EMBEDDED SECURITY DIGEST

Fall 2017

www.maximintegrated.com/embeddedsecurity

maxim integrated™

Table of Contents

DON'T BECOME THE NEXT HACKING HEADLINE

By Kris Ardis, Executive Director, Micros & Security Business Unit, Maxim Integrated

From all of the headlines we continue to read, it's clear that connected, embedded devices need built-in security. As sensors in internet of things (IoT) products continually gather valuable data that we use for decision-making or for machine-learning, we have to trust the root data being used. Similarly, distributed actuators need to be able to trust the commands that they receive.

It's not that we lack good embedded security technology. Why, then, are smart products such easy targets for security breaches? Security and hacking involves a balance or risk versus reward. Consider the Jacquard loom, one of the first programmable devices that, you could say, marked the dawn of the era of smart devices. But we certainly haven't heard about these looms being attacked because, after all, what would the reward be? Room-sized computers that later emerged to support government, the military, and big business could have brought bigger rewards, but the risk of attacking them was very high.

Now, as more of us carry products with a great deal of intelligence and sensors, the risk of breaching these devices has dropped substantially. Devices are more accessible and the rewards can be great.

Two big issues are delaying more prevalent implementation of security. Fortunately, there are also great ways to move forward and reverse this disturbing trend. For example, Maxim's MAXREFDES143# IoT embedded security reference design protects an industrial sensing node via authentication and notification to a web server. Many IC companies, including Maxim, also offer components such as secure microcontrollers that provide a foundation for creating smart products that are also protected against hacking, cloning, counterfeiting, and other nefarious activities.

Read my Embedded Computing Design article, "Make your device unattractive to hackers: Design in security early on," to learn some useful tips and tricks for better IoT design security.

**This article originally appeared on Embedded Computing Design on March 30, 2017.*

Figure 1. Jacquard loom, one of the first programmable devices

WANT TO AVOID COUNTERFEITING? CHOOSE THE RIGHT SECURE AUTHENTICATION METHOD FOR YOUR DESIGN

By Christine Young, Blogger, Maxim Integrated

Any reputable company that cares about its customers, brand, and reputation wants to protect its products from being copied or cloned. Yet counterfeit electronic goods continue to persist, costing industries billions of dollars a year. There are, for example, estimates that the gray market gobbles up around eight percent of the total market revenue for electronics components.

Unfortunately, there isn't one magic solution that provides long-lasting, impenetrable security. But while nefarious forces work to stay ahead of their deterrents, those on the good side of the law have authentication technologies in their own arsenals.

There are, of course, different levels of effective authentication. Take printer ink cartridges, for example. To validate that it's genuine, a cartridge could send out a password. But the drawback to this approach is that someone in the middle could catch the password while it's being transmitted and reuse it. Challenge-response authentication, where the cartridge could prove that it knows a secret without disclosing it, presents a better option.

There are two different crypto-algorithm types to consider: symmetric keys (or secret keys) and asymmetric keys (or public keys). Let's take a closer look at each type.

Symmetric Keys for Two-Way Authentication

Symmetric keys have these characteristics:

- The host and slave must operate from the same secret key
- The secret must be protected from disclosure attack on both sides
- There's support for bidirectional authentication
- For a comparable security level, there's less algorithm complexity and shorter computation time

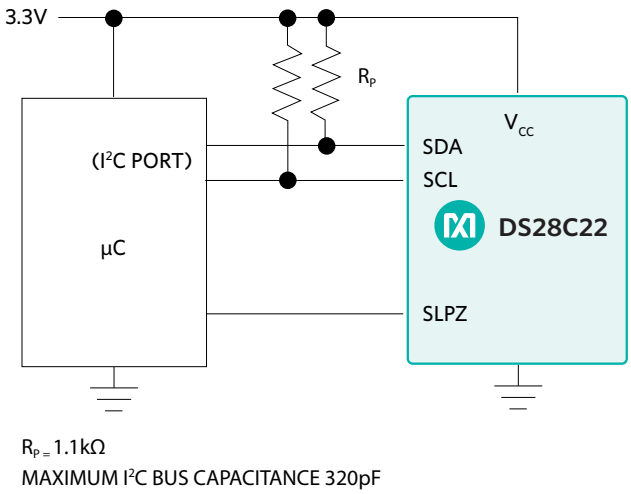

Figure 2: Maxim's DS28C22 DeepCover Secure Authenticator protects embedded designs, peripherals, and sensors with bidirectional challenge-and-response SHA-256 authentication and encryption.

