



IoT and Security

By Shrikant Shitole and Mohan Raju

In collaboration with Dr. Rishi Bhatnagar



Executive Summary

The Internet of Things (IoT) already helps billions of people. Thousands of smart, connected devices deliver new experiences to people throughout the world. Examples include connected cars, robotic manufacturing, smarter medical equipment, smart grid, countless industrial control systems and many more. Unfortunately, this growth in connected devices brings increased security risks. Threats quickly evolve to target this rich and vulnerable landscape. Serious risks include physical harm to people, prolonged downtime, and damage to equipment such as pipelines, blast furnaces, power generation facilities etc. As several such facilities and IoT systems have already been attacked and materially damaged, security must now be an essential consideration for anyone making or operating IoT devices or systems, particularly for the industrial Internet.

How can anyone secure the IoT? IoT systems are often highly complex, requiring end-to-end security solutions that span cloud and connectivity layers, and support resource-constrained IoT devices that often aren't powerful enough to support traditional security solutions. Security must be comprehensive or attackers simply exploit the weakest link. Of course, traditional Information Technology (IT) systems often drive and handle data from IoT systems, but IoT systems themselves have unique additional security needs.

The security solution should be powerful and easy-to-deploy foundations of security architectures to mitigate the vast majority of security threats to the Internet of Things, including advanced and sophisticated threats. This paper describes the necessity and strategies for easy and effective implementation. No single, concise document can cover all of the important details unique to each vertical. Instead, this paper attempts to provide advice applicable to all verticals, including automotive, energy, manufacturing, healthcare, financial services, government, retail, logistics, aviation, consumer, and beyond.

Protecting Communications

Protecting communication requires encryption and authentication for devices to know whether or not they can trust a remote system. This leaves the core challenge of managing all of the “keys” for authentication. Why does authentication matter? It is dangerous to accept data from either unverified devices or unverified services. Such data can corrupt or compromise your devices, and give control of those devices to some malicious party who wishes to harm devices or harm others through the device. Using strong authentication to restrict such connections helps protect devices from such threats, while helping to keep control of devices and services. Regardless of whether a device is connecting to another device as a peer, or connecting to a remote service such as a cloud based service, the communications must be protected.

Protecting Devices

Protecting devices against attack requires code signing, to be sure all code is authorized to run with run-time protection and to be sure malicious attacks don't overwrite code after it is loaded. Code signing cryptographically ensures code hasn't been tampered after being “signed” as safe for the device, and it can be done at “application” and “firmware” levels, even in devices with only a monolithic firmware image. All critical devices, whether a sensor, a hub, or anything else, should be configured to run only signed code and never run unsigned code.

Integrity of Devices

Still, devices must be protected long after code begins running. Host based protections help here. Host-based protection provide hardening, lockdown, whitelisting, sandboxing, network facing intrusion prevention, behavioral and reputation based security, including blocking, logging, and alerting for a variety of IoT operating systems. Recently, some host-based protections have been adapted for IoT, and now run well without requiring access to the cloud, and without undue strain on limited devices.

Security Analytics

Of course, no matter how well the devices are secured or everything locked down, and no matter how well the devices are managed, some threats can defeat all of those countermeasures to establish a toehold in the devices or applications or systems. For such reasons, it's crucial to have an IoT Security Analytics capability that helps to understand the traffic on the network, flag anomalies that might be suspicious or dangerous, malicious behavior of devices or system, faster detection & response mechanism to advanced threats.

