Detecting Security Attacks on the Enterprise Internet of Things: an Overview

Mowbray, Miranda

Hewlett Packard Labs
HPE-2017-04

Keyword(s):
internet of things; security analytics

Abstract:
This article describes a paradigm for detection of Internet of Things (IoT) security issues in the enterprise. IoT is becoming increasingly important to enterprises. The scale of IoT, the simplicity and homogeneity of IoT devices, and the possibility of using sensor data to detect attacks make IoT security different from traditional PC network security. These features of the IoT, together with the large memory capacity of coming hardware devices, can be used for a security analytics tool specially attuned to IoT security.
Detecting Security Attacks on the Enterprise
Internet of Things: An Overview

Miranda Mowbray, HPE Labs Bristol

Abstract: This article describes a paradigm for detection of Internet of Things (IoT) security issues in the enterprise. IoT is becoming increasingly important to enterprises. The scale of IoT, the simplicity and homogeneity of IoT devices, and the possibility of using sensor data to detect attacks make IoT security different from traditional PC network security. These features of the IoT, together with the large memory capacity of coming hardware devices, can be used for a security analytics tool specially attuned to IoT security.

1 Introduction

Internet of Things (IoT) use offers enterprises significant potential for business advantage, and enterprise IoT is predicted to have very substantial growth. As enterprises increase their reliance on IoT devices, security of these devices will be increasingly important. IoT security requires consideration not just of the device itself, but of the broader ecosystem that makes it work, including for example related apps, web interfaces, cloud services, and other devices that interact with it – this will be referred to as an “IoT system”. In part because of the large attack surface, IoT security is inherently difficult; this will be discussed further in Section 2. Enterprise IoT systems are therefore unlikely to be free from vulnerabilities. The detection and remediation of security attacks on IoT systems will become an increasingly important part of the enterprise security industry.

Advances in processing and memory predicted by Moore’s Laws suggest that in the next decade a tool for data analysis to detect security attacks should be able to analyse ten million events per second (Fink, 2015). These events could all come from taps of a relatively small number of servers serving a very large network; but alternatively, they could come from ten million sensors or other IoT devices.

Section 2 of this use case cites predictions for the expected growth in enterprise adoption of IoT, explains why it is hard to make IoT secure, and gives evidence of its current level of insecurity. Section 3 describes features of IoT that can be exploited to make the paradigm more effective for IoT security than traditional security tools designed for traditional PC networks. Section 4 gives examples of analytics might be used to detect attacks on IoT systems (and also malfunctions and misconfigurations). The last subsection of Section 4 describes five real examples of attacks on IoT systems (not just vulnerabilities, but instances in which those vulnerabilities were exploited), and explains how similar attacks might be detected. Finally, Section 5 describes a proof-of-concept analysis of real IoT data from weather stations, and gives examples of several malfunctions and misconfigurations revealed by this analysis.
2 Why IoT Security is Important

2.1 IoT Predictions

It has been widely predicted that IoT will be the greatest engine of future growth in the information technology industry. Gartner, Inc. forecast in November 2015 that 6.4 billion connected things would be in use in 2016, up 30% from 2015, with 5.5 million new things getting connected each day; and that by 2020 the number would be 21 billion, and the total market size 3 trillion dollars (Gartner, 2015). International Data Corporation has forecast a 98.8 billion dollar IoT market in manufacturing operations by 2018, with early growth driven especially by retail digital signage (Hughes and Murray, 2015).

IoT use offers enterprises significant potential for business advantage. A Forbes article says that “the flow of IoT data should mean better products, better service, and more value for the customer, with a lower risk for the manufacturer” [Woods, (2015), p.3]. A Verizon report predicts that “by 2025, organizations that adopt IoT extensively will be at least 10% more profitable than competitors that don’t”, through increased revenue, improved operational efficiency, and finding new ways to do business [Verizon (2015), p.4].

2.2 IoT Security: necessary and challenging

IoT systems are already used for applications critical to human safety (e.g. pacemakers) and business viability (e.g. factory fire sprinkler systems). Networked industrial control systems already control water and sewage systems, oil and gas pipeline flows, power stations and wind farms, ships, airports, and traffic. (Industrial control systems may be Internet-connected, or may be separated from the Internet and networked over an Operations Technology (OT) link. The phrase “Internet of Things” is limited by some authors to mean only Internet-connected things, but the paradigm described in this article is also applicable to industrial control systems in OT networks.)