An example of symmetric key authentication can be realized using a message digest computed from input data together with a symmetric key and by utilizing the Secure Hash Algorithm (SHA-x). Designed by the National Security Agency (NSA), SHA-x cryptographic hash functions are computationally complex mathematical operations run on digital data. You can determine data integrity by comparing the computed hash to a known and expected hash value1. Cryptographic hash characteristics are non-reversible, making it computationally infeasible to determine the input corresponding to a message authentication code (MAC). They are also collision-resistant, so it's impractical to find more than one input message that produces a given MAC. What's more, they possess a high avalanche effect such that any change in input produces a significant change in the MAC result. As a result, SHA-x has proven to be highly effective for secure authentication and small digest encryption. Figure 1 provides an example of a symmetric-key cryptography solution that uses a FIPS 180-based SHA-256 authentication algorithm.

The message digest is computed on the slave side based on the shared secret and data coming from the host.

Asymmetric Keys Reduce Key Management Complexity

Asymmetric keys have these characteristics:

- The host operates with a public key, while the slave has a corresponding private key
- The private key must be protected, but there's no requirement to protect the public key against disclosure
- There's support for authentication of the slave only
- For a comparable security level, there's increased algorithm complexity and longer computation time

An example of asymmetric key authentication can be realized using a digital signature computed with the Elliptic Curve Digital Signature Algorithm (ECDSA) (Digital Signature Algorithm (DSA) and RSA-DSA are other examples.) ECDSA uses elliptic curve cryptography, in which the bit size of the key is equivalent in terms of strength to twice the size of a symmetric cipher (256-bit ECDSA is as secure as a 128-bit AES). With ECDSA, the public key is only used for verifying; there's no need to protect the public key from counterfeiters or hackers. It's only critical to protect the private key. For systems where it's difficult or even impossible to secure host keys, ECDSA asymmetric authentication provides very strong security. It can also be ideal if you're using multiple contract manufacturers, or if you license your product to your customers. Figure 2 provides an example of a FIPS 186-based ECDSA engine that implements asymmetric cryptography.

Figure 3. Maxim's DS28E35 DeepCover Secure Authenticator provides crypto-strong authentication security for a variety of applications, including medical sensors, industrial programmable logic controller (PLC) modules, and consumer devices.

Online Tool Mode Helps You Select Authentication Solution

So how do you decide which authentication method to use for your design? Maxim offers a simple online authentication advisor tool that helps you select the right secure authentication solution based on your end application. Providing advanced physical security ranging from digital IDs to crypto-strong authentication, Maxim's DeepCover Secure Authenticators provide low-cost IP protection, clone prevention, and peripheral authentication. Try the online tool today to find a solution to address your requirements or get new ideas for authentication applications.

SAFEGUARD IOT DESIGNS WITH HOLISTIC APPROACH TO SECURITY

By Christine Young, Blogger, Maxim Integrated

We know that consumer trust takes time to build. This is all the more reason why we can't afford to leave internet of things (IoT) devices vulnerable to attack.

"We have seen so many different news (items) recently…we see devices like cars (and things) in the home and in industrial getting hacked," said Majid Bemanian, director of segment marketing at Imagination Technologies and a board member of the IoT Security Foundation (IoTSF). "The challenge that exists is, trust takes time to build. We can't afford to have IoT devices out there being compromised and lose the trust of the consumer."

This spring, technologists gathered for the first Bay Area meeting of IoTSF at Imagination Technologies offices in Santa Clara. The non-profit, vendor-neutral IoTSF was launched in London in September 2015 to promote knowledge and best practices in appropriate security for those who specify, make, and use IoT products and systems. Its 90-plus members come from industry and academia.

Why Technology Alone Won't Solve the Security Problem

The IoTSF has formed several working groups to address topics including connected consumer/home, patching constrained devices, vulnerability disclosure, the IoT security landscape, and trustmark/regulatory issues. Pamela Gupta, president of OutSecure Inc. and chair of the IoTSF's self-certification working group, told the Bay Area gathering: "We are not going to solve this problem by technology alone. We need a holistic approach to security."

