WHITE PAPER

Hardening the IoT Stack

Table of Contents

Introduction 3
End-to-End Trust 4
Cyber Risks vs. Cyber Threats 4
Gap Analysis 5
Achilles Heel of Open Source 5
Raising the Stakes 8
Intertrustability of Systems 9
Trust Must be Baked In, Not Bolted On 10
Lifecycle Protection for an IoT Device 11
Level of Assurance Matters 12
Mocana Security of Things Platform 12
Conclusion 14

List of Figures

Figure 1: Comparison Metrics 7
Figure 2: Intertrustability of the Supply Chain 10
Figure 3: The Chain of Trust for OT-IT Convergence 11
Figure 4: Degrees of Assurance 12
Figure 5: Mocana IoT Security Stack 13
Figure 6: IoT Device Life Cycle 13

Introduction

The IoT infrastructure encompasses a broad array of services and applications orchestrated for the enterprise, home and government sectors.

These include a wide variety of multi vendor devices and platforms. The security, interoperability and connectivity in a loosely coupled network of sensors, gateways, services and applications across operations technology (OT) and information technology (IT) stakeholders requires strategic rethinking of policies and processes in the context of cyber vigilance and resilient systems.

From the brown fields to the green fields, the Internet of Things (IoT) exposes a new set of security vulnerabilities and avenues for compromise by state and non-state cybercriminals. The cybercrime syndicate exploits published exposures in operating systems, application frameworks, communication protocols and open source. This is self evident from the recent distributed denial of service attacks staged by Trojans and botnets from IoT and embedded device platforms. This is also a call to action for corporate boardrooms and solution architects to seriously rethink cross-realm end-to-end trust for convergence of operations and information technologies. The smart cities, smart factories, smart grids, smart vehicles, and smart homes rely on intertrustability as the cornerstone of IoT security.

Today state of the art Information Technology (IT) is driven by security and compliance requirements powered by threat intelligence to manage user devices. The primary risk is theft of intellectual property, such as classified documents or sensitive client information (e.g. name, address, email, password, social security number). The threat intelligence is typically available as remotely sourced indicators of compromise. Security countermeasures are provided by means of a local policy engine (for example, antivirus or host based intrusion detection). Contrary to IT, operations technology (OT) is driven by safety and resiliency considerations for anticipation and preemption of undesirable outcomes. Devices in the IoT sector are unmanaged headless (i.e. no interactive user) special purpose appliances. The risks posed include mission critical disruption of services and loss of human life and/or property. The threats must be sourced locally on a platform instrumented for trust measurements and require a remote policy engine for intervention and remediation.

End-to-End Trust

The first mile of the IoT topology includes a plurality of OT managed ubiquitous connected devices such as sensors, actuators, controllers, and monitors. The last mile comprises of IT managed cloud silos organized as web, application and database tiers. The transit miles include on-premise, field service and cloud edge gateways. The enterprise and cloud connectivity requires a trusted network for secure transport traversing bump-in-the-wire security devices and network elements managed by wide area and broadband network service providers.

Operational integrity measurement and attestation must extend beyond the platform as a service (PaaS) and infrastructure as a service (IaaS) layers to the entire IoT stack. The IoT stack comprises of common industrial protocols such as Modbus, MQTT and WebSockets, and applications for client-side analytics of IoT data feeds and server-side analytics and processes. All these must rely on underlying secure cryptographic functions and mutual certificate based authentication for data confidentiality and integrity. Further, life cycle certificate management poses challenges in scalability and automation for device identification, registration, and deregistration of thousands of IoT elements. Interoperability requires device authentication for trusted connections and a standards based protocol rather than proprietary protocols over HTTP.

Cyber Risks vs. Cyber Threats

Threats may be beyond ones ability to quantify and difficult to eliminate. On the other hand, risks can be measured and mitigated. Compliance alone does not guarantee safety. While in the IT realm, risks are limited to intangible digital assets, in the OT realm tangible assets and human life are exposed to harm.