IoT devices may be sensors, which obtain data about the physical world, or actuators, which take actions in the physical world, or they may do both some sensing and some actuation: for example, a digital thermostat both senses temperature and adjusts heating. Subversion of actuators can do harm directly. Subversion of sensors can be used by attackers to feed incorrect data into the system, or to suppress the feeding in of correct data, as part of an attack; for example, an attacker might block signals from a burglar alarm, or feed false data into a competitor’s agricultural sensors so that their crops were watered at the wrong time. Moreover, the devices themselves are just part of a larger IoT system, which may include for example wireless connections from the device to the local network and web-based user interfaces for the device, which may have vulnerabilities themselves that can be exploited (Smith et al., 2014-2016). Vulnerabilities in IoT systems can open up possibilities for attackers to use them in ways that are not obvious from the intended use of devices, for instance potential theft of personal data using APIs for connected cars (Hunt, 2016), or the potential use of insecure hospital videoconferencing systems for phishing, or for exfiltration of healthcare records, which are valuable on the black market (Filkins, 2014). An insecure IoT device may also provide an entry point into other parts of the network.
As enterprises in a wide variety of industries increase their reliance on actionable information generated by IoT devices used in production and distribution or sold to their customers, they increase their vulnerability to attacks on these devices. IoT security is, however, a challenging problem. Attacks on an IoT system may exploit flaws in hardware security, wireless security, phone app security, web app/operational security, desktop security, or in interactions between these. Multiple vulnerabilities have been found for IoT products at all of these attack surfaces. Moreover, the supply chain for IoT products can be long, involving many small teams in different countries building different layers of the product, few of which include security specialists, and any of which may inadvertently or deliberately leave a backdoor in the product (Guzman, 2015). As the IoT market evolves, interactions between different IoT products and services will become more common, producing even further expansion in the attack surface. The lack of ruling standards also means that individual protocols may not be audited enough, and the need to interface multiple protocols is yet another contribution to the attack surface size.

The size of the attack surface is not the only challenge for IoT security. Since the profit for IoT devices is made from their associated services rather than the hardware, margins are squeezed for the physical devices, some of which (particularly sensors) have been designed with insufficient power, processing, memory and/or bandwidth to allow for the use of standard secure protocols. While Moore’s Law can ease this problem over time, legacy devices with these or other security flaws may continue to cause problems. For example, the Raspberry Pi model A (Raspberry Pi Foundation, 2016) is still being produced because it is so widely used in industrial applications. The default user name and password for every Raspberry Pi model A are “pi” and “raspberry”, and users do not always bother to change them (Rogers, 2015). Good cryptography is reliant on a suitable entropy source for random number generation; some sensors lack such a source, as they are designed without a user interface or other suitable incoming connection.

Some devices are hard or impossible to update or replace if an attack is discovered; as an extreme example, sensors may be built into the fabric of bridges and roads. On the other hand, some IoT products make updates too easy – they allow firmware updates that are not encrypted or signed, and so may be from an attacker. Unlike traditional IT products, many IoT products are produced by companies whose principal business is not in IT, and may not have resources for effective IT vulnerability response processes. This is particularly true of small businesses in traditionally low-tech sectors. At the other end of the scale of technology expertise, power station operators have their own specialist security experts, but the bureaucratic and (rightly) scrupulous processes of testing and authorization required before changes can be made to critical parts of their code can mean that it may take a year to correct a known vulnerability.

2.3 IoT Security: necessary and challenging

As a consequence of the issues just described, and others, the current state of security in the IoT is not good. HPE Fortify research found that there were an average of 25 privacy and security flaws per device in a study of 10 of the most popular devices for common IoT niche applications, including a sprinkler and a door lock; that man-in-the-middle attacks on a smartwatch communicating with a smartphone would be “effortless”; and that 10 out of 10
home security systems were vulnerable to account harvesting (Smith et al., 2014-6). The authors of a Rapid7 report (Stanislav and Beardsley, 2015) which found 10 new vulnerabilities in 7 baby monitors, say that “it is rare to find an IoT device that doesn’t exhibit at least one critical failing” (p.6). An article in The Register (Chirgwin, 2014), reporting a discovery that an attacker with physical access to a Nest thermostat could gain full administrative control of it in 15 seconds and cause it to run arbitrary code just by holding down the power button and inserting a memory stick (Hernandez et al., 2014), had the subtitle “Security? But this is the Internet of Things!”