To define a holistic security approach, the self-certification working group has developed a trust framework for self-regulation that focuses on the device in the scope of the ecosystem and the different touchpoints. Learn more about the framework and the IoTSF by reading my article, "Want consumer trust? Secure your IoT design" in Embedded Computing Design.

Simplify Security with Embedded Security ICs

Even though technology alone isn't enough to solve the security problem, it's still an essential component in protecting designs from security breaches. Between software- and hardware-based security methodologies, hardware-based approaches have proven to be the most robust. Establishing a "root of trust" using a secure microcontroller that executes software from an internal, immutable memory can guard against attempts to breach an electronic device's hardware. Since the executed software is stored in the microcontroller's ROM, it's considered to be inherently trusted because it can't be modified. That's why it's called the root of trust.

Security managers, secure microcontrollers, and secure authenticators are examples of embedded security ICs that can help simplify the process of protecting entire systems. For example, Maxim's DeepCover portfolio of embedded security solutions provides advanced physical security to safeguard critical data and keys. Maxim also offers reference designs that ease the design process. For example, the MAXREFDES155# IoT embedded security reference design can be used to authenticate and control a sensing node using elliptic curve-based public key cryptography with control and notification from a web server. The MAXREFDES155# reference design features an ARM® mbed™ shield and attached sensor endpoint; the shield contains a DS2476 DeepCover ECDSA/SHA-2 co-processor. The sensor endpoint contains a DS28C36 DeepCover ECDSA/SHA-2 authenticator. Because the design is so simple, it can be quickly integrated into any star-topology IoT network.

Tapping into a holistic design methodology and integrating embedded security ICs into your IoT design can give your customers the confidence that their data is protected.

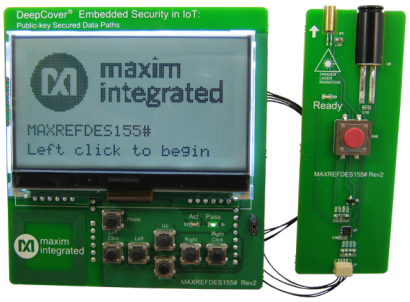

Figure 4. MAXREFDES155

KEEPING HACKERS AWAY FROM YOUR POS TERMINALS

By Gregory Guez, Executive Director, Embedded Security, Maxim Integrated

A few years ago, big-box retailers including Target and Home Depot made headlines when their point-of-sales (POS) systems were breached. Personal data from millions of consumers was leaked. Despite incidents like these, spoofing, skimming, and hacking aren't very difficult and are still happening. In fact, a researcher with security data and analytics solution provider Rapid7 devised a small, $6 tool that can open hotel room doors and break into POS systems and cash registers.

The global Payment Card Industry (PCI) Security Standards Council maintains, evolves, and promotes security standards for the industry. Founded by major payment products companies, the organization aims to standardize security efforts across the industry. Its PIN Transaction Security (PTS) standard, PCI-PTS, calls for robust security controls for payment systems, adding testing requirements to validate vendor documentation of policies and procedures related to device management.

Figure 5. Invenco's G7 outdoor payment terminal accepts a variety of payment options and can display customized content to help drive additional sales

Maxim's MAX32590 DeepCover secure microcontroller, which has achieved PCI-PTS v4.1 certification, is inside the Invenco G7 OPT (outdoor payment terminal). Invenco is a finalist for the NZ Hi-Tech Company of the Year award. A modular EMV-compliant payment system with a 12-inch multimedia touchscreen, the G7 OPT enables a self-service payment experience. The system accepts EMV, magnetic stripe, contactless (including mobile phones), barcode-reading, and mobile wallet payments. Users can program its display with responsive content that can help drive additional sales.

To comply with PCI PTS, the G7 OPT had to pass stringent levels of differential power analysis (DPA) attack testing. Maxim provides a cryptographic library with sophisticated algorithm protection means—one of the few IC suppliers to do this. The company also provides a security evaluation report from an independent laboratory, decreasing the amount of time and cost associated with PCI-PTS certification by several months. Having the MAX32590 in its design helped G7 OPT's compliance with the challenging certification requirements.