There are several new challenges that IoT field devices pose – including the need for encryption at downstream devices, and pathways to backhaul big data streams for upstream analytics. But that is not the core problem. In the IT world it is about “users to applications”.

In the OT world, it is "devices to applications" – where devices not only outnumber users, but they have inadequate security baked or bolted in as a technology, policy or process, are unmanaged (like Bring Your Own Device in IT parlance), have no/poor reporting capabilities, and no authoritative identifiers/credentials for on-boarding. That is where one must bridge the divide with (a) device and application tethered to a root of trust, (b) certificate chains and (c) compute/memory/network efficient attestation, encryption, and event logging respectively. Beyond open source and device manufacturers there is an adoption deficit that matters, namely applications. Application developers are primarily focused on vulnerability management as the means to hardening. Applications lack the APIs they need to enable end-to-end intertrustability. That is where a trust chain is required. The devices and applications must be enabled to participate in the trust chain – without heavy lifting on the part of the application developers. Analogous to how the TCP/IP stack abstracted connectivity to enable applications to network without having to deal with the intricacies of the underlying fabric and network protocols.

Gap Analysis

There is a powerful cyber crime syndicate with the means, motive and opportunity for Hacktivism.

They possess the sophistication of methods and tools to orchestrate targeted and coordinated attacks. Hackers exploit gaps in protocols, policies and processes that increase the window of exposure and dwell time of an infection. The risks associated with open source, implicit trust, and non-hierarchical entities warrant closer attention and assessment of the ramifications.

Achilles Heel of Open Source

Undocumented design and code has been a root cause of major security breaches. Embedded open source code poses a far greater risk. Open source tends to be quicker in plugging vulnerabilities due to the community driven nature. Patching is common in third party software packages that embed open source components. Software vendors may not be aware of unpatched code that originated from open and freeware sources. This requires active and close monitoring. The root cause of many application security vulnerabilities may be resident (passively) in the source code. By shielding insecure applications behind perimeter defenses, organizations try to avoid the higher costs associated with baked in security.

OpenSSL is a library. Therefore once a vulnerability is exposed, every affected vendor needs to patch their packages and notify their customers, who then must go through their application development, test, and QA verification cycles before the patch can be applied to production and end user systems across the enterprise. In some large enterprises this can take months because of IT policies and processes. Then there is the matter of supply chain hygiene – partners, suppliers and contractors who connect to the network must also be up-to-date on patch management.

To complicate the process further, OpenSSL may be embedded seamlessly (static binding) in third party (and custom built) applications that IT may be unaware of. Some client-side applications may not go through the same level of due diligence assessments as server side applications often do. Today, many client side applications use MQTT, HTTPS and WebSockets which underneath may be linked to OpenSSL. Hidden open source may be putting your applications at risk (http://www.linuxinsider.com/story/61202.html).

This is the classic window of exposure, dwell time, and cost of harm cyber metrics. A significant number of NIST CVEs are published annually (for example, over thirty in 2016 -https://www.openssl.org/news/vulnerabilities.html). The fact that hackers can take early advantage of published open source vulnerabilities because of the long window of exposure does give them an unfair advantage. While security through obscurity is certainly not a solution by any means, it does put hackers at a disadvantage.

One could fairly argue that these may be true with closed source SSL/TLS protocol stacks as well. A key difference is that not all versions of OpenSSL may have patches available - only the latest version may be supported. This requires all affected packages and applications to migrate to the latest version of OpenSSL – which is never trivial (especially if a FIPS certified version is required). Platform vendors in the supply chain are more likely to provide patches for all supported versions in the field – which is beneficial for application vendors. This renders OpenSSL patch management a "distributed and ad hoc" activity that is difficult to manage and introduces uncertainties.

Open vs. Closed Source Code

Metric	Open Source	Closed Source
Code Reviews	Ad hoc	Formal
Ownership	Community	Vendor
Documentation	Unmanaged (Unreliable)	Managed
Defect Exposure	High (Transparency to developer community)	Medium (Opaque to developers)
Code Churn	High	Low
Quality Assurance	Low	High
Patch Frequency	High	Medium-High
Time to Plug Published Exploits	Medium - High	Low
Hidden Risks	High (Open source code fragments may be embedded in third party software)	Low
Cost	Free to use, Expensive to maintain	Pay for use, Low maintenance

Figure 1: Comparison Metrics

Raising the Stakes

The emerging IoT technologies have a significant global market impact for the enterprise, home and government sectors.

The design and evolution of smart cities, smart factories, smart grid for utilities (energy, water, transportation), smart homes and smart vehicles hinge on a robust and resilient technology stack for safety of operations. The degrees of risk include (a) inbound intrusions and software updates over-the-air and over-the-web, (b) outbound compromised devices, services and applications, and (c) lateral threats that are the epicenter of an attack aimed at network reconnaissance, equipment damage, service or process disruption and data contamination. The OT/IT edge is fundamentally different from the enterprise edge – the traditional demilitarized zone (DMZ). The diversity of industrial protocols, resource constraints, data confidentiality in transit, privacy considerations for anonymity, and the headless device versus interactive user differentiation with regards to authoritative proof of possession of credentials and proof of presence (association) with the device for authentication.

Intertrustability of Systems

Trust may be implicit or explicit, transitive or non-transitive, hierarchical or non-hierarchical. A root of trust (RoT) anchor may be implemented in firmware (ROM), software (flash, RAM) or hardware (ancillary processor or co-processor). The primary capability that a root of trust provides is attestation of keying materials (branches) tethered to the root. The keying materials are made operational by applications (leaves) on the basis of explicit trust derived from the trust chain.

Once the applications are loaded into memory and commence execution, the trustworthiness of the platform is a function of in-process integrity of operations in memory (RAM). The exposure at execution time comes from an application's vulnerabilities (e.g. buffer overflow, privilege escalation, code injection, brute force or side channel attacks) and exposures to an attacker (e.g. protocol or application programming interface based exploit staging surface, co-resident attacker in a multi-tenancy). This phase of trustworthiness requires a trusted execution environment to camouflage the unencrypted code and data in memory and prevent unintended pathways in the call flow graph.

Holistic trust models require continuous and verifiable metrics on (a) data at rest, (b) data in process and (c) data in motion. Data at rest may be protected with symmetric key encryption wherein a protected primary seed and key derivation function dynamically regenerates the symmetric key. Data in process requires secure key operations wherein the private key never leaves the chip in the clear. Data in motion requires confidentiality (encryption based on a one-time session key), integrity (signed message digest) and authenticity (certificate based device identification).

Trust Must be Baked In, Not Bolted On

Fundamental to the notion of a root of trust is the plurality of technologies necessary to build the end-to-end supply chain of trust in a converged OT/IT ecosystem comprising of manufacturing, assembly, field deployment, operations and supervisory controls. The trust chain model begins with the genesis of trust at the anchor point – i.e. the root of trust. The trust becomes transitive in the supply chain, through transfer of ownership from the chip to the printed circuit board (PCB), the device enclosure, and eventually for device enrollment, device management and operations.

Device hardening, based on the desired level of trust assurance, requires the secure platform to be trustworthy through attested identification of the device for enrollment, key generation, certificate issuance, and cryptography for the integrity of data transport and confidentiality of communications between trusted devices. Component level assurance requires protection of keying materials secured by the hardware root of trust for tamper resistance.