These studies were mostly on consumer IoT devices. Enterprise uses have potential vulnerabilities that are not so much a concern for consumer use. For instance, large numbers of people may have physical access to an enterprise device, which increases both attack opportunities and potential consequences of damage to actuators; enterprise wireless networks may be more widely accessible than home networks, for example through “wardriving” (accessing open wi-fi networks from a moving vehicle); some enterprises need to safeguard especially valuable data; and attackers may profit from an enterprise’s woes via market speculation.

3 What Makes It Different?

Since enterprises are increasing adopting IoT systems, and good IoT security is difficult to achieve in general and not as widespread as it should be at present, these enterprises are increasingly reliant on systems that are likely to contain vulnerabilities. These vulnerabilities will be discovered by attackers over time and will be exploited to carry out attacks on enterprises. The detection of IoT security attacks, therefore, is likely to be a prominent sector of the enterprise cybersecurity industry, and there will be a market for tools specially designed for this.

This section describes features of IoT that make IoT security different from traditional network security, and how these features could be exploited in the design of a security analytics tool making use of advances in memory capacity to produce improved performance over competitive offerings based on security solutions for traditional networks.

3.1 Partially Centralized Architecture

The security architecture containing the security analytics tool would be a partly centralised one. The centralised piece would be the security analytics tool itself. This could sit within an enterprise network, and analyse data just from that network; or it might access data from consumer devices sold by a single enterprise from the cloud. Individual devices will almost certainly not have direct IP communication with the tool and will not have an individual IP firewall. Rather, they will connect (wirelessly or otherwise) with a local IP gateway, which will typically aggregate data from several different devices.

Some detection and remediation of security problems is most efficiently done at a local level, so local security activities can be carried out at the level of the gateway; this is why the security architecture is only partially centralized. Either the tool could have a tap to gateway communications, or gateway data could be filtered or summarized locally and only items for which more global analysis would be useful would be forwarded to the centralized tool.
Automatic remediation may be challenging without deep knowledge of the environment. However, once the centralised tool has detected an attack it might suggest a series of tests and steps for remediation, and perhaps also take precautionary actions, such as instructing a gateway to block outward connectivity from a compromised device.

In addition to analysing data produced by the IoT devices themselves where this is possible, for example sensor readings or notes of actuations forwarded via the gateways, the analytics tool might use several other data sources to detect attacks. Some example data sources include logs for firewalls and intrusion detection systems, logs recording connection attempts (successful and unsuccessful) between devices and other machines in the network or in the outside world (for example from netflow, HTML proxy logs, and phone logs/phone bills), and information on privilege escalation events (eg from Microsoft event logs). Section 4 will give examples of uses of these data sources to detect attacks on IoT systems.

3.2 Differentiators

This subsection is about ways in which a partly-centralized security analytics architecture can have functionality that is especially suitable for IoT security, thus differentiating it from security analysis tools designed for traditional networks.

Some providers of security analytics tools for enterprise PC networks are marketing these tools for use in security analytics for IoT systems. For example, the security analytics section of IBM’s white paper on IoT security (IBM Analytics, 2015) promotes two tools, the IBM Security QRadar® Security Information and Event Management system and IBM Operations™ Analytics – Log Analysis, which were designed for enterprise PC networks. Some analytics techniques that were developed for PC networks can be effective on IoT networks as well, and it makes sense to apply relevant PC network techniques to the IoT case. However, there are also some aspects of the IoT which make securing enterprise IoT systems different from securing traditional enterprise PC networks.

The first aspect is scale. A very large enterprise network can have hundreds of thousands of active PCs, laptops and servers; but an enterprise might easily have ten million sensors. It is already a challenge to scale some enterprise security analysis tools to the size of a large enterprise PC network, without adding IoT systems. Building the tool that forms the centralized part of the security analysis system specifically to make use of the improved memory scalability of future hardware will allow greater scalability than these competitive security analytics tools.

