NETWORK ENABLED SECURITY FOR EMBEDDED & IOT SYSTEMS (NESES)

NESES is a network-centric security architecture for protecting Internet of Things (IoT) devices. It utilizes IoT Radio Frequency (RF) signatures, scalable virtualized network functions, software-defined network fabrics, and machine learning to secure IoT devices from a variety of threats. NESES software is intended to be deployed inside IoT gateways to prevent network-based attacks. It can identify IoT devices based on their physical and media access traffic fingerprints and apply appropriate security polices to prevent attacks originating from the Internet or other physically compromised devices.

Need for NESES

Internet of Things (IoT) and embedded systems present a significantly different set of security challenges than enterprise IT systems, which traditionally feature host-based security measures, patch management, and network perimeter defenses. The scale of IoT networks, low on-device compute resources, and high expected longevity of "things"—esp. in the context of energy grids, industrial, and transportation systems—means that it is difficult to keep them patched through their lifecycle to keep up with the evolution of security threats and defensive security technologies.

IoT security is a complex challenge that involves addressing:

- Low device security capabilities and resources
- Risks associated with IoT's connection to the Internet
- Difficulties with patching IoTs over expected longevity (decades) of IoT infrastructure
- High scalability needs
- Large legacy deployments

Our Approach

NESES has a fundamentally different perspective on IoT security from the current industry focus on device security features (OS, software, reliance on patches) and Cloud based solutions. NESES aims to reduce the risks associated with outdated and un-patched security in IoT devices by enforcing security controls at the network edge. At the same time, by reducing the need to place security functions in embedded systems, we expect to gain efficiencies in device performance and lifecycle cost from reduced power, space, weight, operations, and maintenance needs.

NESES builds IoT-specific security intelligence at the network edge, where it has visibility to PHY and IP layers, and can be centrally managed and updated without changing deployed IoTs. It deploys network-based intelligence inside Smart IoT gateways to identify IoT devices based on a multi-layer set of attributes and applies appropriately configured security functions at the network's edge.

Benefits

- NESES architecture allows legacy and new IoT devices to be secured against ever-evolving threat landscape.
- It is a non-proprietary architecture for IoT gateways that provides IoT traffic visibility and control to network defenders.
- It provides simplified management and greater scalability of security functions using service chains of discrete, containerized, virtual network functions inside Smart IoT gateways.
- Machine Learning based IoT RF signature fingerprinting is used to detect and stop tampered & impersonating IoT devices, and alert on abnormal RF conditions.
- Centralized management of Smart IoT gateways using on-premise or cloud-based tools is supported for flexible and scalable deployments.

MITRE

Competitive Advantage

NESES could be used to augment commercial offerings in Industrial IoT gateways and enterprise segmentation solutions. Industrial Internet of Things (IIoT) gateways are used to convert message protocols to interface disparate and often proprietary networks. Gateways generally integrate security functionality specific to the industrial protocols used, but they typically do not support cross-layer (physical and network layer) security and scalable security service chains that NESES could offer.

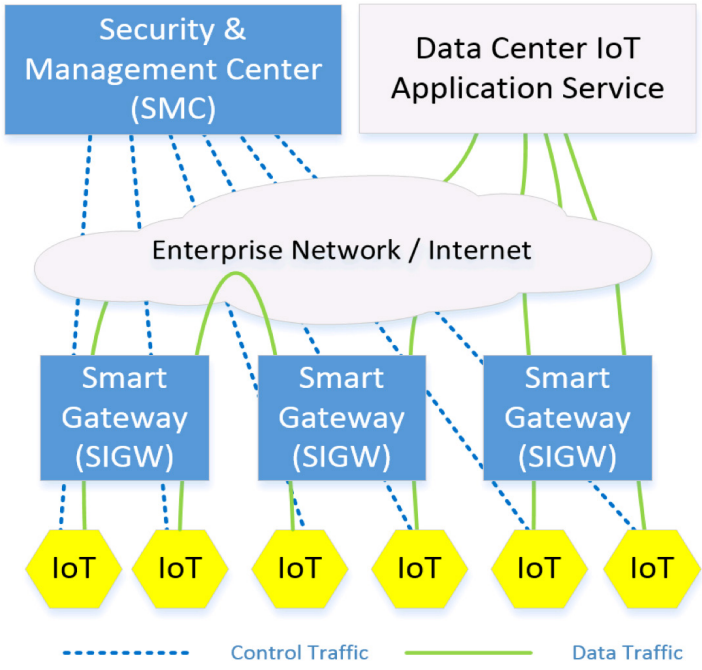

Figure 1: NESES high-level architecture. RF fingerprinting functions and network security service chains reside in the SIGW

Licensing Opportunities

The MITRE Corporation is seeking licensees for commercial development of the NESES technology. NESES prototype technology has been demonstrated in laboratory settings and is available for licensing to interested companies.

For more information, please contact: techtransfer@mitre.org

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD