CERTICOM WHITEPAPER SERIES

Securing Sensor Networks

GETTING IT RIGHT FROM THE START, WITH PUBLIC-KEY

BlackBerry | certicom

Introduction

Until recently, monitoring and control systems have worked solely on data fed into them by fixed devices connected by wires. But ongoing developments in low-power VLSI chips have produced devices that integrate sensing capability with computation and wireless communication. Emerging applications include industrial and manufacturing device monitoring and maintenance, complex information-gathering for indoor and outdoor environments, including offices, factories, warehouses and homes, farmland, endangered species habitats, and urban traffic.

But with these capabilities come increased possibilities for misuse. The danger is not from malevolent groups of sensors self-organizing to block us in our homes, but from the hundreds of events that can make new technologies seem unreliable or badly designed: remotes that control the wrong devices, fire alarms that are triggered unnecessarily, environmental sensors that give bad or no readings, industrial machinery that doesn't shut down when sent a stop command.

Security methods alone can't prevent these issues. But security can limit the set of variables that can go wrong. For these emerging wireless networks of sensor and control devices, any system downtime, whether from network failure, an unresponsive device, or an active network attack is a failure to secure the network. In large-scale networks and critical applications it's essential to implement public key technology which can be used to provably identify a node on a network, and then to securely send or retrieve data from that node.

This authenticated identity can be used to manage the network device life-cycle and decrease management costs, while improving the security of the network and giving the network owner better control over the devices.

Not all sensor applications will require security. However, these devices operate independently and are open to mismanagement and misuse, especially when using wireless communications. For some applications, and particularly for wireless devices in which the potential for attacks is seen as greater, security will be demanded.

Public key cryptography: With public key technology, one key, which only the device knows, binds the device to its identity on the network; and a second key, mathematically related to first, is used by the network to verify that identity. This enables device identification to be done rapidly, surely, and in a cryptographically strong manner.

Public key methods are used in several ways:

- **To identify a person or device uniquely from millions of others.**
- **For exchanging keys over a network, enabling two people or devices to communicate in a secure fashion.**
- **To create a digital signature, which can be used to verify the integrity of a message.**

Technology Background

As microcontroller devices become smaller, cheaper and more capable, applications for these devices are rapidly developing. Data collection and physical monitoring are the basis of these applications, and wireless connectivity enables immediate response to readings.

The IEEE 802.15.4 standard describes a low-power radio for networking sensors wirelessly. On top of this radio, network and application layers establish the network and device operations. Network layers include ZigBee, IP version 6, and a variety of proprietary schemes. Applications are varied but generally involve a small set of code to enable and monitor the physical sensor and to respond to external events and receive commands.

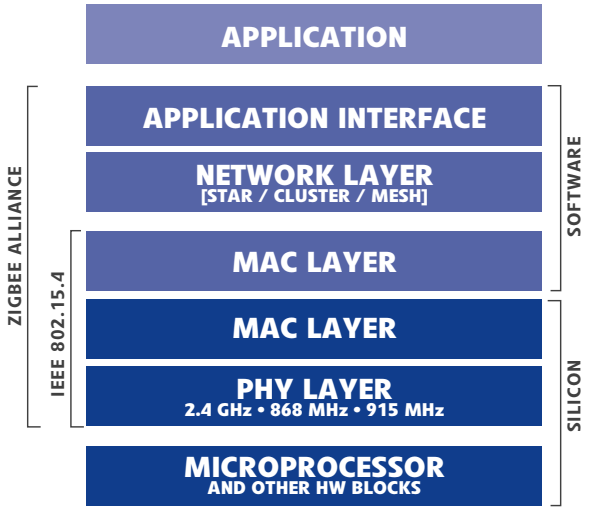

Figure 1: The wireless microcontroller stack.

The Problem: Building Robust Networks

The market is full of examples of products that succeed because they are considered strong, robust, secure. Examples of secure products include Volvo cars, which sell because they are considered safe; the "bullet-proof" Master Lock; Jeld-Wen doors and Pella windows, which sell at a premium because they keep the outside out. E-commerce, after a slow start because consumers were afraid to put credit card data onto the Internet, has expanded rapidly as public confidence in SSL technologies – based in part on public key methods – has solidified.

There are also plenty of products that failed because they did not have these characteristics – but these are less well known. However, failures of security do generate headlines: In 1982, the Tylenol murders caused the recall of 31 million packages at a cost of more than $100 million, and quickly

cut Tylenol's market share from 35% to 8%. This incident also started the pharmaceutical industry toward tamper-proof packaging, and it is still innovating to improve the security of its products. In the technology world, Internet outages caused by denial-of-service attacks have periodically derailed the positive news of developing communications.

Wireless networking technologies have repeatedly come under fire for security problems, including technologies such as Wi-Fi, which spawned a culture of stealing access from open or poorly protected networks; and Bluetooth, which has repeatedly been criticized for its security problems, including bluejacking and bluesnarfing.

Wireless sensor and control networks will also face these problems, as well as some that are unique to these new architectures. Mesh routing and ad-hoc cluster formation enable wide distribution of nodes and the potential for collaborative sensing and processing, even in remote areas. Using flexible topologies and enabling use of distributed clustering means that nodes must be able to recognize their counterparts and be able to readily interact with them.

The problem, then, is to avoid the protection and customer confidence issues that have troubled other wireless technologies. And the challenge is to make this work on low-power devices, providing capabilities for emerging applications.

Why Security is Essential

There are several fundamental operations that must be addressed in order for a network of wireless devices to function properly. For many applications, validating the identity of a participating node is more critical than other security concerns. Once this is accomplished, the network establishes communications between nodes; in a secure network this is done by establishing routing and exchanging security information including a key. This key is then used to encrypt the data, rendering it useful only to nodes holding the correct key. Finally, the communications undergo an integrity check to ensure that the messages have not been altered or corrupted.

A set of examples can be used to describe the use of these operations:

- Lighting control systems for commercial buildings can offer reduced energy use, lower costs and lighting that is responsive to occupants' needs. These systems work through central control, by issuing commands to individual banks of lights. In this type of system, ensuring that accurate light sensor readings and commands are communicated successfully is essential; the efficiency of the system is directly tied to accurate, authentic communication to specific nodes.

- Warehouse or baggage-handling asset management systems have operational needs that are different from lighting systems. These systems offer the capability to track items, usually high-value items as well as operating equipment, through the warehouse to provide immediate data on the location of tracked items. As assets move throughout a warehouse, nodes move and re-configure network topology as necessary, and each asset can be monitored for efficient movement and to avoid loss. Device policy may be used to define that only specific nodes can monitor or request data from nodes.

- Medical applications are being developed to monitor vital signs such as patients' heart rhythms and blood oxygen levels, and to communicate these readings wirelessly to readers over a network at the hospital, in an ambulance, and at home. In these patient monitoring systems, security and reliability are critical. In addition, privacy constraints from legislation such as HIPAA require that networks transmitting medical data use strong security.

- Fleet management is emerging as a method to remotely monitor and manage vehicle operation, including automatic reporting of fluid and fuel levels, emissions monitoring, and ABS braking events, offering fleet managers convenience as well as savings on time and expenses. Managing government compliance is a second benefit. The US DOT's Intelligent Transportation System initiatives include a recent study of on-board technology which could be used to monitor vehicle and driver status and electronically maintain driver history. Concerns listed for this type of system include privacy concerns, electronic falsification of data, and accuracy of measured data.

- In a military setting, all of these capabilities may be necessary, and rapid deployment may be required. The U.S. military has started trials of wireless sensor devices. However, in order to deploy widely, it is likely that stronger and proven security will be required.

Ways to Solve the Problem: Symmetric vs. Public-key

The current solution to the problem of establishing reliable and secure sensing and control networks, is to work around it using symmetric-key schemes, accepting a simple IEEE address as identification for nodes and requiring interaction with an always-available management system to establish communication.

These solutions use central key management, which verifies node identities and distributes keys with which nodes can establish secure connections. This works for small and self-contained networks, but becomes a roadblock to system growth. A central controller works like a traffic officer managing a busy intersection; but any increase in lanes, streets or traffic can rapidly turn chaotic and noisy.

Centralized control of wireless sensor network operations presents practical problems: Setting up connections between networks is problematic; a node, unable to act on its own, must somehow determine which controller on which PAN to turn to for direction. Sharing data from physically separated nodes, across distance or across networks, may lead to future applications; but requesting direction from a controller may introduce delay and increase network complexity. Finally, centralized control creates a central point of failure for a secured network.

In contrast, public key-based network operation does not rely on active central control, but rather enables nodes to operate independently and collaboratively. Each device is issued its own keys and security policy. Identities and policies can be created centrally, then distributed to nodes to enable network operation. In the examples described above, public key capabilities enhance the operations of lighting control and asset management systems by providing an irrefutable identity to every element of the system. Some early systems use a fixed IEEE address for identification, but this is a weak identifier, open to spoofing in the same sense that a person's government ID number can easily be used for identity theft. The use of a distinct, provable public-key-based identity enables faultless deployment and enrolment of nodes, and facilitates network management.

