4-QUADRANT SECURITY ASSESSMENT METHODOLOGY

ESSENTIAL SMART GRID INTELLIGENT DEVICE SECURITY SERVICES

SMART GRID ENVIRONMENTAL CHALLENGES:
Today, an electric utility uses many different technologies and networks to meet its varied needs for communications – some legacy, some still evolving. Accelerated Smart Grid deployments have dramatically increased the presence and role of intelligent endpoints, controls and sensors in the electrical system. Most noteworthy are utility Advanced Metering Infrastructure, Distribution Automation, and Substation Automation programs. This distributed intelligence requires secure and reliable Field Area Network (FAN) communications and devices, which necessitates rethinking of traditional utility operations technology security. Critical enhancements to traditional security capabilities include:

- New methods, techniques and tools to identify intelligent device vulnerabilities
- New tools to provide visibility into wireless network traffic
- New means to monitor and detect anomalous behavior and potential signs of intrusion
- New capabilities to support forensics and diagnostics

TRADITIONAL APPROACHES ARE NOT ADEQUATE:
The challenges of security assessments and risk management for Smart Grid systems differ from traditional IP-based computer networks in scope and technique. FAN infrastructures consist of a large number of embedded intelligent devices typically in the form of dual-band wireless nodes, signal repeaters, Smart Meters, SCADA Remote Terminal Units, line sensors and various monitors. While powerful, these embedded mini-computing systems are much less capable than their enterprise counterparts and their security controls are typically much less mature. Many of these intelligent endpoints cannot be physically protected and are thus susceptible to both physical and cyber attacks.

FAN wireless networks are heterogeneous and may consist of three or more different radio systems, such as 3G/4G/LTE technologies (usually for backhaul), proprietary access radios, and short range ZigBee Home Area Networks (HAN). Communication is usually carried over a mix of standards-based and proprietary protocols and network technologies, making visibility into the network difficult and rendering traditional IT security assessment methods and tools unusable.

FANs further employ a variety of security controls including public-key infrastructure, mixed asymmetric and symmetric cryptography, new secure broadcast protocols, and proprietary secure-session approaches with many options. Depending upon what security features a utility has chosen to deploy and how those
features are configured, each utility may be susceptible to different, yet related types of attacks. Once vulnerability is identified, mitigation is an even greater challenge as utilities cannot layer on their own security, but instead must rely on vendor-specific solutions. These challenges require a different approach to better understand the attack modalities applicable to each utility’s FAN and its intelligent field devices as well as technology to monitor and detect the presence of such attacks, especially if mitigating controls are not yet available.

**VENCORE LABS 4-QUADRANT SECURITY ASSESSMENT METHODOLOGY**

Unlike newcomers or circumscribed consultancies, Vencore Labs’ 4-Quadrant Security Assessment Methodology, a component of its SecureSmart™ service, combines traditional penetration testing techniques for networks, computer systems, and applications, with a detailed embedded hardware security and unique radio communications analysis capability. The 4-Quadrant Security Assessment Methodology focuses on four areas: wireless (radio), network, software, and embedded hardware/Firmware.

Vencore Labs uses its proven 4-Quadrant Security Assessment Methodology to perform vulnerability assessments and penetration testing across enterprise networks, communications systems, utility and Smart Energy systems, industrial control systems, IPTV and protected content systems. This methodology takes into account the embedded systems nature and deployment of intelligent electronic devices (sometimes over a wide geographical area), extended traditional IT vulnerability assessment and penetration testing beyond application, operating system and networking vulnerabilities for physically secure, IP-based and web infrastructures. Our 4-Quadrant methodology seeks to validate whether the security controls claimed by the system vendor, operator and owner actually exist and are operational as planned. It then focuses on the discovery and means to exploit design, implementation and configuration weaknesses. This methodology is designed to perform the same attacks resulting in operational disruption.

Our 4-Quadrant methodology covers the four quadrants of the vulnerability assessment space for these systems, addressing application and management software, wireless communications, back-end and tiered transportation network access controls, and embedded hardware and firmware. While the results from each quadrant individually provide deep insight, Vencore Labs goes further linking the testing efforts and findings across each quadrant to evaluate cross-quadrant vulnerabilities, linking vulnerabilities together from different quadrants into a larger operational exploit, thus exposing the true risk and potential for damage that is sometimes not apparent when looking at only one category.

