DHS Science and Technology Directorate

Homeland Security
Science and Technology

EMBEDDED DEVICES ARE VULNERABLE

Embedded devices are critical components of 4G and next-generation 5G telecommunication networks but still are vulnerable to cyberattacks. Vulnerable firmware in embedded devices in mobile infrastructure allows for both direct attacks against the device firmware as well as more complex attack chains that require compromising devices inside the network infrastructure or internet of things (IoT) devices.

Existing layers of defense such as secure boot help but only protect against specific attack chains. Direct defense in device firmware is needed to provide the defense in-depth needed for protection against modern attack chains. Firmware level layers of defense could detect and prevent zero-day exploits and advanced attack techniques such as Return Oriented Programming chains.

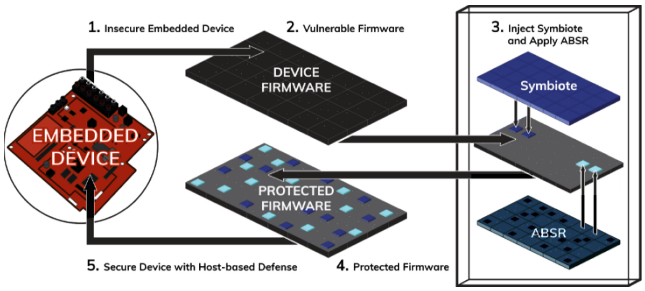
MITIGATING EXPOSURE TO ATTACK CHAINS

Through this Secure and Resilient Mobile Network Infrastructure project, Red Balloon Security is integrating its patented firmware hardening and runtime protection technologies—Symbiote and Autotomic Binary Structure Randomization (ABSR)—into mobile network infrastructure embedded devices to mitigate exposure to a wide range of attack chains.

Symbiote is a host-based defense injected directly into the firmware binary and runs parallel to normal device execution, providing runtime protection to detect attacks and respond in real time.

ABSR provides firmware hardening via automated attack surface reduction and randomization of memory and code at the binary level. The Symbiote and ABSR modifications can be made in minutes following a normal firmware built and deployed via existing firmware update channels.

Red Balloon will expand its Symbiote embedded defense technology to defend against mobile network infrastructure firmware attacks such as buffer/heap overflow, rootkits or attack chains involving any embedded or internet of things device. A key feature of this project will be the development and testing of a new capability to modify firmware to add or remove functionality.



Red Balloon Security injects firmware hardening and runtime protection into embedded device firmware.

Red Balloon Security also will develop prototype integrations in relevant 5G mobile network infrastructure devices and will reach out to mobile network infrastructure vendors to partner in incorporating firmware hardening and runtime protection into their devices.

PREVENTING FIRMWARE-LEVEL ATTACKS

Symbiote and ABSR provide a variety of firmware hardening and runtime protections, preventing most firmware-level attacks, including memory corruption, command injection, privilege escalation, rootkits, buffer overflows, and heap overflows. In this project, randomization is being added as a defense against memory-based attacks that allow attackers to gain control of systems.

These technologies also provide a deeper level of forensics than the current state-of-the-art technology that sends only application logs by integrating with existing Security Information, Event Management, and Intrusion Detection Systems to report security events.

The increase in firmware security will help organizations meet existing and potential future compliance requirements in addition to discouraging and thwarting attackers by increasing the work-factor to successfully attack a system.

UPCOMING MILESTONES

- Design document—June 2021
- Prototype demonstration—June 2021

SRMNI R&D PERFORMER

Red Balloon Security, New York, New York.