Security in IoT systems

Following on from our article “8 good reasons”, we try and outline what IoT is and how difficult it can be to secure properly.

In an article written by the world- renowned security expert – Bruce Schneier www.schneier.com/crypto-gram/archives/2017/0215.html he describes the The Internet of Things as a Robot and he has a valid point. A classic robot – one that places and welds car panels on a car has all the components that make a robot – namely sensors, processing and actuators. Humans have much the same features – senses (touch, smell, sight, hearing etc) – processing in the brain, and muscles and tendons that do work.

The Internet of Things can be thought of as robot – with the following features

1. Smart sensors, gather information on their immediate physical location and report this to “the Cloud”.

2. In the Cloud (in the good old days this was just called the server) algorithms aggregate the data. They perform “what if” analysis and predictions based upon past trends - the so called “pattern of life”. The cloud sends commands to the smart actors to alter the physical world based upon the algorithms.

3. Smart actors receive commands from the cloud and operate real world machinery to alter our physical world.

To illustrate just how the Internet of Things is all pervasive and already in our lives the following is an example from a national electricity grid.

This industry is focused on generating and providing energy to millions of customers nationwide. It has a number of different generation capabilities – nuclear, coal, wind, solar, oil, gas, water and bio-digestion, each with different characteristics. Fast reacting systems are oil, gas and water storage. Slow reacting systems are coal, nuclear and bio-digestion. Unreliable generation is wind and solar. In addition, there are seasonal effects on generation. The demand is also effected by seasonal and daily events.

So the problem is to manage the generation and distribution of electricity across a country in the most efficient manor, and increasingly, with the environment in mind, carbon tax.
Effective systems have evolved that monitor the weather, nuclear and bio-digestion production. These are systems that either cannot be controlled (in the case of the weather and the sewerage produced) or they are very difficult to alter the production of energy. These are systems that will be altered at last resort.

Unreliable energy production is used next, because the weather cannot be turned off, so either the wind farm is left to “free wheel” or it is used to generate electricity. Additionally, these large capital expense items need to pay for themselves.

Top Up energy production, to meet the varying demand, is generated by Oil, Gas and water storage systems. These can come “on-line” within seconds or minutes and help manage the load on the grid.

All of the generation and consumption system can be viewed as a Smart System with sensors, processing and actors. Smart sensors gather information on the weather, the rate of sewerage entering a bio-digestion facility, the state of the tide etc. Cloud computing aggregates this data, performs statistical analysis and predictions. Historical data, time of day and special events – “e.g. world cup final events” are all used to predict the future supply and demand. Smart actors are then commanded to bring on line, throttle or remove generation capability from the grid to meet the forecasted demand.

In our example, what you may ask, has this to do with Cyber and IoT.

Well as with every system on the earth they are slowly being connected to the World Wide Web of computers. Problem is, the Web was never designed with security in mind and especially IoT. Governments, Companies and customers are scrabbling to catchup with the level of disruption caused by state actors, criminals, hacktivists and hackers.

The energy generation and supply system is especially vulnerable to this and governments are actively perusing strategies to protect this critical national infrastructure. The Ukraine power outage shows just how vulnerable the systems are and how ingenious state actors can be in disrupting systems that most people and never heard about.

How do we go about protecting IoT systems, that are distributed and have a number of competing requirements?

We have discussed trust, authentication and communication in the last article, but just to recap…. The cloud computer (just like a human) can only make decisions based upon accurate information from its sensors (eyes, ears, nose etc). The sensors in the IoT system must deliver accurate and timely information to the cloud otherwise the cloud might make erroneous decisions that could lead to disasters.

In a critical system, like an aircraft, the speed indicator is crucial to the operation of the aircraft systems – thus there are numerous, independent ways to measure speed. In addition, the communication between the speed sensors and the aircraft control computers are in closed systems that cannot be altered. Not so for IoT.