Public key technology for medical and fleet management applications offers user confidence and regulatory compliance by installing irrefutable, unique identification into each device. Perhaps more importantly, it allows the device to validate the identity of all monitoring equipment, ensuring that only properly credentialed monitors have access to patient or vehicle records. Finally, secure key exchange is enabled between a variety of nodes, meeting regulations for protection of transmitted data.

The public-key model can also address the complexities that arise from the interactions of proprietary, open-source and consortium-driven sensor networking technologies. A provable identity based on public-key can be used by the same back-end systems, independent of the type of network that is in use. In other words, public-key identification is technologically 'portable'.

4 Easy Steps to Secure Networks

Public-key capability is embedded into devices using firmware code and a hardware multiplier to accelerate mathematically intensive cryptography. Operations can be rapid and power-efficient even on tiny devices.

During manufacturing, an identity credential (with information detailing device capabilities) is embedded in the device. This credential enables automatic enrollment onto a network, as the device's ID, public key, and capability set are validated by the manufacturer's signature and the device can respond to a challenge by a network management tool.

On appearance on an 802.15.4 network:

a. the node's manufacturer credential is verified
b. the node is issued a credential or security policy by the network (which may be composed of many PANs
within a company or installation), making it a part of the network.

The device is now capable of roaming between PANs within the network (if company policy allows).

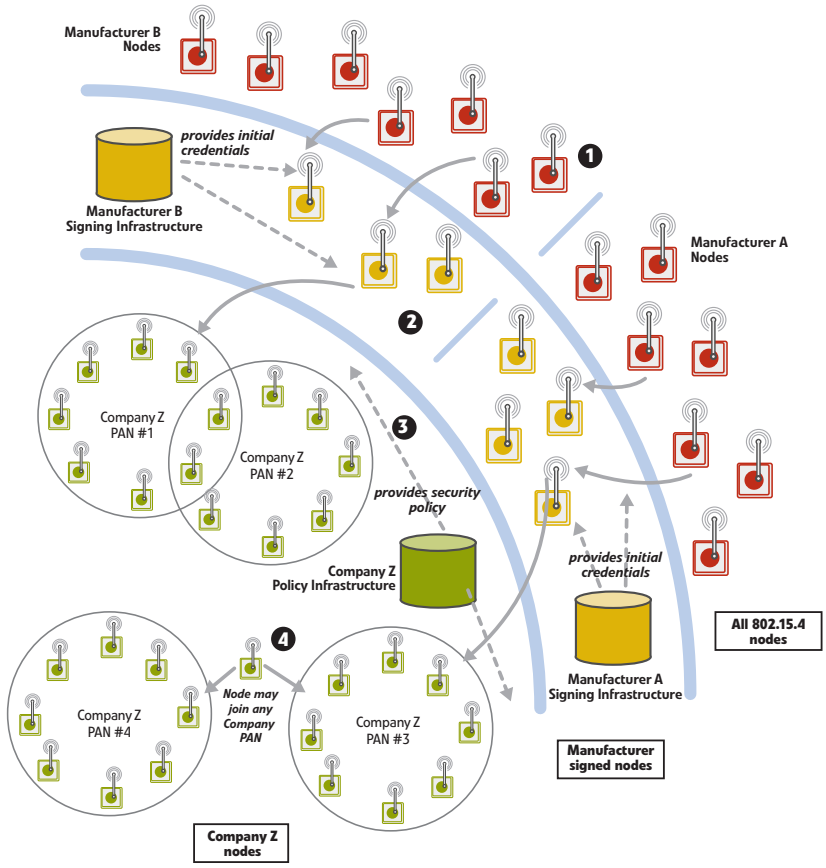

Figure 2: Public-key enables mesh networking with mobile nodes and ad-hoc cluster formation.

Right From the Start

Wireless sensor and control network technologies have the opportunity to do security correctly early in the deployment of these systems. This offers not only a chance to do the right thing; but also to avoid the failures of other products and to be known as a strong, robust, "bullet-proof" technology.

This has business benefits as well, saving deployment costs and enabling the use of innovative applications. Much as the Internet has fostered innovation in the dissemination of information, sensor networks using flexible topologies will provide a stage for innovation in information gathering and responses.