Secure Microcontroller Saves Design Time and Costs

Using a secure microcontroller such as the MAX32590 addresses the challenges of speeding time to market and also lowering costs. The 32-bit, Linux-based microcontroller simplifies designs because it requires fewer external components. The highly integrated chip features an ARM926EJ-S processor core, patented external bus, advanced physical security, and much more. Learn more about how the MAX32590 delivers tamper-resistant security by reading my article, "Safeguarding POS Terminals with Secure Microcontrollers" on Fintech Finance.

WHY YOU CAN'T AFFORD TO OVERLOOK DESIGN SECURITY

By Christine Young, Blogger, Maxim Integrated

In early April, a suspected hack caused emergency outdoor warning sirens to sound overnight in Dallas, Texas. Normally, these sirens are used to warn residents about impending tornadoes and the like. This time, city officials suspect that someone gained access to the system to trigger intermittent alarms across the city. Around the same timeframe, U.K. payday loan firm Wonga suffered a data breach that affected potentially up to 245,000 customers, whose names, addresses, and bank account numbers were stolen. Earlier this month, the massive WannaCry ransomware attack affected computers in at least 150 countries in Europe, South America, Asia, and North America, causing problems for hospitals, universities, manufacturers, businesses, and government agencies.

Figure 6. Security cameras are among the everyday devices that have been targeted by hackers

DDoS attacks are on Wired's list of the biggest security threats for this year, as are ransomware, weaponized consumer drones, and another iPhone encryption clash. Hacking incidents such as the examples just mentioned are in the news with increasing regularity around the world. And as everyday objects become smarter and connected, they're providing more points of access and vulnerability. As RSA notes in its white paper, 2016: Current State of Cybercrime: "From mobile threats and ransomware to the role of biometrics in reducing fraud, a myriad of threats exist across the cyber landscape and the commoditization of cybercrime is making it easier and cheaper to launch attacks on a global scale."

The most recent cybercrime report from the FBI, its 2015 Internet Crime Report, notes that its Internet Crime Complaint Center (IC3) has logged more than 3.4 million complaints since the center was formed in May 2000. In 2015 alone, complaints amounted to more than $1 billion in reported losses from more than 288,000 complaints.

There are ways to close the door on hackers—technologies and techniques that aren't a drain on budget, time, or resources. But why aren't more designers using them? Especially when a breach can be far costlier in terms of dollars as well as brand reputation and customer loyalty.

New White Paper: What You Need to Know About Design Security

Too many perceive security to be expensive, time-consuming, and/or difficult to implement. This is a misconception that Gregory Guez, an executive director in our Embedded Security Business Unit, corrects in his new white paper, "Why Hardware-Based Design Security is Essential for Every Application." This paper will help you understand why hardware-based security is a much more robust option than its software-based counterpart. You'll also find out how easy and cost-effective hardware-based security can be when using embedded security technology. Read the white paper today and learn useful tips to safeguard your next design against the prying reach of cybercriminals.

ARE YOU DOING ENOUGH TO BUILD TRUST IN OUR CONNECTED WORLD?

By Christine Young, Blogger, Maxim Integrated

"In order to achieve the benefits of a connected world, you have to create trust in that connected world," Bill Diotte, CEO of Mocana, told the audience during the opening talks at this year's IoT DevCon.

In the IoT world, security remains the top challenge. It was also a main theme as the conference kicked off on April 26 at the Santa Clara Convention Center.

In his talk, "Shifting the IoT Mindset from Security to Trust," Diotte told the crowd, "Mocana and all of us in this room today have a mission: as we build, we have to secure." Based in San Francisco, California, Mocana provides a comprehensive IoT security platform that protects more than 100 million IoT devices and ensures secure device-to-cloud communications. The problem, Diotte said, is that cybercrime has moved from credit card and password theft to the dismantling of infrastructure, cyber weaponization, and proxy warfare. Citing a report by Gartner, he noted that 20% of enterprise attacks will involve the IoT in 2020. In the face of these scary trends, the reality is, many of the engineers building smart, connected products don't have adequate tools for proper security, Diotte said. Applying traditional IT model methods such as perimeter defenses, password protection only, or simple SSL connections to the IoT world simply doesn't work, he explained.

