Internet of Things a Potential Security Disaster

Experts believe the Internet of Things will be highly insecure, at least in the early days.

By **Paul Rubens** | Posted September 04, 2014

The Internet of Things (IoT) could be a security disaster waiting to happen.

That's the view of Andrew Rose, a Forrester Research analyst. He believes that early IoT implementations will inevitably be highly insecure, forcing companies involved to ratchet up security later to avoid serious problems.

"I think that will pretty much be the case," he said. "The cause will be naivete. People won't have thought through all the use cases for the Internet of Things when they implement it, and they will focus on functionality rather than control systems. That will give malicious people an opportunity to work the technology for their own benefit."

In fact, a recent study from HP Security Research found that 70 percent of Internet-connected devices are vulnerable to attack. Insecure Web interfaces and a lack of encryption were among the issues flagged in the study.

Network Topography of the Internet of Things

To get an idea of where potential security problems can arise, let's consider the topography of a network of things. It's a collection of objects equipped with sensors which generate data and transmit it over a communications network to each other and to servers which control the sensors and collect data from them.

A classic example is a smart metering system, which involves a network of electricity meters that measure consumer electricity usage and send the data back to an electricity company's servers. The servers may also send data, such as tariff changes or firmware updates, back to the meters.

It's immediately apparent that there are a number of ways that the integrity of data collecting in this type of setup could be compromised:

- A fake meter that transmits false data (probably indicating less consumption than is actually occurring) could be installed on the network to impersonate a genuine one.
- A genuine meter could be tampered with so that it sends out incorrect data - either by modifying its physical connections or the software it runs.

- The data from a meter could be intercepted and modified by a network eavesdropper.
- Malicious users could install a fake server or compromise a genuine one to issue malicious commands or upload malicious firmware to meters on the network.

Likely IoT Attacks

When a similar topography of sensors, network and servers is used in an industrial or national infrastructure setup, successfully hacking the system could have potentially devastating consequences, according to Claude Baudoin, a senior consultant at Cutter Consortium. In a report on IoT security he suggests three likely forms of attack on this type of Internet of Things:

- **Listening in on the data or the commands** could reveal confidential information about the operation of the infrastructure.
- **Injecting fake measurements** could disrupt the control processes and cause them to react inappropriately or dangerously, or could be used to mask physical attacks.
- **Sending incorrect commands** could be used to trigger unplanned events, to deliberately send some physical resource (water, oil, electricity, etc.) to an unplanned destination.

In addition to criminals or terrorists, these types of IoT implementations could be at risk from script kiddies, hacktivists, disgruntled employees or even foreign intelligence or military agencies, Baudoin suggests in the report.

A general tenet of IT security is that if the physical security of a device has been compromised, this is tantamount to a logical breach; that's why data centers have access controls and other security measures to keep out unauthorized people.

Keeping IoT devices secure from theft is hard, so the challenge will be to make them tamper-proof to ensure their physical connections can't be modified, their operating system or firmware can't be altered, and any data they contain can't be extracted in an unencrypted form. That's especially true when some "things" are used as data collection hubs for other sensors located nearby, making them more valuable targets for hackers.

IoT Security Standards and PKI

The good news is that PKI technology, which includes the ability to digitally sign firmware updates, and for devices to authenticate that they are genuine, is readily available. It also enables data to be encrypted securely while it is stored on devices and as it travels over communications networks. This last is especially important if the data travels over a public network like the Internet.

PKI technology also provides a way to prevent eavesdroppers intercepting and modifying data, and for genuine control and data collection servers to authenticate themselves to prevent malicious users setting up fake ones.

The problem is that PKI technology may be sound, but implementing it correctly can be very difficult.

But enterprises may not have to worry too much about that themselves, because a group of hardware and software companies including Cisco, Intel, General Electric, AT&T and IBM have teamed up to form the Industrial Internet Consortium (IIC) to produce security standards for the IoT. These will include standards for securing the integrity of the devices themselves, and also standards for secure data communications.

IoT Weak Links and Black Swans

But standards won't solve all of the problems. Security is only as secure as the weakest link in the chain or, in the case of the IoT, the least secure device on the network. That means that enterprises will have to make a huge effort to ensure that every part of any IoT they are involved with is secure and standards compliant.

"The Internet of things is a network of many things; it is the world's biggest mashup," said Rose. "You are drawing in data from many sources, and the problem is that each source is independent. Not all will be the same quality, and the chances of all of them being secure is pretty remote. Things that are not secure will be part of the system, and then you have a problem."

As an illustration of this, researchers at French technology institute Eurecom recently downloaded about 30,000 firmware images from potential IoT device manufacturers including Siemens, Xerox, Bosch, Philips, D-Link, Samsung, LG and Belkin. They discovered a range of security problems in the firmware, including poor encryption and backdoors that could allow unauthorized access to devices. In total more than 123 products contained 38 different vulnerabilities.

Then there is also the Black Swan problem that applies whenever something new, like the IoT, is implemented. There is always the risk that any emerging standards will overlook a security problem that is obvious in hindsight, but not obvious before it is recognized.

As an example, consider Windows XP. When it was launched it was touted by Microsoft as its most secure operating system ever. But it had to be patched regularly to close critical security vulnerabilities as they were discovered after it was released.

It's likely that the same will be true with IoT implementations, according to Ruggero Contu, an analyst at Gartner. "Some security measures are often not thought of originally and embedded in the system, so they have to be put in later," he said. "A lack of attention and planning is always a source of security problems that inevitably come up when new technology is deployed."

Microsoft coped with this by instituting its Patch Tuesday routine, but clearly "things" like sensors in autonomous cars will need to be patched as soon as possible to prevent security vulnerabilities resulting in serious injury or worse.

Privacy and the Internet of Things

One final potential security problem that is worth mentioning relates to privacy and data protection, where security breaches can lead to heavy fines. "Data that you collect can become personal or private when you collect lots of it, because it becomes easy to identify people - it pops out of the information - when you have enough of it," Rose explained.

No matter how secure the IoT infrastructure, in other words, enterprises will still have to pay extra attention to the security of all the data center infrastructure that stores and processes the data that comes in from the IoT.

As an example of a potential problem, Rose imagines a car hire company that has a device in each car that collects information about where the cars go, how far they travel each day and how fast they are driven.

"A marketing department would love to know this kind of information, and if the data was uploaded automatically it could be very beneficial," Rose said. "But if the data shows that someone was traveling over 70 miles per hour, it would be evidence of a crime, and you don't want to store that. So you have to start thinking about data security and what information it is sensible to keep, or what information is too sensitive."

Paul Rubens has been covering enterprise technology for over 20 years. In that time he has written for leading UK and international publications including The Economist, The Times, Financial Times, the BBC, Computing and ServerWatch.