SLiM Security for Cellular, Satellite, and Constrained Networks

January 31, 2020

OVERVIEW

Security standards introduced in the 1990's have not kept pace with the rapid advances of communication networks and growing technology verticals; specifically, the Internet of Things. Several factors have contributed to this growing security gap:

- Long-lasting standardization processes
- Lack of practical cryptographic innovation
- Need for interoperability with legacy security protocols
- Slow uptake of security by companies and industries

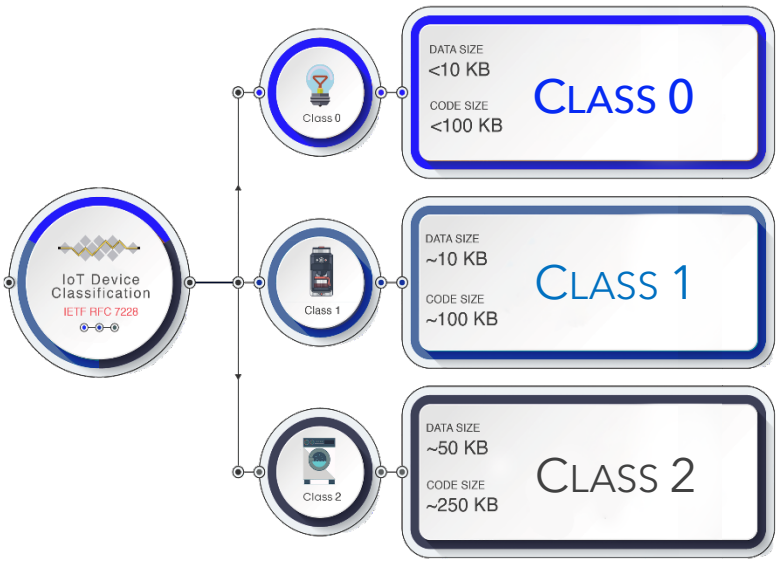
According to NIST, cryptographic protocols take upwards of 15 years to gain widespread adoption.

AgilePQ, a disruptive post-quantum IoT security company, has developed solutions for several issues arising within the constrained world of the Internet of Things.

IoT—THE WEAKEST LINK

The trend of microprocessors to become more powerful had the side effect of creating a market of capable, but constrained, microcontrollers whose primary function is collecting and transmitting data. These Machine-to-Machine (M2M), or Internet of Things (IoT), devices are at low price points and with minimal features in order to remain competitive in the market.

The Internet Engineering Task Force, RFC 7228, classifies these constrained devices into three primary categories based on computing capability and available memory.



These devices are gaining widespread adoption in virtually every vertical to improve visibility, collect data, enhance operations, and automate numerous tasks:

- Medical
- Automotive
- Industry 4.0
- Critical Infrastructure
- Building Surveillance and Home Automation
- Smart Cities

While these devices may be constrained, they are an attacker's foothold and the weakest link in a network's security. Data from these IoT devices influence decisions, contain sensitive intellectual property, control critical operations, and contain sensitive personal information and credentials.

Intercepting and manipulating the data from these devices allows an attacker to influence decisions, enter the network, interrupt operations, and cause significant harm.

IoT COMMUNICATIONS

Constrained devices do not use the traditional internet protocols widely used by mobiles, PCs, and cloud infrastructures, and numerous innovative communication protocols have been developed specifically for these deployments.

These protocols are designed for low-power operation over long distances, leveraging licensed cellular or unlicensed Industry-Science-Medical-Band (ISM) frequencies. Similarly, constrained protocols exist for satellite deployments.

IoT Protocol	Features
LTE-M	Higher data rate Constrained Packets
NB-IoT	High latency Low bandwidth
EC-GSM-IoT	Medium latency Low bandwidth
Sigfox	Limited messages/day Delivery not guaranteed
LoRaWAN **Zigbee** **BLE**	Limited data rates Limited bandwidth

Real-world deployments are facing a serious issue when it comes to securing these devices; they fail to establish a connection due to heavy data and processing requirements, and they cannot communicate any data or updates securely.

An attempt has been made to carry standard security technology such as Transport Layer Security (TLS) into constrained devices and networks; however, packet loss,

noise, and low-power microcontrollers are failing to support even the most lightweight implementations. TLS was designed in the 1990s as the successor to SSL—the technology used by your computer to securely pass banking and other credentials to websites.

However, AgilePQ has developed an efficient, low-bandwidth solution for identity provisioning, establishing sessions, and securing the communication links that can be delivered into any class of IoT device, and it meets the needs of these constrained communication protocols.

AGILEPQ'S POST-QUANTUM SECURITY FOR IoT

Component Name	Category	Function	Attack	Security Functions
RSA / ECDH / DH	Asymmetric	Key Establishment	Shor's Algorithm	Forward Secrecy Secure Key Establishment Identity Proof
DSA / ECDSA	Asymmetric	Digital Signature	Shor's Algorithm	Identity Verification Data Integrity Signature Non-Repudiation
AES / 3DES / ChaCha20	Symmetric	Data Encryption	Grover's Algorithm	Confidentiality
SHA-*	Symmetric	Hashing	Grover's Algorithm Simon's Algorithm	Integrity

The cryptographic security components in TLS are faced by an imminent threat of a rapidly developing technology: quantum computers. This threat is especially relevant to IoT deployments which may remain in the field for over 15 years.

These cryptographic components rely on what are known as "hard mathematical problems" that cannot be easily solved on classical computers today.

However, mathematicians began to explore the possibility of solving these problems using quantum computers, and they found that these computers are vastly more capable for these specific use cases.

Proposals for new quantum-computer-resistant cryptography methods have been made public, and these rely on a new class of hard problems—those that cannot be solved easily on classical nor quantum computers.

Deployment of Agile, Post-Quantum Security

AgilePQ's solution incorporates proprietary and public methods to deliver the most capable and efficient post-quantum security solution for IoT on the market. Its expertise can scale these solutions to the most constrained IoT device, up through more powerful server and cloud applications, to provide a full end-to-end encryption solution for data-in-transit and data-at-rest.

Delivering this solution in a standard SIM card applet allows for cross-compatibility across these constrained IoT cellular protocols. It has an added benefit of secure key storage, and it gives the device owner a platform-agnostic security solution.

For non-cellular communication networks, such as satellite and Sigfox, or any other WiFi or traditional deployments, the AgilePQ libraries are available as software libraries that easily integrate with the device firmware. These software libraries are designed to fit within Class-0 device constraints, and they average around 2KB or less depending on the compiler toolchain.