IoT Security—Silicon, Software, Manufacturing and Everything In Between

Joseph Byrne, Senior Strategic Marketing Manager, NXP
Ravi Malhotra, Senior Software Product Marketing Manager, NXP
Geoff Waters, Senior Principal Engineer, NXP

Security remains a top concern with the IoT. High-profile breaches over the past few years illustrate hacking of IoT devices to steal personal data, money, and the services of the devices' own CPU cycles and network connectivity. When the scope of the IoT expands to include enterprise, industrial, and municipal applications, the risks of an insecure IoT increase. But such expansion—and the benefits it affords society—will not occur until the IoT is secured. The risks are too high for stakeholders to invest in the IoT otherwise.

Because of ongoing security issues, the United States Department of Homeland Security (DHS) in November 2016 listed **six principles** to address IoT security challenges:

1. Incorporate security at the design phase
2. Advance security updates and vulnerability management
3. Build on proven security practices
4. Prioritize security measures according to potential impact
5. Promote transparency across IoT
6. Connect carefully and deliberately

NXP finds these principles to be a useful framework for OEMs and users to understand the Trust Architecture implemented by our processors and accompanying software. Instantiated in multiple product generations, our Trust Architecture helps designers craft secure IoT devices so that users can reap the rewards of internet-connected systems.

Design-Phase Security

The industry is clearly failing to incorporate security at the design phase. High profile attacks in 2016 took advantage of Internet-connected devices with hardwired default passwords and open network services. The failure is not just the poor security of these devices, but also the lack of mitigation elsewhere in the IoT. Routers on the local network or at the edge of the internet are particularly well suited to address ill-behaved things. Doing so presents an acceptance challenge because it puts the onus of securing the IoT on ISPs. They haven't been the target of IoT hacks, but ISPs suffer indirectly from them. As more of the IoT moves to expensive wireless links, ISPs may show more interest in securing their borders.

For network equipment companies and their processor suppliers like NXP, this type of security is familiar territory: filtering packets based on headers or applying deep-packet inspection (DPI) and possibly using IPsec or SSL, more for these protocols' authentication than their securing of data in flight. Depending on the processors' capability compared with network speeds, these functions may be accelerated.

Where this security becomes less familiar is with respect to user/entity behavior analytics (UEBA). This technique extends DPI, which is often used to track endpoints and their communications, and basic heuristic techniques. It uses machine learning trained on big data sets of monitored packets to identify anomalous network traffic, be it out-of-control IoT devices, data exfiltration, or insider-based financial fraud. At the customer premises, UEBA may be implemented in software on general-purpose processors. In the future, it could be offloaded to specialized machine-learning processors.

More responsible IoT developers will implement security in the design phase. They must make one critical change in how they select processors, however. They must make security, particularly platform security, a top criterion when selecting components. The capabilities NXP provides are unique among processor suppliers. In addition to network security functions, our processors implement platform trust features that extend the basic trusted execution environment (TEE) capabilities of ARM CPUs. Our platform trust approach secures devices throughout their lifecycle—manufacturing, commissioning, operation, update, and decommissioning and throughout their power-on-to-power-off cycle. In so doing, we enable designers to create systems capable of protecting their own integrity, per the DHS's admonishment to use "hardware that incorporates security features to strengthen the protection and integrity of the device."

Security Updates and Vulnerability Management

Not surprisingly, security updates and vulnerability management are also industry weaknesses. For the average user, this is likely a big part of what security means to them: can I lose control of my device or data to a hacker?

As weak as IoT devices are in this regard, smartphones are proving ever more secure. In 2016, even the FBI struggled to retrieve data from an iPhone, and Apple is making the task harder. The techniques Apple uses are not out of reach of developers of things and IoT infrastructure. Our trusted platform ensures that only OEM-signed code boots the device. Further, it can secure blocks of code and data stored within the device and provide the building blocks for the OEM to restrict the code that the device will run, much as the iPhone only runs Apple-approved code provided through the company's app store.