Life-cycle Savings and Reduced Total Cost of Ownership

Manufacturers, system integrators and installers can attest to the fact that the initial purchase price of a device is small in comparison to the life-cycle costs associated with that device. Because of this, improvement in device reliability, and the associated small increase in device cost, is returned several times over during the course of a device's useful lifetime.

Deploying devices: Devices can be securely commissioned using public keys. At installation or at manufacture, a device's ID is bound to its public key by a digital certificate. The associated private key, which only the device knows, proves the unique identity during network communications. (The details are done using complicated mathematics; however, these techniques are well-known and proven.)

Deploying devices and admitting them to a network is then simply a matter of validating the device against the digital certificate. This eliminates "spoofing" of a device, and can be used in conjunction with network management to ensure that no unwanted devices have joined the network.

Network updates: A small network operates in an acceptable fashion using symmetric keys. All share a network key, and negotiate communications as needed. However, when a new device is added (either as a new function or to replace a faulty or retired device), or when a device is removed from the network, the network key must be updated to every node in the network. As a network gets larger, and as networks become more ad-hoc – with nodes joining and leaving regularly – updating symmetric keys can take a lot of time and network bandwidth.

Using public-key methods, however, network-key updates are minimized. Each device has a unique set of keys, and when a device leaves or joins the network, it simply enrolls with the network. All other nodes require no change.

The point at which the number of nodes on a network becomes inefficient will depend on how frequently nodes will be added to or leave the network, whether nodes will be mobile between networks, and node failure rates.

Fosters New Application Models

Innovative applications can result from networks that are fluid and easily reconfigurable. Current symmetric key deployment models build secure networks by making all communications dependent on a single management device. This not only provides a single point of failure for the network, but it also adds additional steps in setting up communications between nodes. Using public key technology enables improved node mobility and flexible topologies which will serve as a catalyst for new and innovative applications.

Mobility and flexibility: Devices that may move between networks – packages and other tracked assets, medical sensors, vehicles, portable tools and other devices – are problematic for symmetric-key based networks. If a node mobility policy or automatic enrolment protocol is in place, the device can move within a corporate network or register with a new network using its signed, provable identity, proving (if its credentials are accepted) that it is trusted and can join the network. This allows for more flexible uses of wireless devices, in which they are not limited to a single physical network.

[Note that some devices, such as most light switches and security systems, should only allow access on one network, such that an outside controller cannot add these devices to a second network.]

Promotes Buyer Confidence

As described earlier, security can strongly affect the perception of a product. An insecure system not only presents problems for misuse, but can also appear to be unreliable. Therefore, especially for commercial, industrial and military customers, capable security is a requirement for a product to succeed. Strong security from the start will be an enabler for sensor network adoption.

Improved security: In a symmetric-key system, if a network key is extracted from a device, then all communications on the network are vulnerable; an outside party could listen to communications or introduce different communications, such as falsified commands to industrial equipment or fire alarm systems. And because manufacturers will likely not bear the cost of putting secure storage on all devices, this is a serious risk.

In a public-key system, if a private key is extracted from a device, only communications with that device are vulnerable, until the private key expires. Communications between other devices are not at risk. This means that any devices used in applications considered essential – industrial, medical, military and business-critical – can be protected with public-key technology, limiting exposure and building robustness into the network.

Certicom's Solution

Certicom is working to provide strong security for emerging sensor networks. Because of the constrained nature of these products, Certicom's ECC technology, which delivers more security per bit, is a clear fit. Certicom has worked in cryptographic protocols for over 20 years and is an acknowledged leader in embedded security.

Certicom Security for Sensor Networks

Establish trust and manage the lifecycle of sensor networks

Certicom Security for Sensor Networks enables developers of low power sensor devices to build secure, reliable operation into networks from design and development through to manufacturing, deployment and upgrade. Public-key-based operation eliminates the need for active central control of network communications, instead distributing security functions throughout the network to each of the individual sensor devices. This gives each node a provable identity to enable its operation and enables sensor networks that are scalable, fluid and easily reconfigurable, providing capabilities for an array of new and innovative applications.This enables sensor networks that are scalable, fluid and easily reconfigurable, providing capabilities for an array of new and innovative applications.

Certicom Security for Sensor Networks offers a full implementation to meet the security needs of low-power wireless networks, designed in a modular fashion such that it can be connected to a variety of implementations.

This development required that the security operations be optimized for tiny microprocessor devices, distributing security functions throughout the network to each of the individual sensor nodes. By providing the necessary components as a security agent, ready to be implemented in a variety of devices, we are making the public-key operations widely available.