Fortunately, he said, there's good awareness now around security, along with resources like secure chips, point solutions, and do-it-yourself methods. The problem here is, most of these options are disconnected, so it's up to developers to stitch something together, which exposes systems to risk. Making matters even more challenging are the hundreds or even thousands of manual pages that time-strapped developers must read through if they want to, for instance, utilize the secure functions of a chip or align with the latest standards.

Clearly, a new approach is needed. "We believe it's about trust – creating from the ground up, hardening devices so we know they are trustworthy up to the gateway cloud," said Diotte.

What constitutes trust in the IoT world? Knowing that the device boots up in a known, secure state and has the right level of firmware is essential. Also important are having trusted updates, operation, and transport (from the device itself through the gateway to the cloud and back to the apps).

Figure 7. Mocana's Bill Diotte addresses IoT security at this year's IoT DevCon.

Hardened devices and applications can make all of this possible. To that end, Mocana is building an ecosystem that allows developers to create trusted environments, whether those developers are creating secure chips, operating systems, apps, or end devices. The company's IoT Security DevKit, which runs on a Raspberry Pi board, features the Mocana IoT security stack, a strong crypto engine, SSL/SSH/Wi-Fi security, automated key and certificate management, and sample apps.

What happens if trust is broken? This year's IoT DevCon was paired with the inaugural Machine Learning DevCon, bringing together two of the biggest topics in tech. These topics are also very much intertwined. Analytics, Diotte noted, will continue to improve such that we will be able to take action in real time based on real-time analytics that indicate when there's an unauthorized attempt to communicate with or update firmware on a device, for example.

"I thought Web 1.0 was the most amazing thing that could happen," said Diotte. "Today we're sitting on the precipice of an incredible opportunity – connected devices, applications, cars, homes, cities. It's everybody's responsibility to put into place systems that not only deliver amazing experiences but are hardened and protected."

Zero-Touch IoT Device Onboarding

ToAnother security-related talk during the IoT DevCon keynote sessions came from Jennifer Gilburg, director of strategy, Internet of Things Identity at Intel. In "Zero-Touch Device Onboarding for IoT," Gilburg discussed the drawbacks of today's manual IoT device onboarding and offered a more secure method. Security needs to be integrated into products right from the start, beginning with a hardware root of trust and hardware security and building up from here, she said. Otherwise, there's a risk that security won't scale once we reach 20 billion IoT devices. Developers should also think about security across a device's lifecycle, from the silicon at the fab to the OEM, installer (onboarding) and through provisioning, end user operation, and even decommissioning, she explained.

There's a new recognition that hardware delivers an essential foundation for security use cases. Intel develops its chips with security building blocks for protected boot and storage, hardware and software identities, and a trusted execution environment. Software makes data privacy, security management, platform integrity, and secure communications possible. Gilburg also discussed Intel Enhanced Privacy ID (Intel EPID), a group signature scheme that allows platforms to cryptographically sign objects while preserving the signer's privacy. Each signer in the group has their own private key, but verifiers use the same group public key to verify individual signatures. Intel EPID is designed into all Intel silicon.

"We've kind of forgotten about privacy…and I blame Facebook for that," Gilburg said, laughing. With all of the data being shared today, developers need to consider the minimal amount of data that is needed in order to perform a task and collect only that data, she said.

In today's manual IoT onboarding process, once a device arrives on site, a technician installs it and turns it on and conducts manual provisioning. The IT backend accepts the device credentials, connects it to a device management system, and the device starts working. By contrast, a zero-touch onboarding process from Intel separates the roles. The installer sets up the device and IT takes control of the device to get it on the network and control platform. Proxy installation and provisioning are handled by an onboarding service with a unique identifier for device authentication. This approach is currently in a proof-of-concept phase as Intel collaborates with other entities in the IoT ecosystem to craft protocols and reference codes that enhance privacy, scale, and automate the process of device registration.

Figure 8. Intel's Jennifer Gilburg explains a more secure process for onboarding IoT devices at this year's IoT DevCon.

As everyday products get smarter and connected, it's clear that developers have a big responsibility in ensuring that their designs are secure. To help ease the process of IoT device node authentication, Maxim offers an IoT embedded security reference design. Known as MAXREFDES155#, the reference design authenticates and controls a sensing node via elliptic-curve-based public-key cryptography.