Ideally, an IoT device is based on a trusted platform and ships with no vulnerabilities. Realistically, all devices have bugs, most of which can be fixed in software. Our trusted platform, in conjunction with our secure provisioning and update tool, enables updating even buggy firmware secured by the unique cryptographic keys stored within our chip. It does so by installing new firmware and keys and by revoking the old keys so a hacker cannot roll the device back to an erstwhile valid firmware image.

Under the heading of secure updates and vulnerability management, the **Department of Homeland Security** makes the vague but tantalizing suggestion: develop an end-of-life strategy. Should devices decommission themselves after a fixed time or upon a signal from the OEM? This is certainly possible using the secure boot or update processes mentioned above: an OEM can program the device at the factory to brick itself at a particular time or can push out an update commanding the device to self-terminate.

Reuse Proven Security Practices

As a technology supplier, we invite our customers to "build on proven security practices" by taking advantage of the extensive security features we build into our products. We've proven our hardware features in many processor models over multiple product generations. Extensive documentation and customer-support services enable OEMs to employ these features properly. We also offer consulting services for customers seeking customization or help verifying systems adhere to best practices suggested by organizations such as **DHS**, **NIST**, and the **Open Web Application Security Project**.

Accompanying our hardware is a set of trust-tool software for:

- Offline configuration
- Secure boot
- Runtime execution

Offline configuration tools enable OEMs to do things such as sign code, debug securely, and program on-chip fuses (e.g., for key storage). Secure boot tools include an on-chip secure boot kernel and external secure boot code such as UEFI code or U-Boot. Runtime tools include middleware APIs and tools for secure provisioning and updating.

Prioritizing Security Measures

From our perspective, taking advantage of our processors' platform trust capabilities should be an IoT designer's highest priority owing to the impact it can deliver. Many vulnerabilities melt away by preventing execution of unauthorized code.

Transparency

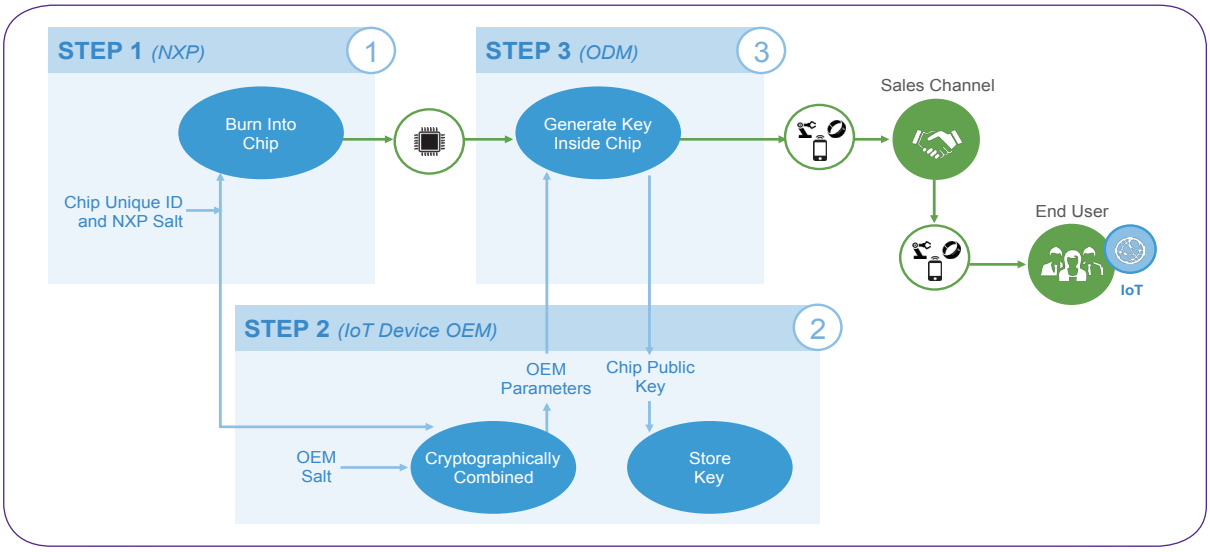
Transparency allows IoT stakeholders to accurately assess trustworthiness. IoT system users must understand potential vulnerabilities in the system, and IoT system developers must understand potential vulnerabilities' hardware and software components. Even where there are no known vulnerabilities to review, visibility into security development processes allows for more informed risk assessments.