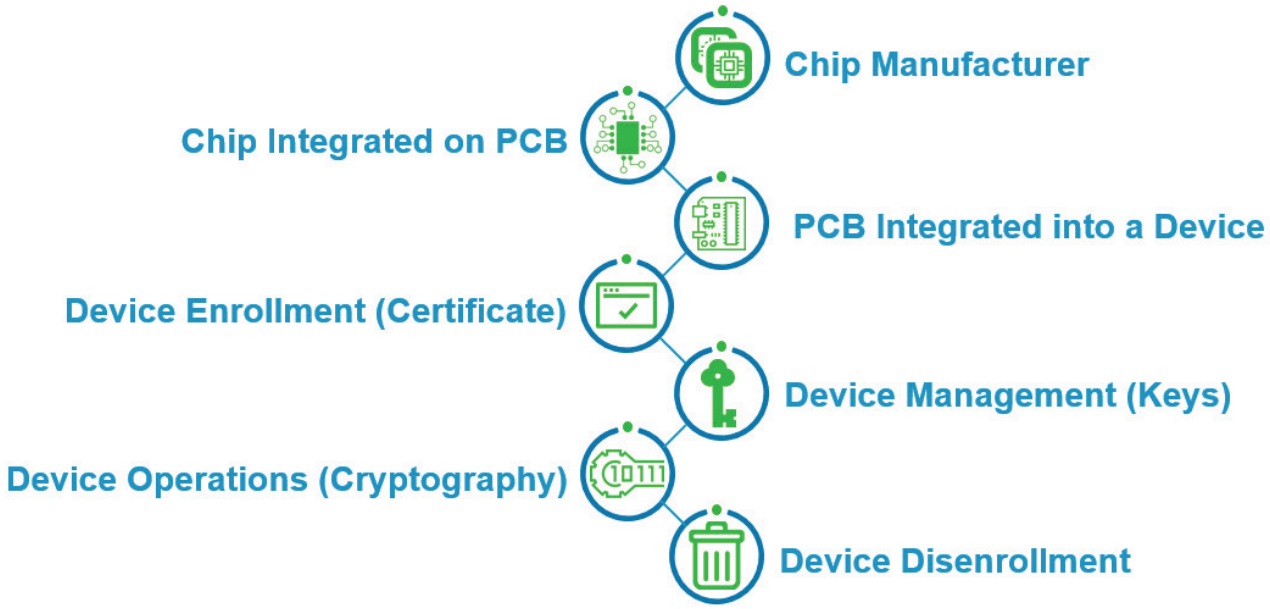


Figure 2: Intertrustability of the Supply Chain

Convergence of IoT devices in the OT realm into the IT managed services realm requires the chain of trust to traverse through the demilitarized zone of edge defenses. The confidentiality and integrity of cross realm data and control flows require a bidirectional trust anchor. The confidentiality provided by encryption, and integrity provided by digital signatures, requires trustworthiness in the keys and certificates that constitute the basic tenet of cryptography.

Security protocols merely provide a means to negotiate keying materials for communications. The strength and protection of keying materials on the devices constitute the quintessential pillars of trust. Further, the proliferation of IoT devices, distributed services, and inter-device group communications necessitates an automated and scalable mechanism to distribute and manage keying materials.

