforceable policies. Couple this prevention with security training from our industry-leading experts, and your organization will be well prepared to combat emerging online threats and defend your valuable assets.

Learn More about Foundstone Services

Fill the gaps in your information security program with trusted advice from Foundstone Services—part of the McAfee® global professional services organization that provides security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Speak with your technology advisor about integrating our services. You can get more information at **www.foundstone.com**.

[1] Forecast: The Internet of Things Worldwide, 2013, Gartner Research.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

62320ds_fs-embedded-systems_0316
MARCH 2016