Security for Intelligent, Connected IoT Edge Nodes

- The Internet of Things (IoT) reflects one of the biggest technology waves to pass over in a couple of decades. With forecasts of as many as **50 billion connected devices in 2020**.
- In assessing IoT network vulnerability, developers have zeroed in on the most fundamental elements — the edge nodes. Otherwise known as the “Things” in the Internet of Things, they are the many sensors and actuators that provide the data for the IoT and carry instructions out from the Cloud or a user interacting via a computer, cell phone, in-car system, smart appliance, or other platform.
- When it comes to securing such systems, people often equate “encryption” with the term “security” when in fact that is **only a piece of the security puzzle,*BUT***

Security for Intelligent, Connected IoT Edge Nodes

- **But** one of the first things that must be done to create a secure environment is to reliably discover and prove the identity of elements that are connected to your network.
- To get a better feeling for node security, let’s look at logging into your online bank account as an analogy. You first set up a secure (i.e. encrypted and authenticated) connection between your computer and the bank’s website (which is an https link). However, this secure link does not authenticate you — it only authenticates your computer while creating an encrypted communication channel between your computer and the bank. At this point, the bank does not know you from an imposter. That is where your password comes in. Your password is your cryptographic key, so in theory, only you and the bank know your password. Once you send it to the bank, it compares that to your password it has stored. If they match, then as far as the bank is concerned, you are proven to be who you say you are.

Security for Intelligent, Connected IoT Edge Nodes

- From this example you can see that online banking security is provided in two layers:

  □ The transport layer that sets up the secure connection.

  □ The application layer that proves (authenticates) your identity via your password. **Similarly**, IoT node security must also be multi-layered if the IoT is to be taken seriously.

- For IoT nodes, **TLS** is also used to create a secure connection, such as to the cloud. But, to be truly secure, an IoT node must also obtain application layer security. That means that **the node itself**, and not just the communication channel (i.e. the pipe), should be authenticated. **In addition to channel authentication**, encryption and data integrity should be established at the application layer to protect the data flowing through the pipe.

Security for Intelligent, Connected IoT Edge Nodes

- Tight security involves three fundamental elements, which we refer to by the acronym “CIA”:

  Confidentiality – data, whether stored or in transit in a message, should be visible only by authorized persons;

  Integrity – a message sent should not change on its way to its destination; and

  Authenticity – one needs confidence that the sender of a message is who they say they are.

- Different technologies contribute to these elements, but common among them is the use of secret or private keys that serve as part of a unique, verifiable identification tag. How those keys are managed – their storage and communication – determines the security of a system.

Edge-Node Vulnerabilities: What Could Possibly Go Wrong?

- we need a better picture of what the vulnerabilities are so that we can provide effective protections. There are two aspects to this: identifying ways that an attacker can compromise the node, and understanding the consequences of such action.

  Attack Modes

  There are four ways to get into an edge node:

- Through the network
- Through external ports
- Through proximity attacks (also referred to as “side-channel attacks”)
- Breaking into the device (Physical attack)

Consequences

- Of course, we lock only those things we think contain valuables. It might seem that a simple sensor node would be of limited value to an attacker, but the consequences of a successful attack can put an entire network, and anything connected to that network, at risk.
- By breaking into the edge node, even through a network security weakness, the attacker may get access to all of the secrets that the security is supposed to protect – and in particular, the keys needed to implement security. Once the keys are taken, then all other security protections can be defeated – including encryption and message authentication.

The Right Way to Protect an Edge Node

- The following measures, all of which involve key storage in one way or another, will ensure that such attacks can be thwarted. While there are never 100% guarantees with security, these measures offer the best possible protection, and they ensure that an attacker has no way of determining critical system keys. These approaches each support the important elements of CIA:

  Authenticity – Prove the identity of any visitors coming in over the network.

  Authenticity – Authenticate any accessories that try to attach to the node.

  Confidentiality – Encrypt messages.

  Integrity – Append a Message Authentication Code (MAC) to all messages to prove that no one has altered the message en route.

Future work

- There are a variety of enhancements that could be made to this system to achieve greater accuracy in sensing and detection.

  1. There are a lot of other sensors that can be used to increase the security and control of the home like pressure sensor that can be put outside the home to detect that someone will enter the home.

  2. Changing the way of the automated notifications by using the GSM module to make this system more professional.

  3. NFC technology