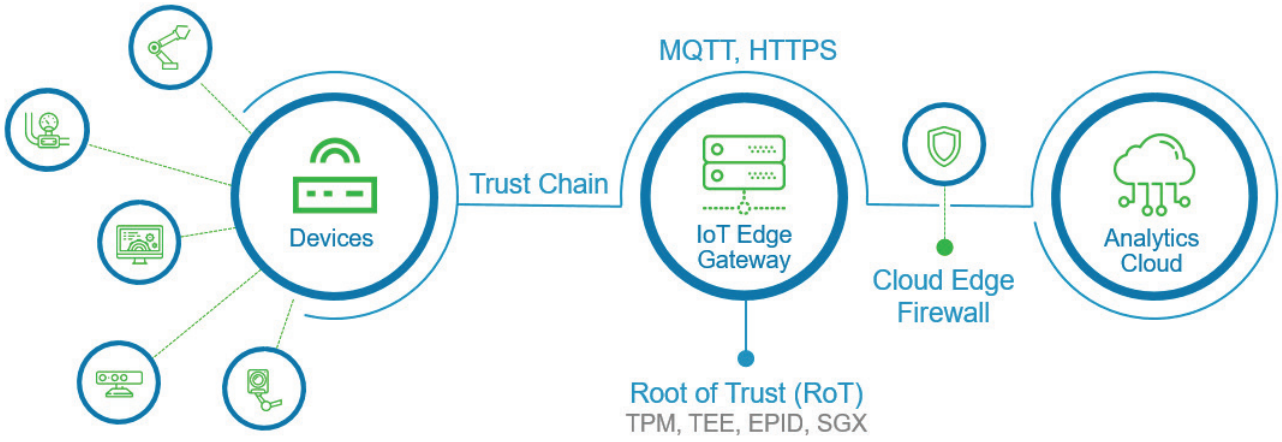


Figure 3: The Chain of Trust for OT-IT Convergence

Lifecycle Protection for an IoT Device

The lifecycle of an IoT device begins with a secure boot at power-on, attested to by measurements performed by a root of trust to verify the integrity of the boot image from a persisted store (e.g. flash memory).

The initial provisioning to commission a device for ownership requires an automated and scalable mechanism to generate an attestation identity for the device to register with an authorized remote management service. Subsequent device updates require non-repudiable signing and verification to harden software distribution to in-field devices over-the-air or over-the-web. Finally, continuous integrity monitoring of the in-service device requires field assessed trusted platform measurements of the boot and runtime profile attested to by specialized security modules anchored to a root of trust.

Level of Assurance Matters

Security is not adequately built-in at the application level (e.g. securing private keys for cryptography, password management, shared secrets, certificate management for mutual attestation). While there are various IoT SDKs for data analytics in the cloud (e.g. Amazon Web Services, Microsoft® Azure, Oracle®, SAP®), there are inadequate provisions for device level analytics to facilitate application hardening and end-to-end trust. Monitoring requires trustworthy measurements for safety and compliance assessment.