HOW SECURE ICS PROTECT DATA IN TRANSIT IN IOT DEVICES

By Stephane Di Vito, Principal MTS, Embedded Security, Maxim Integrated

Smart, connected devices are making our lives more convenient. But on the other hand, the proliferation of these devices also means that more of our data—including personal and/or sensitive information—is vulnerable to security breaches. Protecting data that is in transit and at rest has never been more critical.

The Transport Layer Security (TLS) protocol, the successor to Secure Sockets Layer (SSL), prevents eavesdropping or tampering of data in transit as internet of things (IoT) devices communicate over the internet. It essentially creates a secure communication channel between a client and a server. Hypertext Transfer Protocol Secure (HTTPS), which we see when we visit a website secured by an SSL certificate, brings together HTTP with SSL/TLS to deliver encrypted communication with, along with secure identification of, a Web server.

Figure 9. Secure companion ICs can protect a TLS implementation for your IoT design.

TLS involves a "handshake phase" that uses asymmetric keys to agree on a symmetric key pair, which is used only for that session and enables efficient and fast data encryption and decryption. A secure IC can handle this handshake phase, storing the private session keys and performing the encryption/decryption in a separate device with countermeasures against known methods of hacking and attacks. If the private keys and certificates aren't stored securely and protected from improper modification, these assets can be exposed to attacks. There are invasive attacks where the attacker attempts to open the device's enclosure to manipulate the memory content, replace the firmware, or probe the PCB traces. And there are non-invasive attacks, where logical bugs in the device's firmware are targeted.

Fortunately, there is a low-cost, low-complexity solution that can secure the implementation of the TLS protocol in a connected, embedded system while also reducing the burden on the device's application processor.

Pitfalls of TLS Integration in Embedded Devices

One of the advantages of the TLS protocol is that it can be integrated fairly easily into any application using off-the-shelf software libraries. However, even if you have a bug-free TLS stack, the integration and use of the TLS library in your software may still be flawed. Common weaknesses of a TLS integration in an embedded device include:

- Skipped certificate verification
- Weak cipher suites
- Insufficient protection of certification authority certificates
- Exposure of session keys
- Compromised client authentication keys
- Use of poor cryptographic implementations and low-quality random numbers

There are a set of minimum rules to follow in order to have a truly secure TLS scheme and avoid the pitfalls we've discussed. Protecting session keys while in use, utilizing secure cryptographic algorithms, and safely storing the client's private authentication keys are among the rules. What's also effective is using a companion secure IC to secure the TLS implementation. Without placing any additional burden on your design's application processor, a secure IC can inherently prevent many of the vulnerabilities of a TLS implementation.

Read my application note, "Using Secure Companion ICs to Protect a TLS Implementation" for an in-depth understanding of TLS implementation pitfalls and how a secure IC such as the MAXQ1061 can help you avoid these pitfalls. The MAXQ1061 enables TLS even in resource-constrained embedded systems. The secure IC also reinforces the intrinsic security of the TLS protocol by protecting the critical steps of authentication during the handshake, session key computation, and package encryption/decryption.

LEARN 3 KEY WAYS TO LOCK IN SECURITY FOR YOUR IOT DESIGN

By Christine Young, Blogger, Maxim Integrated

In 2016, cybercrime losses rose 24% to more than $1.33 billion, according to the FBI's Internet Crime Complaint Center. Headlines about hacking incidents continue and the more connected our devices, the more vulnerable they can be to attack. And as we connect more devices within, say, a home or a business, an entry into just one device can put the entire network at risk. Consider this spring's WannaCry ransomeware episode, which impacted 300,000 computers in more than 150 countries. Spread through file-sharing technology used by PCs, the attack impacted banks, hospitals, telecommunications companies, and warehouses.

In a recent blog post, ARM cited some studies revealing that 70% of companies aren't willing to pay more than a 10% premium for security. As the blogger noted, this is surprising, given the risks and repercussions that come with inadequate system security. Fortunately, there are ways to design in security upfront that are robust and won't break the bank.

Maxim is hosting a free webinar that will show you how you can safeguard your connected, embedded devices, protecting your customers and your company from the devastating effects of security breaches. In "3 Key Requirements to Lock In Security for Your Design," you'll learn about:

- The three pillars of security
- Cryptography, digital signatures, and root of trust
- Turnkey embedded security for connected objects

The session will also present a cost analysis that shows you how much you can increase profit with a small security investment that prevents counterfeiting. And our tech expert makes the case for why hardware-based security is always a better choice than its software counterpart.

