TrustWrx at the Edge

Securing IoT Sensors, Hubs and Controllers

As the Internet of Things expands into all aspects of industry, health care, connected cars, wearables, etc., the security of communications beyond the defended perimeter has become a major issue. As IoT devices proliferate across the cloud, the frequency and costs of breaches are escalating, opening up many vulnerabilities across IoT that have proven difficult to defend against.

What is the Edge?

The term, "Edge", is a recent outgrowth of cloud computing. It describes the smart device, such as a hub, that can provide true computing capability to receive and process data from central servers and communicate with the furthermost points downstream, like sensors that create data only. On the factory floor the edge device may be a hub that receives and process data from many equipment sensors in near real-time, storing, analyzing, aggregating and periodically reporting upstream to central servers. In a car the edge device is the smart controller or hub that receives and processes the data from the many onboard sensors, and can also manage the overall vehicle operation. The benefits of edge computing include the reduction of network traffic loads and leaving routine low-level processing actions at the edge devices, along with faster local performance.

The Major Security Gap

One of the major security gaps for IoT is the well-known lack of effective communications security between sensors and the edge device. TrustWrx is confident that our solution today can securely protect communications from the server, across the cloud to any edge device that has the processor and memory capacity to run the TrustWrx thin client. However, at the edge the ability to use cryptography to secure the connection to remote sensors and controllers has not materialized because of the hardware constraints imposed by the tiny-device form factor - constraints that have yet to be dealt with by the sensor manufacturers.

The perceived miniaturization needs of sensors has led to very small-footprint topologies and very little executable memory space, which has left these devices unable to run effective cryptography software. The major operating systems for IoT devices all provide native support for a few encryption algorithms and protected runtime spaces. Unfortunately, there is not enough memory at the sensors to process encryption algorithms.

Today, this is the main impediment to effective edge-to-sensor security.

The Sensor Industry

There are dozens of companies in this space. They provide a wide range of products from individual sensor chips only, to sensors packaged with SOCs (System on a Chip), A-to-D conversion, radios, etc.; all packaged as a complete sensor solution. Many offer multi-sensor capabilities in a single package and they come as battery driven, line power driven, wireless and wired. The factory floor

currently favors wireless sensors that talk to local edge hubs, which then communicate upstream or across the cloud to central services.

Leading manufacturers of IOT sensors are:

- Texas Instruments Incorporated
- Intel
- Stmicroelectronics N.V.
- TE Connectivity Ltd.
- NXP Semiconductors N.V.
- Robert Bosch GmbH
- Invensense, Inc
- Infineon Technologies AG
- Analog Devices, Inc.
- Arm Holdings PLC.
- Omron Corporation
- Sensirion AG
- Smartthings, Inc.
- Konux Inc.
- Lantronix
- *Many Others*

Sensor Memory and Cryptography

The memory currently offered in all sensor packages we have seen ranges typically from 56 kB to 1 MB of programmable flash, and DRAM or SRAM up to 256 KB. We have yet to see a sensor package that offers connectivity for external RAM, although there is no lack of addressability in the operating systems.

Many packages offer OS support for encryption, hardware accelerators and random number generators; typically, AES256/128 with ECC, SHA-1, SHA-2, etc. Unfortunately, without much more memory than that available in current offerings, getting these crypto libraries to operate at the sensor – with any speed or efficiency - is not going to happen. In spite of marketing claims around IoT security by many IoT solution providers, we have found not a single set of application-layer crypto libraries that operate to actually encrypt communications from the sensor to the edge. Digging under the covers of these security claims, we find the usual consulting proposals to identify the usual vulnerabilities and put in place the usual defensive measures.

Lightweight Cryptography Standards Program at NIST

In April, 2018, NIST began proceedings to establish standards for " **Lightweight Cryptography for IoT**." Recognizing the shortage for CPU power and adequate memory for encryption on these devices, NIST has solicited proposals to solve the tiny device problem. Currently, they have 56 round one candidates. Unfortunately, the standards confirmation process up through ISO/NISO may take a few years. As it progresses, we may expect the solutions, no matter how small or efficient, to require much more memory in the sensor.

