A Future-Proof Authentication and Security Solution for Existing Industrial IoT Systems

Derek Atkins, Chief Technology Officer, SecureRF Corporation

Industries have been deploying actuators and sensors to manage their day-to-day operations for decades. Along the way, someone had the idea to connect these actuators and sensors to small microcontrollers, and eventually, they thought it would be an even better idea to link these devices to a network, leading to the invention of the Industrial Internet of Things (IIoT). When these early industrial "things" were developed and deployed, ten or fifteen years ago or more, they included little or no security because you were assumed to be a valid user if you could connect to them. The deployment of connected industrial devices and the way they are interconnected has continued to grow in new and different ways, actually increasing the potential for an attacker to jump between these networks and get to the unprotected actuators and sensors in ways that were never conceived when they were deployed. Imagine a utility's disgruntled ex-employee, accessing their SCADA system to open valves and release sewage everywhere. There is no need to imagine, as this has already happened.

To date, billions of insecure devices are now deployed around the world. Replacing all of these systems and their unsecured devices in order to incorporate proper security would cost trillions of dollars. A more sensible approach, in terms of both cost and time, would be to look at retrofitting existing installations with the security they need. One tactic would be to introduce a security device that sits in front of each legacy IIoT object, enabling authentication and authorization, without the cost of replacing the existing deployments.

In this solution, you would connect a pair of security gateway devices in the communication link between the legacy IIoT devices and their controllers. Such a solution would enable the inclusion of additional security without requiring the replacement of the legacy device. The security add-on would sit as a bump-in-the-wire (BitW) between the legacy device and the other end of the communication link, protecting that link from attack.

An Intel MAX® 10 FPGA -BitW Solution

To demonstrate this solution, Intel PSG commissioned SecureRF to develop an IoT security gateway solution. Using an Intel MAX® 10 FPGA, SecureRF created a solution that can be retrofitted to existing systems and provide secure communication, authentication, and authorization protection to legacy IoT devices by integrating into the communication stream between the device and its controller. A deployment places one Intel Intel MAX® 10 FPGA at the IIoT gateway and at each legacy device to be protected. This BitW approach allows implementation without modifying the existing processors. The BitW processor is provisioned with the legacy IIoT device information and programmed with the proper authorization data necessary to protect the device.

On the other end of the connection, another Intel MAX® 10 FPGA device sits in front of the controller. This side of the BitW architecture ensures that the controller is talking to a valid legacy device because the controller can cryptographically authenticate the Intel MAX® 10 FPGA sitting in front of the legacy device.

This solution delivers additional security to the system. After the endpoints have been authenticated, each transmission is encrypted and protected. This prevents an attacker from reading the data being sent, modifying messages, injecting new messages, or even replaying old messages. These protocols

ensure that only the correct endpoints are communicating, and nothing in the middle can intercept or inject anything.

After building a fully functional system, SecureRF was invited to showcase this solution at the opening of Intel's FPGA China Innovation Center in December 2018. The demonstration showed how this BitW system, based on Intel's MAX® 10 FPGA, can protect the communication between two legacy devices with an attacker connected in the middle (see following image of the delivered demo).

Image of BitW Security Solution now on Display at Intel's new FPGA Innovation Center

The Public Key security methods used in this solution leverages the future-proof Group Theoretic Cryptography (GTC) solutions from SecureRF. The quantum-resistant key agreement protocols and digital signature algorithms enable these devices to securely authenticate without pre-shared key provisioning, the need for a network connection, or a secure database lookup. Moreover, because GTC provides a lightweight implementation, computation requires very few resources, enabling the use of smaller devices and very fast identification and authentication.

Extended Security and Secure Boot on the Intel Atom Processor

Ideally, developers of new devices are advised to add security now instead of trying to retrofit security later. While the Intel MAX® 10 FPGA addresses the needs of the BitW solution described above, those working on new solutions can consider other products like the Intel Atom processor. The Intel Atom is a low-power 32-bit platform that also efficiently runs SecureRF's cryptographic tools.