Internet of Things: Transforming Digital India

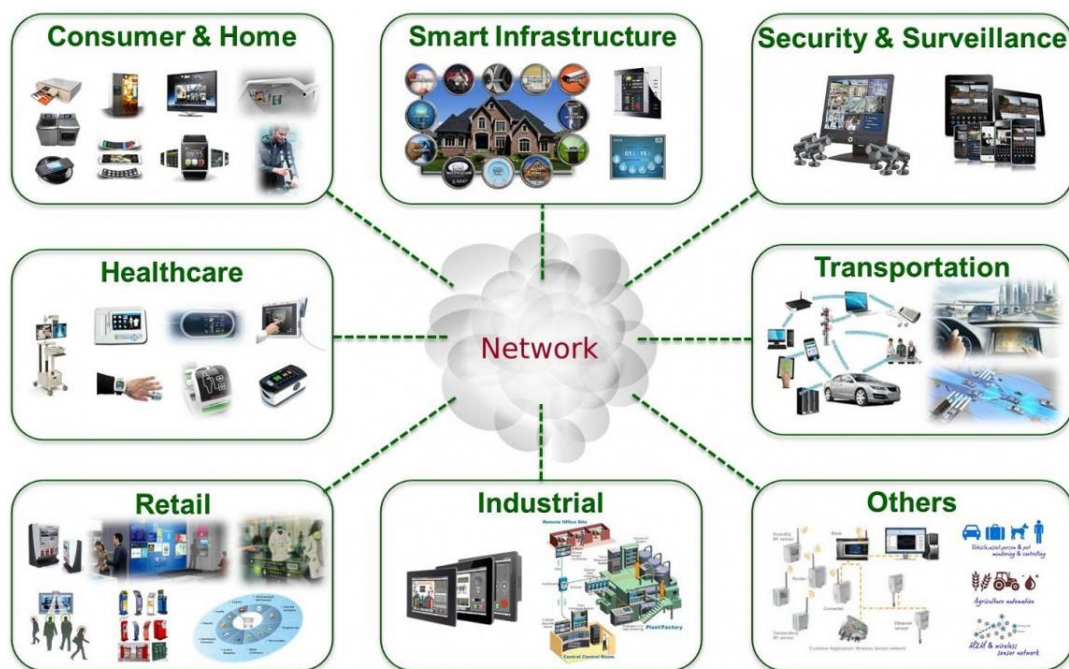
India's economy grew at 7.6% in the year ended March 2016, making the South Asian giant the fastest-growing large economy in the world. With Government's initiatives like Smart Cities, Make in India and Digital India mushrooming startups, there is an enthusiasm that there will be greater innovation in IoT Space in India driving digital economy. As per reports, global IoT industry would be USD 300 billion by 2020 globally. India aims to capture at least 5% to 6% of the overall global IoT industry. The Make in India program will encourage local and global companies to manufacture IoT infrastructure in India, and supply them to local and global markets.

IoT will play a major role in the transformation of India into a digital economy by providing digital empowerment to citizens across various industries like education, healthcare, agriculture, retail, energy, legal, financial etc.

For the Smart Cities initiative, IoT will play an important role on providing real time information on smart parking, traffic etc. thereby addressing the problem of congestion. The other usage of IoT can be on the management of street lights which can result in saving of electricity for the power sector. For healthcare industry, the usage of IoT would be for telemedicine, whereby the doctors from urban areas can provide remote consulting services to rural areas. The IoT connectivity also offers a host of development opportunities to untapped areas, including manufacturing and e-commerce to market local and traditional products.