The DHS report's discussion of transparency focuses on IoT devices' supply chains, highlighting the risk of relying on low-cost, easily accessible software and hardware solutions. As a vital link in the supply chain for IoT devices, we can aid OEMs' transparency efforts. From the beginning of the product lifecycle, we define a secure manufacturing model that allows OEMs to load signed code without relying on NXP confidentiality.

In this model, we burn a unique ID and a salt onto every chip, and provide this information to the OEM and its ODM contract manufacturer, as the figure below shows. The OEM generates its own salt. NXP does not know the OEM's secrets, which NXP processors can be trusted to protect. After all, transparency does not mean sharing everything.

At the ODM, our processor itself generates a unique public-private key pair, factoring in the salts. The chip can output the public key, but the private key cannot be output. The OEM can use the public key to sign the code that the ODM burns into the device. Once in the field, our processor enables the device to verify code upon boot and check in with the OEM to ensure that it's not cloned. The same mechanisms enable secure firmware updates and device decommissioning. In summary, we enable transparency and integrity throughout a device's lifecycle. Moreover, we explicitly state the security claims of our processors, including what is out of their scope, so that IoT stakeholders can assess their trustworthiness.

NXP'S SECURE DISTRIBUTED MANUFACTURING MODEL PROVIDES TRANSPARENT SECURITY



Careful Connections

The IoT industry is also failing to connect things to the internet carefully and deliberately. It is almost tautological to say that IoT hacks are a failure of properly connecting things because they are mostly cases of unexpected access. Who thought that Target's credit-card terminals could be remotely accessed via a building-services company? Who imagined that customers were exposing to the internet telnet ports on their security cameras?

As noted above, routers at customers' premises or the edge of the internet are in a good spot to police traffic, firewalling networks, spotting intrusions, and analyzing user/entity behavior. As the figure below shows, they can proxy security for IoT devices, doing things the devices themselves would do if better designed or more capable. The routers and better designed unconstrained IoT devices can also employ SSL or IPsec for authentication, rejecting connections from unauthorized network peers.

The tools for securing the IoT are available. It's up to OEMs to use them and network-equipment companies and ISPs to provide another layer of security to protect against hacked devices from less responsible OEMs. NXP is available to help. Working together we can secure the IoT, from silicon, to software, manufacturing and everything in between.

CAREFUL CONNECTIONS FIGURE A SECURE GATEWAY HELPS SECURE END NODES

Conclusion

Security is essential for further investment in the IoT. Consultancy Bain surveyed 533 IOT customers in 2016, finding that 45% of buyers selected "security concerns" as one of their top-three barriers to their implementation of IOT solutions. This was the highest of all concerns, well ahead of second-ranked "high price or unclear economic benefits" with 32% of respondents. **[1]**

Fortunately, the tools for securing the IoT are available. It's up to OEMs to use them and network-equipment companies and ISPs to provide another layer of security to protect against hacked devices from less responsible OEMs. NXP is available to help. Working together we can secure the IoT, from silicon, to software, manufacturing and everything in between.

[1]http://www.bain.com/publications/articles/how-providers-can-succeed-in-the-internet-of-things.aspx

How to Reach Us:

Home Page: **www.nxp.com**
Web Support: **www.nxp.com/support**

USA/Europe or Locations Not Listed:
NXP Semiconductor
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.nxp.com/support

Europe, Middle East, and Africa:
NXPHalbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.nxp.com/support

Japan:
NXP Japan Ltd.
Yebisu Garden Place Tower 24F
4-20-3 Ebisu, Shibuya-ku,
Tokyo 150-6024, Japan
0120-950-032 (Domestic Toll Free)
http://www.nxp.com/jp/support/

Asia/Pacific:
NXP Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@nxp.com

Document Number: IOTSECURITYWP REV 0