So having established that accuracy and timely delivery of information from the Smart Sensors to the Cloud is essential, we need to have a method of guaranteeing (authenticating) the messages. Authenticated messages are only half the story – we must ensure that authenticated messages come from a trusted source. It's no good having an authenticated message from a untrusted source because we cannot be sure that the message is correct.

So we need Trust AND Authentication. Finally, we might want to obscure the message so that it cannot be interpreted by an unauthorised 3rd party.

Trust is built by having an unalterable system that once manufactured and programmed by a trusted company in a trusted country can be deployed, save in the knowledge that it is unalterable.

The idea of a trusted company and country to manufacture the equipment is critical. Equipment manufactured in the far-east has been demonstrated to contain un-trustworthy software & hardware and will compromise the entire system when deployed.

Even if a trusted company and country has manufactured the equipment the final programming of the equipment must be performed by a trusted party at a trusted location. The easiest way to attack IoT is in the supply chain of the equipment where trust is taken for granted but not guaranteed. Think of routers and home WiFi hubs that are manufactured in vast volumes by companies which have little time for security.

The only method to guarantee a trusted system is to have an automatic programming equipment that has been designed as part of the Trusted system. This programming environment cannot be altered and once deployed for the programming of the IoT devices it is unalterable and unclonable. The Automatic Programming Equipment must be designed, manufactured and distributed by a trusted company or country.

An example of this is the easy attack vector for criminals to attack credit cards. They only have to steal/buy/borrow a credit card reader and then perform transactions on that. They are not attacking the credit card itself, but the equipment used to interact with the credit card.

Finally!

We now have a trusted IoT Smart Sensor, that has been manufactured by a trusted company from a trusted country and programmed using a trusted Automatic Programming Equipment! This is connected via an untrusted communication channel that we authenticate and obscure using encryption.

The cloud is on a trusted server, and has the ability to authenticate and decrypt the messages from the smart sensor. Finally, the cloud can communicate with a Smart Actor that is trusted, has been manufactured by a trusted company from a trusted country and programmed using a trusted Automatic Programming Equipment. The actor executes the commands received from the Cloud computer after authentication and decryption.

IT IS CRITICAL TO UNDERSTAND THAT A SUCCESSFUL ATTACK AT ANY POINT IN THE ABOVE CHAIN WILL RESULT IN A BREACH OF THE SECURITY.

This is why cyber security is so pernicious and difficult to get right. The attack surface for IoT is immense. Every connected IoT device (Smart Sensors and Smart Actors) is a potential entry point for an attacker. The Cloud computer itself has massive vulnerabilities, that if breached will compromise the entire system.

An example of this is the AES256 encryption standard. This is a very good encryption standard with no known successful attack on the algorithm. However, the implementation of the algorithm provides many opportunities to "crack" it. Hardware based AES encapsulated in a special chip is virtually impregnable from attack. However, if the key used is stored in memory, then it is vulnerable.

Software based AES encryption is not secure – period. Many examples exist – from differential power analysis to memory dump and have shown that the implementation is always the critical part of the process. If the cloud computer has been infected by malware then the malware can potentially capture keys and compromise the whole security of the system.

In the attack on the Ukraine power grid, the attack vector was the entry into the SCADA (control computer) by an attacker that had copied/stolen/borrowed a maintenance engineer's key card. Once in the system it was just a matter of time and persistence to map the whole Computer Server and plant malware into critical elements of the system. Even though the Servers had AES256 protection this was rendered useless by the insecure use of key cards.

Summary

So what have we learnt? The lessons are:

1. Trusted IoT devices, must be produced by a Trusted supply chain using Automatic Programming Equipment (APE).

2. Cloud computing (servers) are not secure and must be treated as such.

3. Hardware encryption/decryption is the only guaranteed way to ensure security.

4. The attack surface is very significant for IoT devices.

5. Humans are very bad at security and must be designed out of the loop at any point.

The next article describes how we can produce systems and processes to overcome these lessons.