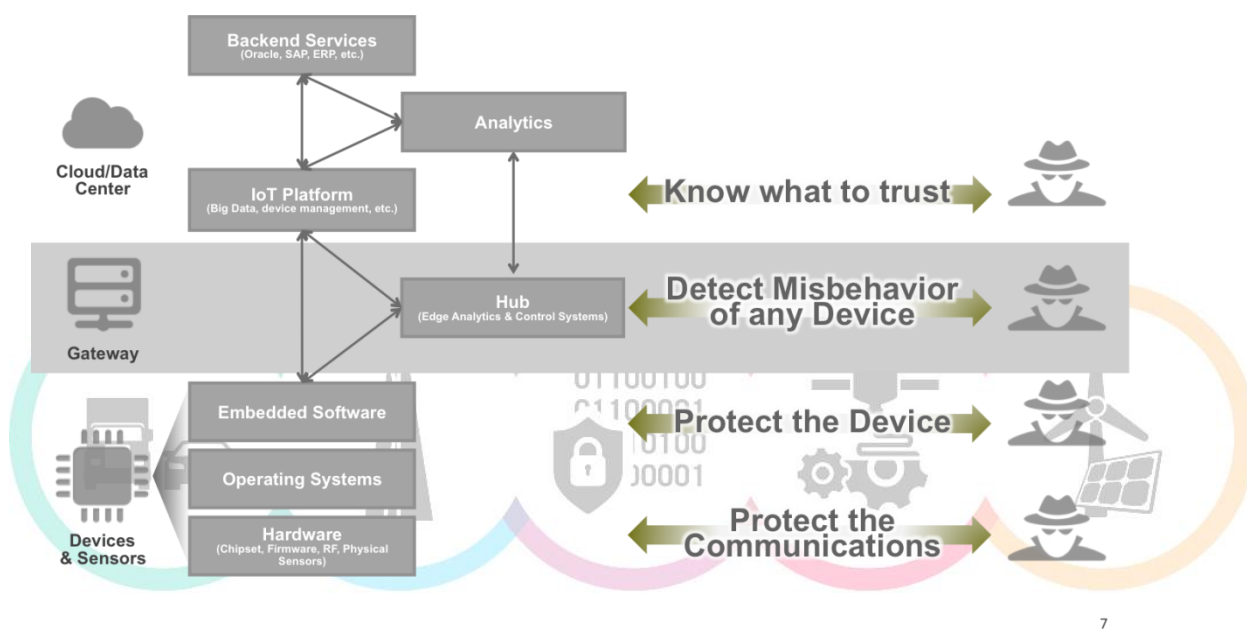
Internet of Things: The Basics



1. The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items — embedded with electronics, software, sensors and network connectivity enabling these objects to collect and exchange data.
2. To most people, IoT currently appears to be a mixture of smart home applications and wearables. But actually it has the potential to have a much wider reach. When the connected world becomes reality, the Internet of Things will transform nearly all-major segments – from homes to hospitals and from cars to cities.
3. Retail - Proximity-based advertising, In-store shopping behavior measurement and intelligent payment solutions are some of the IoT concepts of Smart Retail.
4. Healthcare - The concept of a connected health care system and smart medical devices bears enormous potential, not just for companies also for the well-being of people in general. New kinds of real-time health monitoring and improved medical decision-making based on large sets of patient data are some of the envisioned benefits.
5. Transportation or connected vehicles – Seems to be one of the more popular segments. Whether it is self-driving or just driver-assisted. Connectivity with other cars, mapping services, or traffic control will play a part. Next generation in-car entertainment systems and remote monitoring are also interesting concepts to watch out for.

IoT Security Needs

While identity, authentication, Code Signing, monitoring cyber threats are critical and valuable parts of the ecosystem, the end-to-end security strategy should include lightweight host-based protection for devices with an operating system, security analytics for analyzing the IoT data for different anomalies, IoT threat intelligence, cross-correlation across IT and operational environments for a holistic security view and IoT management to update the software, firmware to manage applications on devices remotely.



1. Firstly, because IoT devices need to be connected at all times to report on real world data, securing the communications against eavesdropping, hijacking and traffic replays are critical to ensuring the integrity and accuracy of the data from the numerous smart or dumb devices. This is crucial in order to have the most accurate data to reflect the reality on the ground that is neither untampered nor can be stolen.
2. Next, because most IoT devices like sensors and embedded devices typically have low computing resources like memory and storage, these devices need to be protected in a way where traditional security like anti-malware becomes unfeasible. Security needs to be purpose built for these devices where it not only makes the device resilient to malware but also tampering with the logic and critical data at rest.

3. A lot of IoT devices today are built as single purpose devices, where they perform predictable actions with predictable outcomes. That is why they need to have a way to ensure that they would know first-hand when, where and how an anomaly occurs. This provides valuable insights on whether the device is misbehaving due to a malicious attack or simply malfunctioning. An example of this would be to detect when a DOS attack is going on, whether against the IoT device or the IoT device actually contributing to a DOS attack.
4. Lastly, the IoT ecosystem is complex. There could be thousands of IoT devices that need to communicate to their backend or between themselves. There could also be third parties that require the data feed from these devices. Having a single root of trust establishes an identity for every IoT device and allows for trust and authentication between the devices and other components in the ecosystem.

IoT Security must be Comprehensive

Protecting Communications - Encryption, authentication, and “key management” are invariably the foundation of meaningfully resilient security. This “trust model” helps their systems safely authenticate systems of other companies and safely start encrypted communications with those systems. This “trust model” is the cornerstone of secure interoperability in computing today, and it is a “trust model” grounded on a very short list of extremely strong certificate authorities (CAs). These very same CAs already embed certificates in billions of devices every year. These device certificates enable the authentication of mobile phones in safely connecting to the nearest base stations, authentication of smart meters for the electrical power industry, and authentication of set top boxes in the cable television industry, among countless other examples.

Protecting Devices - In powering up, each device boots and runs some code. In that context, it is crucial that devices only do what we programmed them to do, and ensure that others cannot reprogramme them to behave maliciously. In that context, signing firmware, boot images, and higher-level embedded code are all increasingly common, including signing the underlying software components such as any operating system, and not just applications, but all code on the device. This approach can ensure that all critical components, sensors, actuators, controllers, and relays are all properly configured to only run signed code and never run unsigned code.

Integrity of Devices - IoT devices face many threats, including malicious data that can be sent over authenticated connections, exploiting vulnerabilities and/or misconfigurations. Such attacks frequently exploit many weaknesses, including but not limited to (a) failure to use code signature verification and secure boot, and (b) poorly implemented verification models, which can be bypassed. Attackers often use those weaknesses to install backdoors, sniffers, data collection software, file transfer capabilities to extract sensitive information from the system, and sometimes even command & control (C&C)

infrastructure to manipulate system behavior. Fortunately, when coupled with a strong code signature and verification model, host-based protection can help secure the device against all of these threats by using a number of technologies including system hardening, whitelisting, application sandboxing, reputation-based technology, anti-malware, and encryption. Depending on the needs of the specific system, a combination of these technologies can ensure the highest level of protection for every device.