Sign up for the webinar today to learn how you can better protect your next IoT design.

Figure 10. "3 Requirements to Lock-in Security for Your Design" Webinar

IOT WORLD: FROM IOT PATTERNS TO BLOCKCHAIN SECURITY

By Christine Young, Blogger, Maxim Integrated

Industry projections call for 50 billion connected devices by 2020, but 2 out of 3 internet of things (IoT) projects fail, noted Tony Shan, chief IoTologist at Wipro Technologies, during a talk at this year's IoT World conference in Santa Clara, California.

"The picture is not so promising," Shan told his audience at the event's IoT Developer Stage. "There are a lot of reasons. We have more than 400 platforms in the IoT space and, talk about standards, there are more than 100 in this area."

Citing survey results, Shan notes that the top three reasons companies develop IoT products are to:

- Improve quality of service or products
- Enhance workforce productivity
- Increase operations reliability

However, barriers ranging from disjointed platforms to IT environment complexity to proprietary products and fragmented implementations are hindering success. This is where an IoT pattern framework can help. A pattern can address specific requirements, such as security or data analytics. You could also combine multiple patterns to solve a tough problem. The benefit of IoT patterns, Shan explained, is to facilitate a repeatable solution and have a common baseline for describing and implementing a solution versus building it all from scratch. The process involves a methodical approach, looking for common seeds to uncover best practices to tackle problems. Design concerns are classified, and the pattern structure informs ways to address these concerns.

The IoT pattern structure is broken down into:

- Category: groups of classifications
- Area: stage breakdown in the IoT pipeline
- Type: kind of IoT solution

These areas are further broken down into these segments:

- BATS: business, application, technology, service
- CUBS: creational, universal, behavioral, structural (classifying different ways to look at patterns)
- SCAD: sensing, connection, analysis, delivery

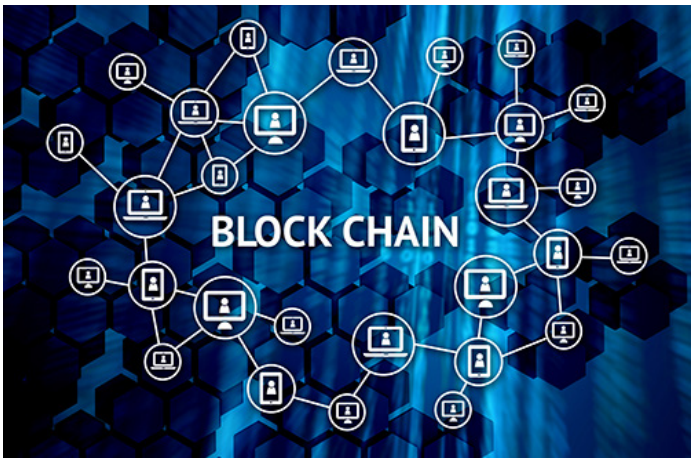

Figure 11. This blockchain flowchart conveys the concept of this tamper-proof method to secure online transactions. The Trusted IoT Alliance believes that the blockchain can also be used to secure IoT applications.

Securing the IoT via the Blockchain

Shan could only scratch the surface of IoT patterning in his half-hour talk. He did mention briefly a couple of top challenges of IoT designs: security and privacy. Security was a key focus in the next talk on the IoT Developer Stage. Members of the Trusted IoT Alliance discussed their efforts to use the blockchain to secure IoT applications. Blockchain, secured via advanced cryptography, provides a tamper-proof distributed record of transactions; it's maintained by a network of computers on the internet. An underlying technology for bitcoin, the Alliance is developing a shared blockchain protocol to secure IoT products. In April, the group, comprised of five enterprises and six startups, launched an IoT "thing" registration API that supports several blockchain implementations. Users can register serial numbers, QR codes, and UPC code identities and bind them to stronger cryptographic identities. Blockchain technology is used to immutably link these cryptographic identities across digital and physical worlds.

"From IT infrastructure to operational infrastructure, software on distributed systems can be fingerprinted elements within the blockchain system," noted Anoop Nannra, a technology strategist in Cisco's Corporate Strategic Innovation Group.