- **Passive production network testing with independent field monitoring system**
- **Controls validation**
- **Wireless network mapping, analysis and situational awareness**
- **Wireless traffic analysis and profiling**
- **Active laboratory testing**

- **Wireless (Radio)**
  - Layered networks with mixed IPv4/IPv6 and proprietary protocols
  - Man-in-the-middle attacks between device wireless modem and network and management interfaces

- **Network**
  - Device IPSec credentials
  - IPSec tunnel encryption

- **Software**
  - Circuit board and chip level design security
  - Device memory, processor control (JTAG debugging interface and triple-wire security control)

- **Embedded Hardware**
  - FLASH image analysis
  - Device cloning
  - Credential recovery and modification

**WIRELESS (RADIO) COMMUNICATION SECURITY ASSESSMENT**

Is a specialized capability that seeks to uncover low-level vulnerabilities in the wireless communications beginning with the modulation scheme and coding, media access control, link-level properties, node announcement and control mechanisms and synchronization, routing and transport security up through application layer communication exchanges in wireless systems such as utility ad-hoc mesh and dynamic networks. Advanced knowledge of wireless modulation techniques, digital signal processing, and specialized test instrumentation is required. Vencore Labs performs wireless analysis and examines network traffic using custom tools and special lab configurations to intercept and demodulate over-the-air traffic, decode bit streams, determine protocol in use, analyze communication flows, identify weaknesses and implementation flaws that could be leveraged in wireless-based attacks. Skills and competencies in wireless and radio communications engineering, standards-based protocols and protocol reverse engineering are required.

**NETWORK PENETRATION SECURITY ASSESSMENT**

Seeks to uncover vulnerabilities in the back-end network(s) that typically interconnect customer/end-user facing devices (and networks) with enterprise management and control applications. In Smart Grid for example, this focuses on perimeter and compartment defenses, edge devices, edge routers and gateways, and means to access backend compartments from FANs, internal corporate data networks, vendor remote access, emergency remote access and sometimes Home Area Network (HAN) interconnection. This assessment focuses on edge devices, network bridges and FAN head-end and Element Management Systems that are used to configure and maintain FAN components. This portion of the 4-Quadrant assessment requires skills and competencies in packet/circuit-level analysis and fixed and wireless networks and transport systems.

**APPLICATION AND MANAGEMENT SOFTWARE SECURITY ASSESSMENT**

Seeks to identify vulnerabilities in both head-end management server applications and middleware that interconnect the head-end to enterprise buses and business support systems. Application and management software assessments typically involve the assessment of web-based technologies, service oriented architectures, web services interfaces, databases, crypto servers and support components. Activities include testing for Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks, privilege escalation, authentication and authorization controls and known exploits. It includes performing a combination of automated scans and manual testing techniques, eliminating both false positives and false negatives. It includes platform configuration analysis and operating system hardening analysis, and may include source code inspections. This portion of the 4-Quadrant assessment requires skills and competency in enterprise service architectures, web technologies, computer science and security vulnerability testing.

**EMBEDDED HARDWARE AND Firmware SECURITY ASSESSMENT**

Is a specialized capability that seeks to uncover vulnerabilities related in the embedded circuitry, such as the storage and use of device credentials, protection of memory and program execution, program logic integrity, on-chip debugging and development functions, and a variety of other low-level weaknesses. It typically involves reverse engineering, circuit modifications, and firmware analysis using special techniques and tools. Firmware analysis on field devices involves disassembling and manipulating code at the lowest level to subvert security controls, take control of field components, reconfigure or clone devices, install rogue code, and possibly propagate malicious code to other nodes. This portion of the 4-Quadrant assessment requires skills and competency in electrical engineering, embedded systems, software vulnerabilities and reverse engineering.

**THE VENCORE LABS ADVANTAGE:**

There is always a risk when introducing new equipment and/or new manufacturers into network infrastructure. For this reason utilities need a comprehensive approach to assessing vulnerabilities and mitigating them both before deployment decisions are made and throughout the products’ lifecycle. We provide utilities with comprehensive, holistic and insightful vulnerability assessment and penetration testing in all four quadrants. The Vencore Labs’ 4-Quadrant Security Assessment Methodology is the only industry approach that can effectively identify vulnerabilities and develop mitigation plans to prevent malefactors from exploiting these vulnerabilities.