WHITE PAPER

Trust at the Security Checkpoint

Introduction

Security is a process that is bolted on to a workflow. Trust is state that must be baked into the full stack and supply chain. Traditional IT security over the past three decades has evolved around rinse and repeat cycles hoping for the desirable outcome, while cottage industry hackers evolved into a formidable cybercrime syndicate, armed with a sophisticate arsenal of tools and techniques. Exploiting published vulnerabilities before IT review and patch cycles could respond and mitigate threats, and automated morphing of malware signatures and memory footprints to defeat a security industry commercializing threat intelligence without attribution, attackers gained the upper hand. Now, the staging surface is expanding to millions of IoT devices across factories, cities, automobiles, public utilities and homes.

Resilience versus Paranoid Measures

Immunity provides the best form of organic defense and self-healing. Achieving resilience in a process requires redundant controls.

The multilayer security architecture of blocking controls at the perimeter, detection techniques at endpoints, harvesting forensic evidence at compromised systems, machine learning, and inspection of network traffic for behavior and anomaly based detection have failed to thwart many of the high-profile data breaches.

The authentication and authorization centric approaches have proven inadequate in dealing with insider threats. As tightly coupled interactive human-machine systems evolve into loosely coupled autonomous headless systems, the need for risk management based on 'indicators of trust' become more valuable than threat management based on 'indicators of compromise'.

Building trust requires a hierarchical mindset and a bottom-up approach. The participants in a transaction include devices, platforms, applications, users, services and a network fabric. The currency is data, the new oil. The three pillars of resilience are confidentially, integrity and trustability. Confidentially provides assurance that the secrecy and privacy of data while in transit is preserved. Integrity of data guarantees tamper proof transfer of information from data source to data sink. Trustability, a key metric for data analytics and process automation, is the ability to attest to the desired operational state of the data producer and data consumer. In layman's terms, it is establishing the trustworthy posture of a device, an application, a user, a service or a network element in the data flow path (the end to end trust chain paradigm).

Trust Begins at the Device

The chain of trust begins at power on from a root of trust that serves as the genesis of trust. This may be a hardware, software or firmware based secure element that provides an authoritative and immutable device unique identity linked to an endorsement key or certificate from the silicon and/or original equipment manufacturer. The secure element must serve as the custodian of private keys (i.e. on-chip secure storage) and the engine for trusted cryptography. The upper layer of system services, transport protocols, and client/server applications may then leverage the secure element as a trusted enclave to generate cryptographic keys, protect private keys in secure storage, perform encryption, decryption, signing and verification in a trusted execution environment, and generate certificates based on proof of possession of credentials endorsed by a trusted platform.

While the public key infrastructure (PKI) provides implicit trust, a secure element based trust chain provides explicit trust. A secure element may be an instance of a Trusted Platform Module (TPM) based on the Trusted Computing Group (TCG) specifications, a TrustZone of an ARM processor, a Software Guard Extension (SGX) or Enhanced Privacy ID (EPID) of an Intel processor, a cryptographic service engine on a SIM or MicroSD card. The transport protocols and end-user applications must remain agnostic to the processor, operating system and secure element for portability across device form factors and cryptographic agility based on purpose-built device functions. Resource constraints and real-time processing may require integration with cryptographic accelerators on processors, microcontrollers or ancillary coprocessors. Trust enablement by a root of trust is therefore the responsibility of the device manufacturer.

Risk is a Measurement

As the adage goes, trust but verify. Verification requires measurements by a trusted entity at boot-time and during run-time. Boot-time metrics establish a transition from power on to a trusted operating baseline environment comprising of core services and applications that provide the device functions. Run-time metrics establish a continuous and local attestation in real-time of hosted services and applications. Holistic state measurements comprising of trust, operational and configuration metrics provide important indicators of trust. The trustability of a device is a function of state measurements and a trust policy that defines the set of safety and compliance controls for risk detection and mitigation. Further, a critical component of trust assessment includes the ability to monitor applications at run-time. Purpose-built applications use certificates, cryptographic keys, cipher and hashing algorithms to perform operations that produce, analyze and/or transport data. Preserving the integrity of applications

requires a secure update process based on cryptographic envelopes and signatures (instead of hard-to-scale black/white lists of file hash digests) for the delivery of update packages from the content publisher to the field device over-the-air or over-the-network. The TPM provides secure storage (platform configuration registers) for measurement performed by trusted host software during the pre-boot sequence. Intel® SGX technology performs local attestation of enclaves for real-time integrity of code and data pages of a process in execution. The ARM® TrustZone based Trusted Execution Environment (TEE) offers secure boot and a secure file system for integrity measurements. ARM based microcontrollers offer cryptographic services engines and registers for secure boot attestation.

Managing risks at boot, during updates, and in operation requires timely and relevant policy based logs to be generated and reported for event driven analytics by security information and event management (SIEM) services. Visibility requires analysis of deviations in the indicators of trust for diagnosis and application of countermeasures based on active forensic evidence. The significant difference between a threat and a risk is that threats cannot be prevented but risks can be managed. Risk management requires instrumentation baked into the full stack for visibility, control and timely intervention powered by an extensible policy grammar. With virtualization in the information technology (IT) realm and field devices in the operations technology (OT) realm, security stakeholders but deal with the "out of sight, out of mind" reality. Visibility in depth is key to monitor the operational integrity of IoT devices. Control is essential to mitigate risks in a timely manner with policy driven countermeasures.

