SECURITY

FOR THE INTERNET OF THINGS

A WHITE PAPER BY INGENU

SECURITY FOR THE INTERNET OF THINGS

Nearly five billion things are already connected via the Internet of Things (IoT) and that number is set to hit 25 billion by 2020 according to Gartner . But what if each of those 25 billion things were easily attacked and compromised by hackers? According to one Business Insider survey, 39% of respondents have that very concern . And that concern is understandable, the data devices collect and transmit is valuable, often sensitive, and should be secured as such. This paper will identify how to keep devices secure on the Internet of Things.

SECURE BY DESIGN

Security by design is a way of designing technology that assumes someone will try to hack it. The difference between security by design and bolted on security, or security as an afterthought, is much like building a road and then realizing only afterwards you want to put sewer pipes in. While it can be done, it will be costly in time and resources and won't be quite the same end product. So designing for security up front changes the way a device is programmed and improves the overall security of the system to which that device connects. Of course not all security issues can be conceived up front but the fundamentals should be, which brings us to our next point: protecting from future vulnerabilities.

> A recent study completed by HP concluded that 70% of deployed IoT solutions contained security exposures

PROTECT FROM FUTURE VULNERABILITIES

As the security landscape changes and new vulnerabilities arise, devices connected to the IoT should be able to upgrade to be secure against those vulnerabilities.

Firmware Upgrades

As more devices are added to the IoT it will become a more attractive target for hackers, who will develop new ways to obtain your valuable data. Not being able to upgrade is a serious concern because it essentially leaves devices in the same state as when they were initially installed. If a new security vulnerability is threatening enough and the data sensitive enough, and your devices can't upgrade their firmware to combat the hack, then companies will be forced to either upgrade to new hardware or abandon the devices altogether. Moreover, some devices only make sense to have connected if the hardware never has to be touched again after installation. Being able to download firmware upgrades makes it so you won't need to touch the device hardware again. So, to prevent such potential loss of economic gains, firmware upgrades should be possible through the chosen IoT wireless connectivity provider.

Firmware Upgrade Authentication

Even if a connectivity provider offers firmware upgrades, those upgrades must also be authenticated. That is, the connectivity provider should be able to assure that the endpoints know when an "upgrade" is legitimate or not. If a hacker accesses the network and sends an "upgrade" to the endpoints that contains malicious firmware they could compromise the entire system. However, with firmware upgrade authentication, your devices can be sure that whatever upgrades they receive are from a legitimate source.

MESSAGE CONFIDENTIALITY

Encrypt Your Messages

Confidentiality means that even if a message gets snooped while on its way to the recipient, the message should not be understandable. Encryption is what offers this kind of confidentiality to messages across a network. Encryption takes a message and scrambles it using a special method that makes it very difficult to unscramble. If your devices send messages across the network without encryption, then, if intercepted, those messages could be read and understood by anyone.

Not All Encryption is Created Equal

The type of encryption used for your devices' messages should be powerful enough that a brute force attempt to unencrypt it should be essentially impossible. Brute force unencrypting is basically taking a very fast computer and trying every possible "key" that could have been used to encrypt the message in the first place. If the number of possible keys is small enough and the computer is fast enough, a hacker could successfully brute force unencrypt your messages.

MUTUAL AUTHENTICATION: KNOW WHAT'S CONNECTED

A lot can be learned from your messages even if they are encrypted. Information like message size, message frequency, and message send times can all be useful even if the actual message content is not obtained. These encrypted messages could be analyzed by tricking a legitimate node into accessing a fake network. Another way to learn about the network traffic is tricking the network into giving a fake node network access. Both of these security vulnerabilities can be addressed using mutual authentication. Mutual authentication means that only the right nodes can connect to the network, and that nodes will only connect to the legitimate network.

MULTI-CAST AUTHENTICITY

Multicasting means simultaneously sending a message to a defined group of endpoints. This is slightly different from broadcasting a message, which is sending a message to all endpoints simultaneously. It isn't a given that a system that is capable of mutual authentication to a single endpoint is also capable of multicast authenticity. Multicast authenticity allows for secure message transmission to a defined group of endpoints. If a network isn't capable of multicast authenticity, then whenever it sends messages via multicast, those messages become vulnerable.

KEEP IT SIMPLE AND FOLLOW THE STANDARDS

It is important that security be kept simple and transparent to IoT customers. If security isn't understood, then its potential vulnerabilities won't be either. Following standards allows for such transparency and makes it easy for customers to know what kind of security they are getting. Some candidate standards and guidelines include the following, among others:

- NERC CIP 002-009 cyber security framework for critical cyber assets
- NIST SP 800-53 guidelines for protecting critical cyber assets
- FIPS 140-2 Level 2 encryption standards
- NISTIR-7628 guidelines for smart grid cyber security

Want more information?

Please contact us via email at **info@ingenu.com** or visit our website at **www.ingenu.com**