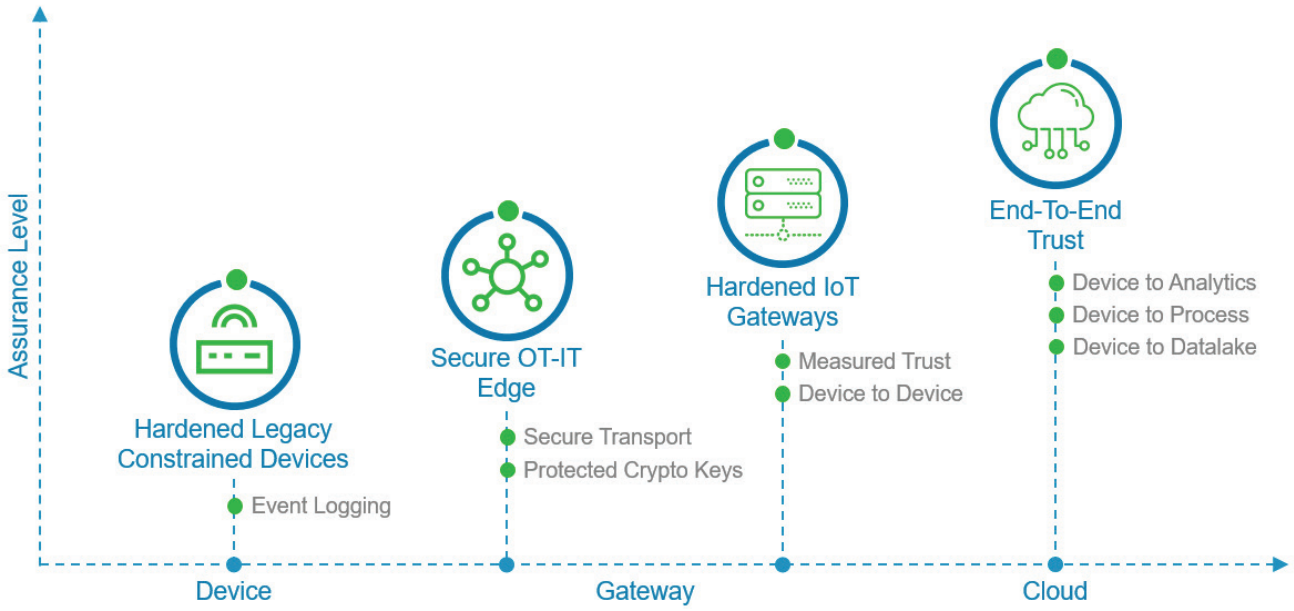
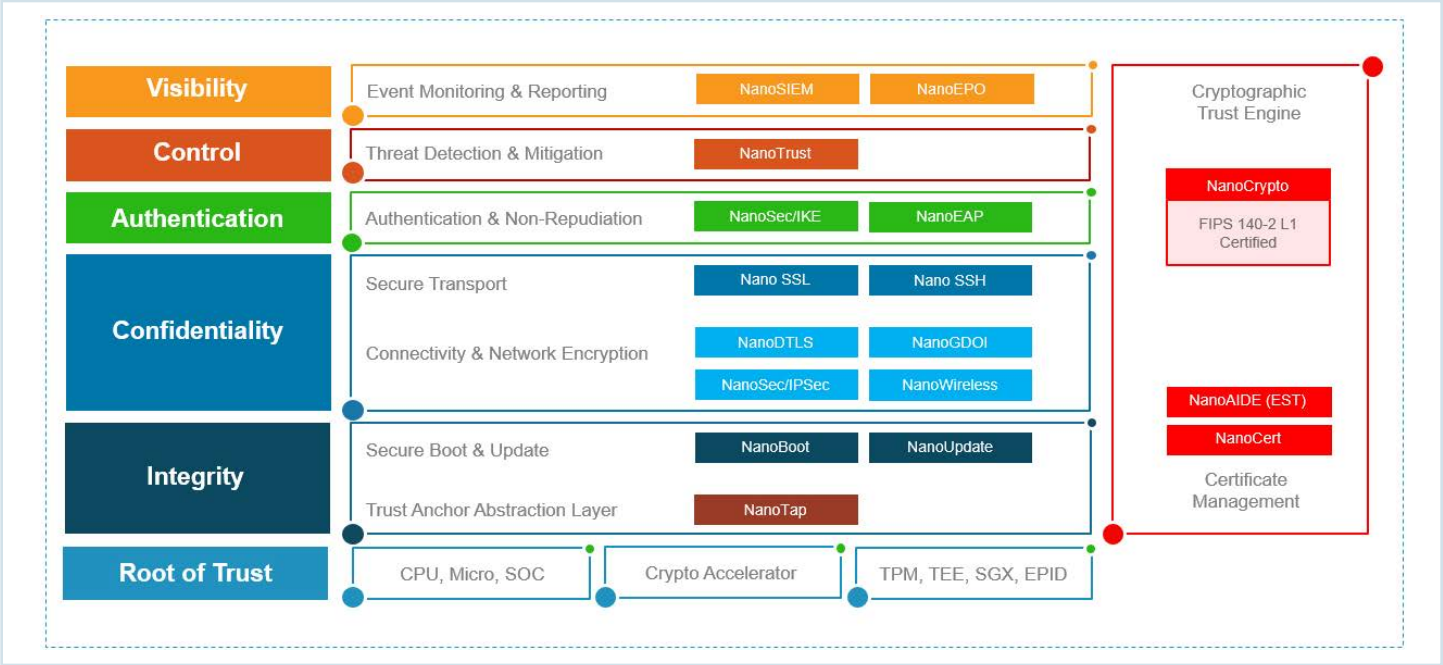


Figure 4: Degrees of Assurance

Mocana Security of Things Platform

Our key differentiator is that trust is baked in (not bolted on) and traverses the supply chain (from silicon vendor, equipment manufacturer, device manufacturer, and platform vendor to the application vendor. The hardening for devices extends from legacy and resource constrained devices to memory-rich devices. The hardening for gateways addresses the needs of OT edge, core platform services, and a plurality of secure elements serving as the root of trust – such as Trust Platform Module (TPM), Trusted Execution Environment (TEE), Intel® Software Guard eXtension (SGX), Intel® Enhanced Privacy ID (EPID), Subscriber Identity Module (SIM) and MicroSD cards. The hardening of services in the cloud includes virtualized secure elements, cloud based HSMs and multi-tenant workloads.