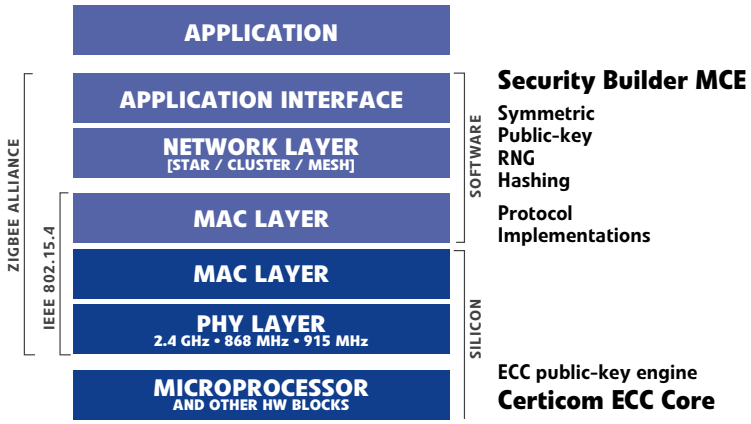

Figure 3: Certicom Security for Sensor Networks provides all the necessary tools to build security into sensor devices.

Certicom Security for Sensor Networks includes:

Security Builder MCE (Microcontroller Edition): provides the cryptographic primitives required to create a trusted platform for low-power devices. In addition to symmetric encryption, it allows you to integrate key exchange and digital signatures based on elliptic curve cryptography (ECC), the only public-key scheme capable of meeting the footprint and power limitations of these constrained environments. Security Builder MCE provides an API to the device networking stack, and can deliver even stronger performance when combined with the Certicom f(2^m) IP Core.

Certicom IP Core: accelerates processor-intensive public-key operations, which are otherwise prohibitively slow for many embedded applications, enabling low-power devices to benefit from the improved security of public-key cryptography. It operates in concert with Security Builder MCE to interface with the device networking stack.

Finally, Certicom will work with applications vendors to ensure that the capabilities offered through public-key operations are extended from the device up to sensor network applications.

Conclusion

The promise and opportunity of sensor networks can only be realized if these networks are trusted and reliable. Certicom Security for Sensor Networks enables developers of low power sensor devices and networks to make use of public-key technology from design and development, through to device manufacturing and upgrades. Public-key technology pushes intelligence into the network, giving nodes an identity and eliminating the need for active control over operations. This enables sensor networks that are scalable, fluid and easily reconfigurable, setting the stage for an array of new and innovative applications.

About Certicom

Founded in 1985 with a long-term focus on Elliptic Curve Cryptography, Certicom has been awarded over 500 patents. As a leader in applied cryptography and key management, Certicom provides managed PKI, key management and provisioning technology that helps to protect customers' device firmware, applications, and long-lived assets. Certicom is a critical element of the Blackberry cybersecurity portfolio deploying the first and best in class end-to-end security solutions used in preventing product counterfeiting, re-manufacturing, and rogue network access. Blackberry Certicom's secure key provisioning, code signing and identity management solutions are field- proven to protect next-generation connected cars, critical infrastructure and IoT deployments.

Corporate Headquarters

4701 Tahoe Blvd, building A
Mississauga, ON
L4W 0B5, Canada
Tel: 1.905.507.4220
Toll Free: 1.800.561.6100
(NA only)
info@certicom.com

Additional Certicom White Papers

To read other Certicom white papers, please visit www.certicom.com.

Sum Total: Determining the True Cost of Security
Sourcing Security: Five Arguments in Favour of Commercial Security Solutions

Government

Making the Grade: Meeting Government Security Requirements (Suite B)
Meeting Government Security Requirements: The Difference Between Selling to the Government and Not
FAQ: The National Security Agency's ECC License Agreement with Certicom Corp.

Mobility

The Inside Story
Many Happy Returns: The ROI of Embedded Security
Welcome to the Real World: Embedded Security in Action

Sensor Networks

Securing Sensor Networks

DRM & Conditional Access

Injecting Trust to Protect Revenue and Reputation: A Key Injection System for Anti-Cloning, Conditional Access and DRM Schemes
Achieving DRM Robustness: Securing the Device from the Silicon Up to the Application(PDF)

Enterprise Software

Using Digital Signatures to cut down on Bank Fraud Loss

ECC

An Elliptic Curve Cryptography Primer
ECC in Action: Real World Applications of Elliptic Curve Cryptography
Using ECC for Enhanced Embedded Security (PDF)