Some vendors have focused on edge-based security for the IoT, which is one approach to providing scalability. For example each IoT device in an enterprise could have device authentication based on secure hardware, and an individual firewall/intrusion prevention system (Wind River, 2015). However, not all IoT devices are suitable for this kind of edge-based solution – for example they may not support an operating system. A good overall solution for IoT security will need to include protection at multiple levels, so edge-based detectors and controls can be useful. However, the information available at the edge is much less rich than the global view. By combining information from multiple devices, a security tool in a partly-centralised security architecture could detect devices whose behaviour is very...
unusual or sensors whose readings are inconsistent with others, and uncover lateral movement of attacks.

The best solution is to do some analysis of the raw data locally and forward outputs of this analysis (e.g. aggregated results or detected events) for further analysis from a global viewpoint. Section 4.1, and the discussion in the rest of this section, suggest some types of analytics that might be used to detect IoT problems. Some of these analytics would be better performed at the local level. One possible rule of thumb is to use centralized analysis just for IoT ecosystem security questions requiring the detection of patterns across multiple devices.

The second aspect is the relative simplicity and homogeneity of many enterprise IoT devices. Most of the predicted 21 billion devices in 2020 will be sensors, which will have a small repertoire of expected behaviours and are expected to connect with only a limited number of other machines or devices, and typically will be deployed in large batches of identical sensors. This allows for the detection of attacks by specifying the expected behaviour and connections of a device, and checking that the device only behaves as expected; and also by looking for devices behaving in a different way from other devices of identical design, although some allowance will need to be made for benign variations in device behaviour in different environments. Detection of policy violations and statistical outliers is already done for traditional PC networks. However IoT security analytics may be able to use policies for simple IoT devices that are much more restrictive than for PCs; and statistical outliers may be detectable with much greater accuracy within a set of simple homogenous devices than within a set of PCs, so that anomaly detection techniques that are too inaccurate to be very useful in practice on PC networks may nevertheless be usable for security analysis of an IoT system. More simply, there are more things that should never happen at all in an IoT device than in a PC, and a tool may be configured to detect these without any increased risk of generating false positives. The very large memory capacity of future hardware can be used to store models for each device describing both a detailed policy of what behaviours and connections are allowed for that device, and a statistical model of the device derived from its past behaviour. The analysis can compare these models with observed behaviour to detect policy violations and statistical outliers. A tool with large memory capacity can allow more detail in the models than is practical for more traditional security tools with smaller memory capacity. Traditional model-based/policy-based security analysis for large networks typically uses models that generalise the properties of a broad class of machines. In contrast, future memory capacity allows more specialized models; potentially every IoT device could have a different model.

The final aspect is the opportunity of using IoT devices themselves in the detection and remediation of attacks. For instance, a physical attack on a thermostat might be detectable because a security camera near the thermostat reported unusual activity, and nearby thermometers reported a sudden drop in temperature; and the temperature drop might be remediated by a heating system actuator separate from the thermostat. In general, IoT devices will be used to control physical properties of a space, and compromised devices will lead to unusual properties. Measurements of such properties, for example temperature measurements, will provide a type of data source that is not present in traditional PC networks. A copy of raw output data could be locally analysed first, with the outputs of this analysis forwarded to the centralised analytics tool. Data from these sources can be stored in the tool’s large memory for use in future analysis. For example, it might be possible to determine from past temperature data that the drop in temperature was highly unusual for the
season of the year and time of day, thus increasing the evidence that it was caused by an
attack on the thermostat.

4 Examples of IoT Attack Detection

This section gives some examples of types of analysis that an IoT security analytics tool
might carry out. It then gives examples of real attacks (not just vulnerabilities) on the Internet
of Things, and discusses which of these analytics could be used to detect similar attacks.

4.1 Types of Analysis

The standard taxonomy for security analytics identifies four different aspects of an attack
which may be detected: the initial infection; lateral movement as an attack moves from one
device to another; command-and-control, as an infected device communicates with its
malware controller; and exfiltration/damage, the unwanted consequence of the attack.

