MOCANA

How to Defend Against Ransomware, Viruses and Worms

From Cybercrime to Cyber Warfare

In the past several years, the frequency of dangerous cyber attacks has picked up significantly. Stuxnet, Shamoon, Black Energy, the Mirai Virus, Brickerbot and WannaCry have taken advantage of numerous vulnerabilities in computer systems, industrial control systems (ICS) and IoT devices. These hacks have compromised more than just data privacy by impacting the safety and reliability of critical infrastructure and services. Modern cyber attacks represent a dramatic shift from cybercrime to all-out cyber warfare.

Multiple Vectors of Attack

Using physical security breaches, social engineering, propagation, and cyber attacks, hackers are able to use inbound and lateral attack vectors to infect a system with malware. Once in a system, the malware propagates itself between networks and individual machines while probing for vulnerabilities to exploit. Viruses, Trojan horses, worms and other malware embed themselves in the OS, application or network and carry out missions like encrypting critical files, spoofing false data to an HMI, changing set points on RTUs and PLCs, or bricking a device altogether.

Something to Cry About

In the case of WannaCry, hackers exploited a known Microsoft Windows vulnerability (MS17-010). The virus infected 200,000+ computers with ransomware; impacting hospitals, auto manufacturers, businesses and other end users just a few days after the initial attack. Once on the system, WannaCry propagates itself rapidly to other systems on the network using peer-to-peer networking built into the Windows network operating system.

Hardening Devices from the Inside Out

Hardening devices by implementing hardware-based secure elements such as TPM, Intel® SGX® and ARM® TrustZone® is critical to ensuring devices have an immutable identity, a first step to establishing device trustworthiness. Using trust chaining to tie multiple cryptographic certificates to a hardware-based root of trust offers a way to significantly improve the integrity of the device. Protecting the device requires implementing secure boot and secure update capabilities to ensure that only cryptographically signed updates are actually installed.

