SERVICE DESCRIPTION

Embedded/IoT Security Assessment

Service Scope

Trustwave's penetration testing services are delivered by SpiderLabs, an advanced security team within Trustwave focused on forensics, ethical hacking, application and network security testing. The team has performed thousands of forensic investigations, ethical hacking exercises and application security tests globally.

The broad experience of the team extends beyond regular corporate information technology environment to various embedded environments including:

- Embedded Systems and Hardware
- ATM/PoS Systems
- Telecommunications Infrastructure
- Wireless/RF Technologies
- Industrial Control Systems
- Smart Grid
- Building Management Systems

Trustwave SpiderLabs' Embedded and IoT Device Penetration Test is a modular test designed to assess the security of the target system/s when subjected to attacks based on industry standard and cutting-edge techniques. A full test focuses on the following areas:

- Local hardware security
- Remote network-based attacks
- Software/Firmware testing & Web/Mobile application security
- Radio communication security

Each test will provide a detailed deliverable with both tactical and strategic recommendations to improve the security posture of the target system. These recommendations are both actionable and advisory in nature and are presented to the customer.

Embedded Device Penetration Test

Approach and Methodology

The Trustwave SpiderLabs Embedded device penetration testing service results in an in-depth test of the target systems and provides a detailed deliverable with both tactical and strategic recommendations to improve the security posture of the target environment.

The approach to assessing the security of embedded systems is an amalgamation of several specialist areas as outlined below.

Embedded Systems Security Assessment

Hardware Security Assessment

The hardware security assessment will determine how susceptible the device is to attacks against the physical hardware. This may include:

- Assessment of physical tamper protections
  - Identification of Failures in Tamper-Proofing
  - Lockpicking
- Non-invasive tests/attacks
  - PCB reverse engineering
  - Data remanence
  - Fault injection/glitching
  - Power analysis
  - Acoustic analysis
  - Review of diagnostic/test interfaces
  - Exploration of firmware extraction methods
  - Review of cryptographic procedures
- Semi-invasive and invasive attacks (some only available upon special request)
  - PCB modification
  - Decapping
  - Microprobing
  - Optical imaging
  - IC Modifications

Network Communications Assessment

The network communications assessment will review the network interfaces, traffic and transport security controls on the device. This may include:

- Network interface and service analysis
- Passive traffic analysis
- Active traffic analysis
- Analysis of any custom network protocols (text based or binary):
  - Reverse engineering
  - Protocol fuzzing
  - Exploitation
- Analysis of the implementation and use of any open/documented protocols (e.g. IPv4/6, TCP, UDP, ARP, DNS, DHCP etc.)
- Review remote access interfaces, e.g. VPN, SSH, custom
- Review of any transport security controls (e.g. TLS, certificate pinning etc.)

Firmware, OS and Application Assessment

The firmware, OS and application assessment will review the software running at various layers on the device. This may include:

- Extracting the firmware from the device
- Reviewing the hardening of the embedded operating system running on the device
- Assessment of any binaries and firmware running on the device, including:
  - Binary/firmware modification and patching
  - Filesystem extraction and analysis
  - Search for hardcoded keys/passwords and other sensitive information
  - Reverse engineering and static analysis to identify vulnerabilities
  - Locating outdated/vulnerable software components
  - Assess any integrity or encryption routines
- Assessment of any exposed web applications/interfaces including:
  - Data Protection
  - Information Disclosure
  - Account Policy
  - Session Management
  - Injection
  - Authentication & Authorization
  - Logic Flaws
  - Application Resource handling
  - Cryptographic controls
  - Bounds Checking (e.g. buffer overflows)

Radio Communications Assessment

The radio communications assessment will assess the risk posed by any wireless communication interfaces and protocols used by the device. This may include:

- Replay attacks
- Jamming attacks
- Man-in-the-Middle attacks
- Insecure CRC checking
- Insecure cryptography
- Protocol fuzzing
- Denial of Service (DoS) attacks (used where authorized)
- Authentication configuration

System Vulnerability Identification

Each in scope host and all associated listening services are probed to locate potential vulnerabilities. Using a large working knowledge of exploit techniques, public information, and extensive private vulnerability research, the Trustwave SpiderLabs consultants catalog all the potential attack vectors that may be exploitable.

Vulnerability Exploitation and System Compromise

Trustwave SpiderLabs consultants will then devise several attack strategies as planning step prior to the subsequent phases. As systems are compromised, key security contacts will be notified. When purpose-built exploits or potentially risky exploit code is required to exploit a system, the authorized point of contact(s) are given the opportunity to decide if the particular system should undergo additional tests.

Deliverables

Following the conclusion of the engagement, findings will be made available via the Trustwave SpiderLabs' Managed Security Testing portal. The deliverables will be both strategic and tactical in nature, presented in a drill down format that will be highly accessible to both management and operational staff. Each finding will have a risk scoring associated with it as well as contain detailed technical information pertaining to the nature of the finding. Each finding will also be presented with clear guidance on how to remediate the issue.