Specifically, SecureRF has a software SDK for the Atom x5-Z8350 processor that enables authentication and Secure Boot solutions on the platform.

With Secure Boot, a developer can ensure that firmware stored in flash or in another long-term storage device has not been altered or modified and verify that it came from the correct owner. To make this work, the manufacturer, using SecureRF's digital signature algorithm - WalnutDSA, embeds WalnutDSA's public key along with the algorithm's signature verification routine in the device ROM, a protected space in the device. Then, the manufacturer signs their firmware packages with the WalnutDSA private key that is the "other half" of the public-private key pair.

At boot time, the ROM will verify the signature on the firmware against the embedded public key. If the signature is valid, then you have proof that the firmware came from the manufacturer (origin authentication), and that it has not been modified or tampered with (integrity protection).

The downside of legacy secure boot solutions is the performance degradation that occurs because legacy digital signatures are expensive, especially in constrained devices. This is not the case with WalnutDSA.

Specifically, on the Atom x5-Z8350 processor, a WalnutDSA signature verification requires only 530,000 clock cycles. This means the firmware can be verified quickly without a significant impact on boot time performance.

SecureRF offers free cryptographic Software Development Kits for FPGA and Atom devices for customers to evaluate today.

Quantum Resistance – Future-Proof Cryptography

The notion of Quantum Resistance is relatively new, but the concepts are not. Imagine a future where an attacker has access to a quantum computer and uses that computer to try to attack today's cryptography. Unfortunately, all of the Public Key cryptographic technology used today would be broken by this attacker in the future. This includes asymmetric systems like RSA, Elliptic Curve Cryptography (ECC) and Diffie-Hellman (DH) key exchange.

The reason these systems will be broken is that a quantum computer of sufficient size can run Shor's Algorithm which can quickly factor large numbers (the security of RSA) or solve the discrete log problem (the security of ECC and DH). To enable Shor's algorithm to work, the underlying mathematics of a method must be finite, cyclic, and commutative, and RSA, DH, and ECC have these characteristics.

In a *finite* system, the internal state of the mathematics has a limited scope. For example, there are only 2^{1024} possible states for an RSA-1024 calculation. This is an example of a finite field.

For a system to be *cyclic*, it must be implemented as a generator to a power, g^x. When this exponentiation occurs within a finite field, it will eventually touch the full extent of the field and then repeat.

When numbers are *commutative*, that means that multiplication can be applied in either direction, *a* times *b* equals *b* times *a*, i.e., 3*5 = 5*3. It is obvious that when dealing with RSA, ECC, and DH, all three of these qualifications are met.

To date, Shor is the most important quantum algorithm to attack cryptography.

The underlying math of GTC is not susceptible to Shor's algorithm. GTC is computed based on matrices over finite fields with permutations and table lookups added in. While the matrix over a finite field is finite, GTC is not cyclic, and it is not commutative. As a result, Shor does not apply to GTC, making all of SecureRF's methods quantum-resistant.

About SecureRF

SecureRF develops and licenses quantum-resistant, public-key security tools for low-resource processors powering the Internet of Things (IoT). The company's authentication and data protection solutions are highly efficient when compared to techniques like ECC and RSA. SecureRF delivers ultra-low-energy, fast, and small footprint solutions ideally suited for constrained 32-bit, 16-bit, and even 8-bit devices like the ARM Cortex M0/M3 and RISC-V processors. SecureRF security solutions are easily deployed on embedded platforms including FPGAs, microcontrollers, and ASICs. Free Software Development Kits and security consultations are available today. Additionally, SecureRF has developed tools appropriate for implementing its solutions for a wide range of environments.

SecureRF is a proud Intel Gold FPGA Design Solutions Network Member and offers a digital signature verification function to deliver secure boot, secure firmware and other security solutions for Intel FPGAs and the low resource devices they connect to. Learn more about our IoT Security for Intel® Cyclone® V SoC FPGAs, Intel® MAX® 10 FPGAs and CPUs. SecureRF is also a General member of the Intel® Internet of Things Solutions Alliance.

More information is available at www.securerf.com