A list of indicators for these four different aspects of attacks on IoT systems is given below. It
includes both indicators that make use of the special features of the IoT described in section
3.2 (these are marked with asterisks), and indicators that can be used more generally but
which are useful for detecting some vulnerabilities known to exist in IoT systems, which are
either common in IoT or produce especially significant vulnerabilities. Traditional network
security indicators can detect attacks on IoT systems that exploit network vulnerabilities, and
so are still useful for IoT security, although the IoT attack surface is larger than that.

The idea is not that the security analytics tool should do all of these types of analysis: rather,
the point of this subsection is to show that there are a large number of opportunities for useful
analysis of IoT systems. In practice the tool could do a selected few, chosen to detect the
most common and/or most significant attacks in particular sectors. The next subsection gives
some concrete examples. An asterisk before an indicator means that the indicator uses the
special features of the IoT described in section 3.1.

To detect an initial infection, an IoT security analytics tool might look for the following:

* 1a. incoming connections from known bad addresses/protocols or not on a limited list of
incoming connections allowed by policy.

1b. traffic triggering intrusion signature detection rules or containing files that trigger known
malware family signature rules; especially if multiple rules are triggered for the same device
or the same rule for multiple devices. These rules may be supplied by Threat Intelligence.

* 1c. direct connections between two control hierarchy zones that are not supposed to
connect, in particular between the external zone and the cell zone. (The Purdue Model for
control hierarchy recommends separating the external zone, the corporate zone, the
manufacturing/data zone, the cell zone containing IoT sensors and actuators for Supervisory
Control And Data Acquisition (SCADA) systems, and the safety zone which contains the
instrument systems that control the safety level of an end device (Williams, 1992). There may
be further segmentation of the data zone according to the privacy/confidentiality level of
hosted data. Note that detecting such connections would require only a single centralized
security analytics tool to analyse connection logs. It would not require a separate tool in every zone.)

1d. multiple failed login attempts in a short time. (Some simple sensors don’t need to be logged into, but any device with a separate admin account does.)

1e. unusual amounts of default account use, or of admin account use by third-party vendors.

1f. configuration changes that occur unusually frequently or at an unusual time of day.

1g. unusually frequent booting or unsuccessful booting attempts.

1h. a device that has a repeated pattern of connecting to a second device, shortly followed by an attempt (successful or failed) at privilege escalation by device it has connected to.

* 1i. a device with behaviour that is statistically very unusual compared to other devices of the same type, or where most other devices of the same type that are logically or geographically close show similar behaviour that is different from the device in question.

* 1j. a sensor near the device, for instance a motion sensor, heat sensor or camera, detects unusual behaviour, after which the device behaves differently than before. (This is intended to detect the case that the device is compromised but the sensor is not. Another possible reason for unusual sensor readings is that the sensor itself is compromised, which may detectable by 1i.)

1k. a sequence of behaviours on multiple devices known to be used for an attack and very unusual in normal behaviour. As for 1b, Threat Intelligence may indicate sequences of behaviours that currently indicate a high risk.

* 1l. a device that moves into a physical location that it should not be in.

To detect lateral movement, it might look for:

2a. login attempts (either failed or successful) with the same credentials for multiple devices in a short time; for some applications this might be normal system behaviour, but e.g. only at certain times of day, in which case the security analytics tool could look for a combination of this with 2b below.

* 2b. unusual patterns of use of multiple devices, e.g. similar actions by multiple devices in a short time interval or at an unusual time of day.

2c. statistically unusual behaviour beginning with one device and then copied by others that are geographically or logically close.

2d. privilege escalations moving from one control hierarchy zone to another.

To detect command and control, it might look for

* 3a. attempted or successful outgoing connections to known bad addresses, or which are not on a limited list of outgoing connections allowed by policy (this may also indicate exfiltration or some types of damage).

* 3b. actions by a device that are statistically unusual in past behaviour, or that are not on an approved policy list of actions by that type of device.

To detect exfiltration and damage, it might look for
4a. devices sending out an unusually large volume of data (either all at once, or in small
chunks; either unusually large compared to past behaviour of the device, or compared to
other devices of the same type).
* 4b. sensors giving readings inconsistent with other nearby sensors.
* 4c. indications of damage from environmental sensors near a device.
4d. unusual items on telecom billing logs, or unexpectedly large bills for a device.