Interim Solutions

Meanwhile, the problem could be solved quickly if the sensor package manufacturers simply added more memory – 500 MB to 1 GB would do it. The form factor of the sensor package might increase by a millimeter or two and the cost increase by a few bucks – but security all the way to the sensor would be achieved. The edge hubs and controllers are already Linux or Windows devices with plenty of memory for encryption. But, hold on; more memory of the capacities required means more energy demand which might well mean that initially only line powered sensors could support the new configurations. Not a problem, because on the factory floor; in machinery, robots, etc. there is no lack of electricity and low voltage DC power. That is also true in connected cars, in hospitals and many other IoT markets.

It does not appear that the market pressures for sensor-level encryption have become critical enough to get the manufacturers to simply provide more memory. When they do, we may expect the IoT solution providers to start offering limited home-grown encryption libraries and application-layer solutions that connect only from the sensors to the edge device, which the implementor will have to program for each situation.

This opens the door for TrustWrx to be there with a complete packaged solution - far more robust and protective – one that reaches seamlessly across the cloud, from the sensors to the edge, and right back to the central servers. Across many industries the many providers of IoT solutions could become TrustWrx customers, as it would be far more efficient, cost-effective and easy for them to bundle a complete security solution into their services mix, rather than starting from scratch to build it themselves.

IoT Operating Systems, Programming Languages and Protocols

The standard IoT protocols, Zigbee, 802.15.4, MQTT and others pose no limitations on cryptography. The newer operating systems from Wind River, Amazon FreeRTOS, Riot, Contiki, Linux and a few others offer a good level of support for various forms of encryption. All these operating systems and protocols operate and communicate in the TCP/IP or UDP transport layers. In the interests of code efficiency, programming languages are typically C and other compliers. This means that the TrustWrx client-side Java code would need converting to C to run most efficiently on the small footprint sensors. That conversion is not a large effort; it will also provide an opportunity to enhance functionality and performance specific to devices and protocols.

OS	Min RAM	Min ROM	C Support	C++ Support	Multi-Threading	MCU w/o MMU	Modularity	Real-Time
Contiki	<2kB	<30kB	○	✘	○	✓	○	○
Tiny OS	<1kB	<4kB	✘	✘	○	✓	✘	✘
Linux	~1MB	~1MB	✓	✓	✓	✘	○	○
RIOT	~1.5kB	~5kB	✓	✓	✓	✓	✓	✓

TABLE I
KEY CHARACTERISTICS OF CONTIKI, TINYOS, LINUX, AND RIOT. (✓) FULL SUPPORT, (○) PARTIAL SUPPORT, (✘) NO SUPPORT. THE TABLE COMPARES THE OS IN MINIMUM REQUIREMENTS IN TERMS OF RAM AND ROM USAGE FOR A BASIC APPLICATION, SUPPORT FOR PROGRAMMING LANGUAGES, MULTI-THREADING, MCUS WITHOUT MEMORY MANAGEMENT UNIT (MMU), MODULARITY, AND REAL-TIME BEHAVIOR.

From Riot OS: Towards an OS for the Internet of Things

Summary

It is now apparent that the edge device-to-sensor security problem is singularly constrained by the lack of adequate executable memory in the remote sensors - memory needed to run encryption algorithms. All other components are already in place, including the operating systems, protocols, hubs and controllers that have all the needed resources to bring sensor security to high levels of privacy – once the sensor memory problem has been fixed. Waiting on NIST and ISO/NISO to provide standards solutions will not be acceptable as the explosion of commercial IoT implementations, and the increasingly dangerous exposure of IoT networks will demand solutions much sooner. Providing more memory would be simple and fix this problem directly.

TrustWrx is uniquely positioned today to provide a comprehensive solution from central servers to the edge. Securing the communications from the edge to the sensors is a fairly straightforward addition. All we need now is for the sensor manufacturers to match their products to the needs of the market.