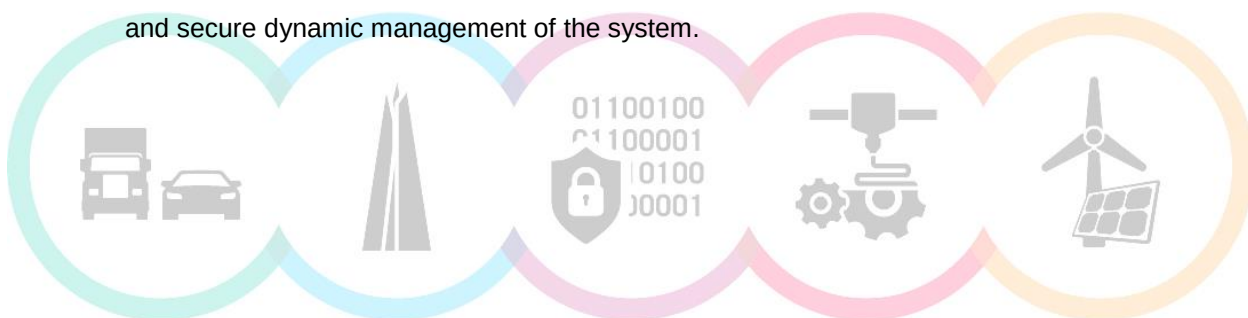
Security Analytics - Managing security for each device can include managing configuration of host-based security technologies, some security technologies need updates of security content such as blacklists, whitelists, heuristics, intrusion prevention signatures, and reputation data. Fortunately, some security technologies depend on policy based mechanisms that only need updates when the software on a device is re-imaged for other purposes, such as adding functionality. However, both types of security technology can generate security telemetry that is valuable in facing Advanced Persistent Threats (APT). For such reasons, the security telemetry should always be aggregated from those host-based (device-based) technologies for more central analysis. Security analytics can leverage security telemetry from devices and network hardware to help provide an understanding of what is happening in the environment, including detection of stealthier threats. Through such analytics, “detection and response” can complement strong protection technologies to provide security against the vast majority of attacks, as well as mitigating risks of the most serious and capable adversaries.



Summary

This paper advocates simple and effective reference architecture for IoT security that should be easy to deploy and scale.

1. The architecture mitigates malicious code by ensuring that all code is cryptographically signed and authorized for the device and ensuring that unsigned code is not permitted to run.
2. It protects communication through mutual authentication and encryption, leveraging time-proven certificate authorities and time proven trust models already protecting more than a billion IoT devices, but leveraging newer ECC algorithms to provide that level of security in resource constrained IoT devices.
3. The architecture further mitigates malicious data through host-based protection and further mitigates all remaining threats through security analytics.
4. As vulnerabilities and threats are discovered, they can be mitigated through effective, safe, and secure dynamic management of the system.



About the authors



Mr. Shrikant Shitole has been Managing Director for India at Symantec Corporation since May 2015. A seasoned industry veteran with over 25 years of experience, Mr. Shitole has held senior management roles across several enterprises in the IT and telecom segment. Prior to joining Symantec, he was the Chief Sales and Marketing Officer at Nelco Ltd. (Tata Enterprise), responsible for sales, marketing and product management. Before joining Nelco Ltd. he was the Managing Director for India and SAARC at Avaya Services, responsible for sales and service delivery. Mr. Shitole has also held various senior roles at Cisco and worked extensively across the Asia, Pacific and Japan region. Mr. Shitole holds an MBA from Narsee Monjee Institute of Management Studies, India and a Bachelor of Engineering degree in Electronics from Walchand Institute of Technology, India.



Mr. Mohan Raju is a distinguished Member of the IET-IOT India panel, a platform for stakeholders to participate in becoming an authoritative, but neutral voice for the evolving movement of IoT in India, where he actively advises & collaborates with industry & government stakeholders to shape health, education and energy initiatives in India by leveraging IoT & Big Data technologies. He is presently working with Bharti Airtel as Business Head based out of Mumbai and has rich experience in working for fortune 500, BFSI, Manufacturing Services and public sector customers in India. Mr. Raju completed his MBA in Marketing education from Narsee Monjee Institute of Management Studies, Mumbai and Bachelor in Engineering (Electronics & Telecommunications) from Utkal University India.

In Collaboration with



Dr Rishi Bhatnagar, Doctorate in IT Computer Science, is currently President of Aeris Communications India, Middle East & Africa. Rishi's career has taken him through more than 15 years of Sales, Delivery, Research, Merger & Acquisitions and Administrative responsibilities. During his PhD, he had developed for the first time "Relationship Maturity Model for IT services Industry" which helps corporates to identify effective relationship management processes & best practices for managing customer supplier relationship. He has co-authored the first book on IoT – Titled "Enterprise IoT". Dr. Rishi is the Chairperson of Institution of Engineering and Technology IoT panel for India.