Note that these indicators in general do not detect only security issues. Many of them can also
detect misconfigurations and non-malicious malfunctions of IoT devices. Knowing about
these can be valuable to an enterprise, allowing swift remediation of problems and more
accurate information from the IoT system.

4.2 Examples

This section gives five examples of actual attacks on IoT systems, and suggests how similar
attacks might be detected.

Example 1: In 2000, a former employee of a company who had previously installed radio-
controlled SCADA sewage equipment for Maroochy Shire Council in Queensland, Australia
was turned down for a job at the council. In revenge, he accessed the council’s insecure
wireless network from his car on 46 occasions, and made configuration changes to the
sewage control system using radio commands, causing 800,000 litres of raw sewage to spill
into the local environment. (Abrams and Weiss, 2008). The damage to the local environment
was obvious, but it was not clear that it was deliberate until an engineer working late noticed
that when he made configuration changes they were being changed back again (Crawford,
2006).

This attack was detected manually by indicator 1f in Section 4.1 (configuration changes that
are unusually frequent or at an unusual time of day), but a similar attack might have been
detected automatically using this indicator, and 1e (an unusual amount of admin account use
by third-party contractors) would also have been relevant.

Example 2: About 6,000 “keyless” cars and vans were stolen in 2014 in London alone, using
a tool that was originally designed for garages to get into cars after owners had lost their key
fobs. The tool obtains information from the car’s on-board diagnostic port, and uses this
information to program a blank key fob. The on-board diagnostic port can be reached by
secretly jamming the radio signals when the car owner tries to lock the car, or simply by
smashing a window (Killelea, 2015; Metropolitan Police, 2015).

This sort of attack could be detectable by looking for access to an on-board diagnostic port
after a car had been left stationary and unlocked for a while, or after a sensor detected a
smashed window in a locked car. This would be easiest for the telecommunication service
provider to do, as they provide the connectivity to the vehicle. This indicator is one example
of 1k in section 4.1 (a sequence of actions by multiple devices known to be used in an attack
and very rare in normal behaviour) and in the case of a smashed window also involves 4c (detection of damage by an environmental sensor). There might be a further indication of type 3c (actions statistically unusual in past behaviour) or type 1j (a sensor detects unusual behaviour, and then the device’s behaviour changes) if the thief’s driving style is very different from the owner’s – for example, if the thief accelerates away faster than the owner would, in order to get away quickly.

**Example 3:** A cyberattack on the Ukrainian power grid on 23 December 2015 left about 700,000 houses without energy for several hours. The trojan-dropper BlackEnergy was found on the networks of the Ukrainian power company Prykarpattya Oblenergo. This malware can be spread over traditional networks, and has been used in a variety of attacks, but is designed to be capable of infecting SCADA systems (Lipovsky and Cherepanov, 2016). According to the US Homeland Security Department, this malware was used in 2014 on “numerous industrial control systems environments” in the US – but only on the human-machine interfaces, so in 2014 it apparently didn’t cause damage to the control systems themselves [Harris, (2016), paragraphs 7-8].

The US Homeland Security’s Industrial Control Systems Cybersecurity Emergency Response Team had released a signature rule for the detection of BlackEnergy in early 2015, so the detection of BlackEnergy on the power company’s network was a case of 1b (traffic triggering known malware/intrusion signature detection rules). Moreover, BlackEnergy exploits vulnerabilities in internet-connected devices to download malware directly into the control environment (Department of Homeland Security, 2015), so indicator 1c (direct connections between two control hierarchy zones that are not supposed to connect, in particular between the external zone and the cell zone) is also relevant, and might detect similar attacks even if there are no signature rules for them. Finally, the malware downloaded by BlackEnergy in this case made machines unable to boot, which might have been detected by 1g (unusually frequent booting or unsuccessful booting attempts).

**Example 4:** In 23 December 2013 – 6 January 2014, spammers sent messages from over 100,000 IP addresses belonging to IoT devices that they had compromised into becoming part of a botnet (Proofpoint, 2014). (The initial report of this attack claimed that one of these devices was a fridge, but this turned out to be probably mistaken. Most were home routers and NAS, and there were also some connected multi-media centres and television set-top boxes.) The attack guessed that the devices were using default credentials, and once it had gained access to a device it configured it as an email proxy.