Building the trust chain requires trust anchors, platform hardening, and application hardening with a trust abstraction API layer, a trust bridge at the OT/IT edge, protection of keying materials, and interoperability. A measurements based safety assurance requires boot metrics, application metrics (i.e. execution environment, trusted enclaves) and platform metrics (i.e. configuration and operational). Policy based risk prevention with trust anchors and trust measurements provides a greater degree of safety and resilience than detection centric black/white lists, file signatures, anomalies, machine learning or regular expression based grammar. Local attestation and remote monitoring of boot and runtime indicators for visibility and remote application capability management for control provides a framework for incident response.



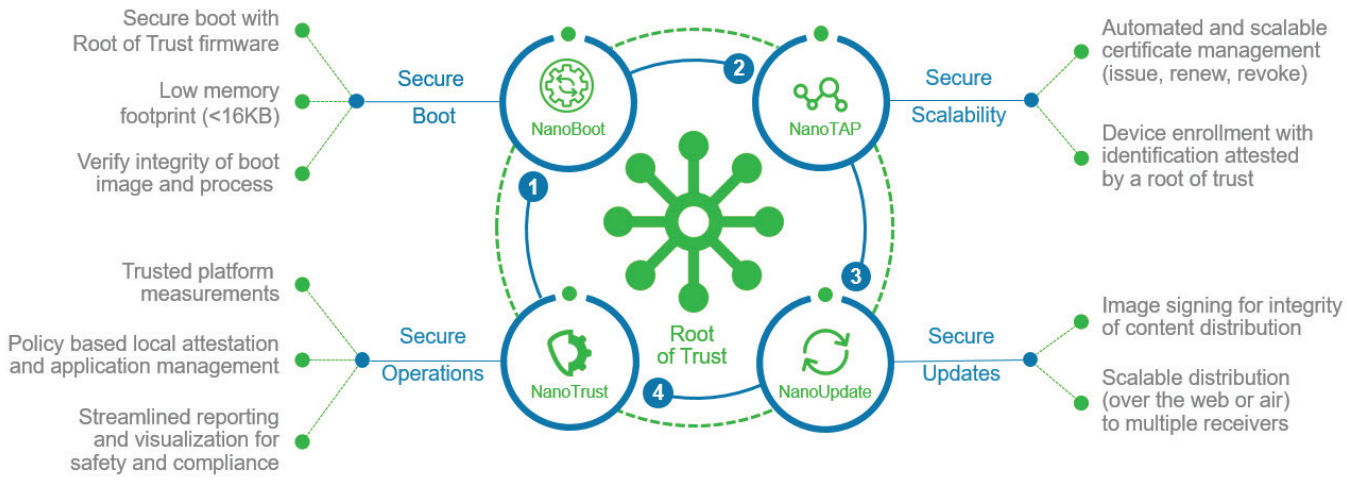


Figure 6: IoT Device Life Cycle

Conclusions

The challenges and opportunities that is evident from the emergence of IoT as a revolutionary catalyst in the industrial, financial, healthcare, retail, utility, automotive, home and educational sectors requires rethinking security as a holistic baked-in platform rather than bolted-on point solutions. Hardening of IoT devices and applications from the production, assembly and packaging lines require a component level trust paradigm. Security is only as strong as the weakest link in the chain. The nature of IoT devices necessitates a multi-vendor multi-platform trust abstraction layer to facilitate device-to-device, device-to-gateway, and gateway-to-cloud secure communications and transport. Enabling inter-realm and intra-realm services requires an automated and scalable platform for distributed analytics and remote monitoring of the trusted entities.

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