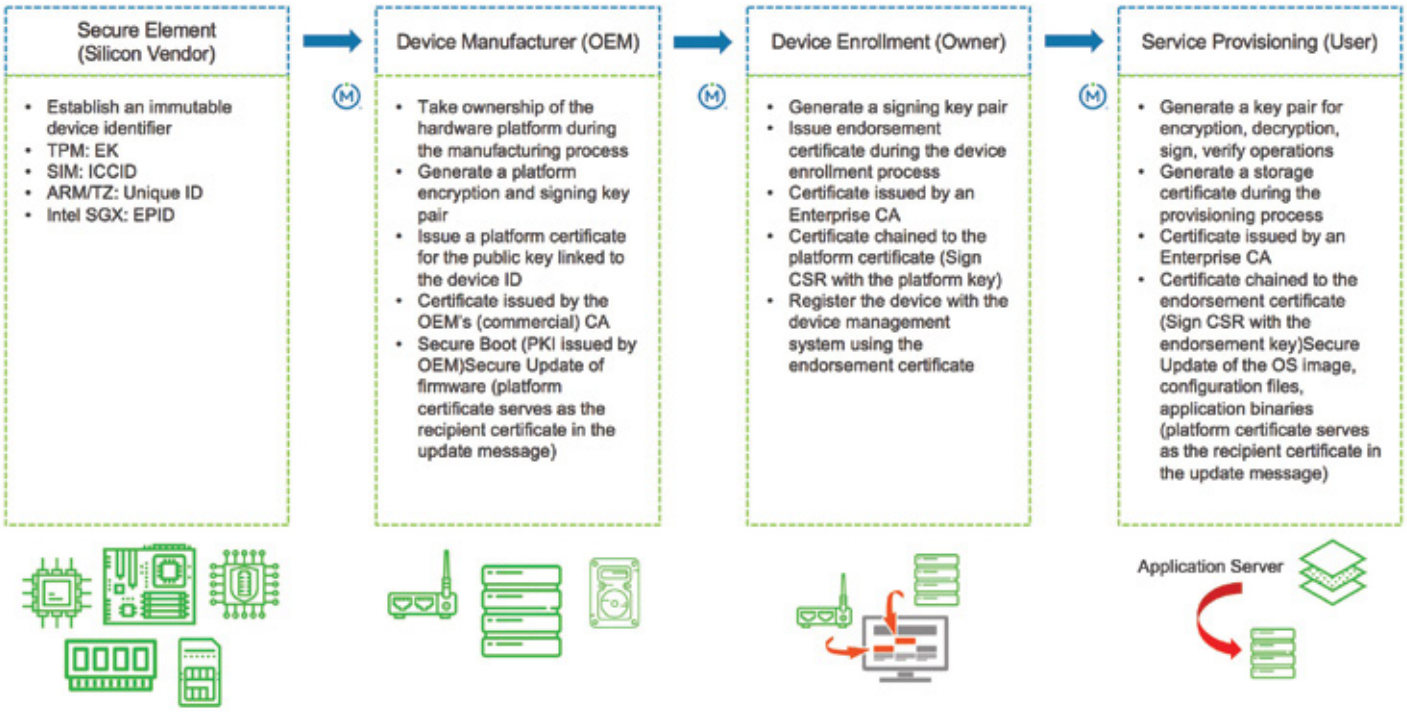
Creating the Chain of Trust

Creating a chain of trust from an established trust anchor installs measurable trust into all platform transactions from power applied through application execution. Building a chain of trust involves using X.509 certificates on the device based on the unique ID of a hardware-based root of trust, such as a TPM. This certificate would be signed by the root of trust and used with a hash of the bootstrap, firmware, kernel and applications on the device to create multiple certificates all signed by the TPM. A single HMAC, comprised of all available device certificates, is then generated. It provides a quantifiable measurement of trust and represents the integrity of the device. In this way, the end user is assured that the device software has not changed since the last boot.

Only Trusted Updates

Whether it is secure updates or platform/operating system validation, the trust chain works to provide a way to detect unauthorized modification attempts to any part of the operating process of a system. Trust values are established at initial system build/deployment, and are used as the basis for measurement against modification requests.

Build a Workflow to Establish a Trust Chain



Only Trusted Connections

When the trust chain is extended to networks, only systems cryptographically validated and approved would be able to establish a connection to a target system, while refusing all other connection requests regardless of service or port. This significantly decreases the attack surface. While cryptographic trust has been around for a long time (e.g. PKI and IPsec/IKE handshake), the difference that strictly-trusted connections provide is that using processes like trust chaining and platform validation and measurement (hash values) increases the effort needed to gain access to a system by compromising a single certificate and makes system intrusion a more daunting and less rewarding task Even on an unpatched system, an initial attack vector would be denied if the targeted device was using trust chaining since the originating system was likely not a trustworthy platform in the first place.

Building Strength with Multiple Signatories

If an individual certificate has been breached, using multi-signatories forces an attacker to compromise more than just one CA to gain approved access to hardened systems. Requiring the use of multiple signatories for system updates helps strengthen the platform because multiple CAs must participate in the verification of the update (hardware, firmware, OS or application software) prior to approval for installation. Unauthorized systems cannot connect, and if any authorized systems are missing valid trust chains (and thus considered compromised), attempts to modify them will result in policy-dependent countermeasures that range from notification of attempt to total denial and system lock-out to the user.

What Should You Do?

Effectively defending against cyber attacks, viruses, worms and ransomware requires silicon vendors, OEMs, end user companies and service providers to build a workflow and establish a chain of trust. Through using only trusted, hardened devices, large and small enterprises can ensure that their systems are protected against unwanted intruders and malicious actors that may want to compromise networks, steal sensitive information or make connected device inoperable.

MOCANA
111 West Evelyn Avenue,
Suite 210, Sunnyvale, CA 94086
E: sales@mocana.com
T: 415-617-0055