Joe Pindar, director of product strategy at Gemalto, emphasized the mutual trust that blockchain technology can bring to internet-based transactions. In the blockchain, all of the players are equal in this environment, and the data is real and trusted by all. By contrast, in a hierarchical approach, he said, the smaller guys don't always trust the bigger players.

Zaki Manian, a founder of Skuchain, added that conventionally, we don't trust IoT devices to make business decisions, like exercising a letter of credit or releasing a payment. However, with the blockchain, control of business decisions can be delegated to secured IoT devices, he said. Manian noted that blockchain also solves the problem of identity, particularly in industrial applications where a connected device (like a shipping container) gets passed from one organization to another. With the blockchain, each organization doesn't have to reprovision the ID for the shipping container each time it changes hands. This can be done when the silicon is manufactured, a much more efficient approach.

Allliance members believe that the blockchain can enable the next level of the IoT, facilitating trusted data sharing and transactions between connected things. They anticipate greater efficiencies and reduced cost of doing business. One example is the Share&Charge charging station network in Germany, which brings together owners of charging stations and electric vehicle (EV) drivers to expand the country's charging infrastructure. Another example is the secondary car market, where the blockchain can make it easier to reliably validate data like vehicle mileage or the health of the EV battery.

Rather than reinventing the wheel, the panelists noted, the blockchain can provide a common identifier for connected devices and a means to build solutions on top of this.

EMBEDDED SECURITY ICS SAFEGUARD PCS AND PAYMENTS

By Christine Young, Blogger, Maxim Integrated

Two companies in different parts of the world, both committed to protecting privacy, one for PC users and the other for point-of-sales (POS) financial transactions. Ultimately, both companies chose secure microcontrollers to safeguard their designs.

A recent blog post from ARM cites a survey revealing that most companies don't want to invest too much in security. Yet, the flow of cybercrime-related headlines, from credit card breaches at big-box retailers to this spring's WannaCry ransomware attack, hasn't shown signs of slowing down. Many businesses have a misconception that implementing security takes a lot of time and money. But as two Maxim customers—Design SHIFT and Beijing Weipass Panorama—have demonstrated, these misconceptions couldn't be further from the truth.

A digital security and consumer product engineering company headquartered in Menlo Park, California, Design SHIFT has created the ORWL secure desktop PC. ORWL provides a key and a password for authentication and also guards against physical attacks. When the company was designing its PC, it looked for robust hardware-based security that would be easy to integrate into its design. Design SHIFT found its answer in Maxim's MAX32550 DeepCover® ARM® Cortex®-Cortex M-3 flash microcontroller. The secure IC provides a cryptographic engine, true random number generator, and environmental and tamper detection circuitry.

"Security is a lot easier with Maxim," said the company's CEO, Olivier Boireau.

Read more about how Design SHIFT created its secure PC using embedded security technology.

Figure 12. Design SHIFT has safeguarded its ORWL PC with Maxim's DeepCover technology.

Beijing Weipass Panorama created and defined China's first full-touchscreen financial POS, the WPOS-3 platform. The company needs to enable safe financial transactions on an open internet-based business platform. Finding a solution that would meet the company's power, performance, and small footprint requirements was also essential. Beijing Weipass Panorama also found its answer in Maxim's DeepCover family, in its case the MAX32555 DeepCover secure ARM Cortex-M3 flash microcontroller. The part is the industry's first secure microcontroller for mPOS featuring secure boot loader with public key authentication.

"(Maxim is) a top player in the security chip solution market, already certified by PCI (Payment Card Industry," noted Marco Ma, co-founder, vice president, and chief engineer at the company. "Using the MAX32555 provides a strong safety guarantee for us."

Read more about how Beijing Weipass Panorama is making safer customer payments, membership programs, and coupon redemption using embedded security technology.

CONTRIBUTED ARTICLES

Protecting Smart Home Devices from Security Breaches
This article originally appeared on Embedded Systems Engineering on January 31, 2017.

Make Your Device Unattractive to Hackers: Design in Security Early On
This article originally appeared on Embedded Computing Design on March 30, 2017.

Thwarting Hackers on the IoT
This article originally appeared on Microcontroller Tips on April 20, 2017.

Protect TLS in IoT Devices with Secure Companion ICs
This article originally appeared on Electronic Design on May 16, 2017.