DHS Science and Technology Directorate

Homeland Security

Science and Technology

MICROELECTRONICS SECURITY CONCERNS

Microelectronic parts within deployed critical systems such as 5G infrastructure and industrial control systems (ICS) are acquired through a supply chain that typically includes not only largely trusted system integrators and/or suppliers, but also numerous entities that have fabricated, tested, and packaged the integrated circuits (ICs); fabricated the printed circuit boards (PCBs); populated these PCBs with ICs and other components; installed firmware into these board-level assemblies; and have added these board-level assemblies into subsystems that are finally integrated into the delivered system. Many entities in these highly complex and global supply chains are untrusted, with some possibly controlled by adversarial foreign governments. Moreover, the specialization and production volume aggregation that has driven the increase in supply chain complexity and geographic distribution has resulted in significant cost-savings for commercially available ICs and PCBs, but also has resulted in making it prohibitively costly to piece together a supply chain that only consists of trusted entities.

In light of these considerations, the problem of ensuring authenticity and security of 5G or ICS microelectronic components should be addressed by verifying that the delivered parts are authentic. The verification method should be highly accurate, cost-effective, and easily and rapidly deployable.

HELPING SECURE 5G INFRASTRUCTRE

In its Secure and Resilient Mobile Network Infrastructure (SRMNI) project, Atlanta-based Aether Argus is developing a firmware-anomaly detection system for 5G and ICS infrastructure components that will monitor device the electromagnetic emissions (EMEs) to detect operational irregularities.

The solution is a novel and unique approach to identify possible firmware supply chain attacks and detecting runtime (software) exploitation for legacy and 5G mobile core network elements (MCNEs), ICS and internet of things (IoT) devices.

Given the increased risk in the global supply chains, there is a clear need for products that can efficiently and effectively inspect hardware elements of connected devices and components for evidence of tampering. This need indicates a market opportunity for products to secure electronics-oriented goods, especially 5G devices, ICS and IoT.

The technology relies on analog side channel signals that are nondestructively collected while the device (or a specific integrated circuit) is performing its normal power-up, self-test, and/or functional testing while the system is operating normally.

IDENTIFYING ATTACKS ON MCNE & IOT

By monitoring and taking advantage of EMEs, the solution will identify anomalies in performance of devices. This will support further investigation by providing a new detection capability for supply chain attacks on MCNEs/ICS/IoTs by tracking EMEs both prior to deployment and while the system operates.

Such checking can be done in the lab or opportunistically on field-deployed systems. Furthermore, if the solution is deployed as part of an MCNE/ICS/IoT installation, it also will be able to track the runtime behavior of the device throughout its operation and alert operators. It can be paired with an automated response system that restarts or quarantines devices, reinstalls a “clean” firmware image, or undertakes other predefined actions.

One of its key advantages is that there is no need to install software on a device, and the monitoring of the vetted device occurs nondestructively and out-of-band. AetherGuard is “invisible” to attackers and cannot be subverted, as is the case with solutions that add software (or even hardware) to protect a device and, therefore, imposes zero overhead on the monitored system. A valuable use-case is to use AetherGuard as part of device-acceptance testing or quality control workflows for device production.

UPCOMING PROJECT MILESTONES

- Project Demonstration—August 2021
- Versions 3, 4 & 5 of Design & Capabilities documents—through February 2022

SRMNI R&D PERFORMER

Aether Argus Inc., Atlanta, Georgia.