Imminent Risks in IoT

There are several staging surfaces and attack vectors that IoT devices must address at the hardware, platform and application level to achieve full-stack protection.

1. Inbound attacks exploit published vulnerabilities in hardware and software to cause equipment damage or process disruption.

2. Outbound attacks hijack the platform for nefarious purposes – for denial of service or mission critical service disruption.

3. Lateral attacks amplify risk of exposure over multicast machine-to-machine communication channels, and conduct network surveillance for targeted attack coordination based on harvested system and topology information.

4. Insider threats may expose devices and controllers to malicious tampering, and serve as the modus operandi to circumvent endpoint and edge security controls. Traditional authentication and authorization controls have been proven to be necessary but inadequate. Trust measurements to manage and preserve a trusted operational environment at runtime is essential to plug the gaps.

5. Breach in the supply chain through Bring Your Own device (BYOD), counterfeit components, and implanted Trojans.

6. Misconfiguration of systems that may occur through provisioning of weak cryptographic ciphers and hashing algorithms, insecure interfaces, inadequate protection of cryptographic keys, use of factory default passwords, absence of non-repudiation controls in authentication ceremonies, and inadequate verification to qualify system firmware, configuration and software updates over-the-air or over-the-network.

7. Lack of device level intrinsic controls for audits and historic event logs to harvest and analyze forensic evidence.

8. Side channel attacks based on physical proximity to the cryptosystem through monitoring of analog time, power or electro-magnetic signals.

"I rob banks because that's where the money is."

- WILLIE SUTTON

IoT edge gateways and controllers based on Windows and Linux platforms are the high value targets (nerve centers) for the cybercrime syndicate. The real-time operating system (RTOS) environment (e.g. VxWorks, QNX, ThreadX, FreeRTOS, uCOS) based resource constrained platforms are equally vulnerable to protocol and cryptography exploits because of cumbersome patch management workflows. A root of trust provides user, platform and owner separation of roles. On headless devices, where such a distinction is in the fog, lack of a secure element exposes the private cryptographic keys and symmetric keys that form the basis of implicit trust to achieve confidentiality and integrity of data at the transport layer.

Mocana Security Platform

Managing the device life cycle with a policy and process driven workflow across the supply chain, without platform or vendor lock-in, requires adoption of a trust abstraction and measurement layer that provides methods that are scalable to millions of devices and driven by automation to augment OT services. Migration from open source or commercial point solutions for cryptographic and PKI functions to a trust chain based paradigm requires API equivalency to transition to the full stack trust model. The API compatibility layer provides a quick and easy migration for OpenSSL enabled HTTPS and MQTT applications such as OPC-UA, SFTP, publish-subscribe (messaging), and web services. A simple set of APIs provide applications with the ability to harness the power of secure elements (e.g. TPM) for secure storage of keys and boot measurements, and trusted cryptographic functions. Support for certificate management with Enrollment over Secure Transport (EST) based on the

RFC 7030 specification simplifies issuance, renewal and revocation of X.509 certificates and enrollment of devices based on trusted identity and platform endorsement keys. The ability to generate policy based trust measurements, leveraging a secure element and trusted boot sequence, for application monitoring on devices, without requiring application reengineering to produce event logs for audit trails offers a high degree of resilience. The PKCS7 standards based signed envelope to manage device updates, spanning across the supply chain of content providers, provides a trusted mechanism for change management in contrast to traditional black/white list based solutions that are hard to scale across millions of vendor applications. The solution also offers a seamless mechanism to extend the trust chain to traverse intermediate network elements (such as OT/IT edge firewalls) without breaking encryption in transit.

Cost versus Benefits of Hardening

The time and effort required to harden devices, platforms and applications must be factored against the imminent risks and real challenges in hardening resource constrained systems in terms of memory and processing available, across legacy brownfield devices and a broad spectrum of purpose-built ground-up greenfield devices, to meet safety and compliance standards.

Mocana's modular security stack offers the smallest code footprint written in C, with foreign function interfaces for polyglot applications (e.g. JCA/JCE/JNI interfaces for Java applications). Further code optimizations are made possible with extensive granular compile flags to include only the required cryptographic and hashing algorithms based on device functions. The thread-less architecture and callback interfaces for hardware acceleration provide higher efficiencies to achieve high performance, and portability across multiple vendors, processors and operating systems. Full interoperability is supported based on NIST/FIPS standards, TCG specifications, and RFCs for transport protocols (SSL/TLS, DTLS, SSH, IPsec), wireless (802.11i supplicant), authentication methods (EAP, RADIUS, HTTP-Authentication, X.509 certificate), key exchange (IKE, GDOI) and certificate management (OCSP, SCEP, EST).

About Mocana Corporation

Mocana Corporation provides mission-critical IoT security solutions for embedded systems and the Internet of Things. Founded in 2002, the company developed security software for embedded systems and mobile applications. In 2016, the company spun out the mobile application security business to focus exclusively on IoT security. Based in San Francisco, Mocana serves more than two hundred companies, including many of the largest manufacturing companies in the world that produce critical infrastructure: aerospace, chemicals, defense, electronics, energy, engineering, and transportation. We are privately held. Our investors include Shasta Ventures, Trident Capital, Sway Ventures, Southern Cross Venture Partners, GE Capital, Intel Ventures, Panasonic.

Contact US

Mocana Corporation
20 California Street, 4th floor
San Francisco, CA 94111

415-617-0055

sales@mocana.com