Although the botnet was used for spam, botnets can also be used for distributed denial of service attacks (DDoS). Imanuel von Cube (2016) reported a discovery that some Lego robots were infected by a credential-guessing telnet worm with the result that the robots could have been used for DDoS, although he did not report that they were actually used in this way.

A similar attack involving multiple IoT devices within an enterprise network might be detected as the infection spread within the network by using indicator 2a (login attempts for multiple devices with the same credentials in a short time), and possibly also 1d (multiple failed login attempts). When the infected devices sent spam or DDoS traffic was sent it might be detected with indicator 2b (an unusual pattern consisting of similar actions by multiple devices during a short time interval). If the volume of spam / DDoS traffic sent or the amount of attack-related activity per device was large compared to normal device behaviour, indicators 4a (sending out an unusually large volume of data) or 1e (unusual amounts of default account use) would also be triggered.
Use of default credentials is a very common vulnerability in IoT. If an enterprise has IoT devices which do not have a mechanism forcing the change of default credentials, then an indicator such as 2a that can detect some attacks using default credentials will be especially useful, and implementing detection of such an indicator should have priority over other less frequently-used indicators.

Example 5: A wind farm in a very remote place was discoverable over the Web. Some of the communication functionality had been left open. A fraudster managed to program it to send to premium-rate phone numbers. No-one was monitoring the billing, so there would be no alarm until the bill limit – of around a million dollars – was reached (Rogers, 2015).

Detection via the bill limit is a manual detection by indicator 4d (unexpectedly large bills), but such an attack could be automatically detected by the same indicator much earlier. It also might have been detected immediately using indicator 3a (outgoing communications to destinations not on a policy list). Moreover, if only a small number of windmills on the farm were affected, or only one wind farm was affected and the enterprise had multiple wind farms, the attack might have been detected using indicator 1i (a device with very unusual behaviour compared with other devices of the same type). For sectors using large numbers of identical devices, detection of indicator 1i may be especially useful.

5 Analysis of Real IoT Data from Weather Stations

As a proof of concept, an experiment was carried out on some real IoT data, a public data set from datacanvas.org (Data Canvas, 2014-2015) with 24 million entries from 85 weather stations in five cities. The data entries recorded sensor readings for temperature, humidity, light, dust and pollution, together with a timestamp, station ID, latitude and longitude. It was not expected that there would be any security attacks in the data, as there is no motive for anyone to attack a weather station: the idea was to see whether it was possible to detect misconfigurations or malfunctions using some of the starred indicators mentioned in section 4.1.

The indicators considered were part of 1i (a device with behaviour that is statistically very unusual compared to other devices of the same type), the related 4c (sensors giving readings inconsistent with other nearby sensors), and 11 (a device that moves into a physical location that it should not be in). Other starred indicators were unsuitable for this data set either for lack of relevant information, or because of the application; for example, 2b identified unusual weather rather than lateral movements of security attacks.

In more technical detail, first, very common values for each sensor type were removed from the raw data: these included default values given by inoperative sensors. The first 2% of the remaining data was used to determine normalization values, using a lognormal model for each sensor type. Geographical clusters were found using the latitude and longitude values. The variance of normalized values for each sensor type in a geographical cluster was calculated over 10-minute intervals in the remainder of the data, and (type, cluster, time interval) combinations with large variance were investigated. Changes in latitude/longitude values were also investigated, as weather stations should not move.

This analysis revealed multiple issues. Some of these could have been detected by analysing data just from the weather station concerned, but not all of them. Here are five examples of issues that were revealed by the analysis.
Example 1: There was a sudden light reading by one sensor in the middle of the night, brighter than that for full tropical sunlight. This was almost certainly a malfunction, possibly caused by an electricity surge.

Example 2: One dust sensor frequently gave readings of minus 1 particles per 283 ml. This seems to have been an erroneous default value.

Example 3: Figure 1 shows dust sensor readings for two weather stations. They appear to be reflecting the same brief environmental phenomenon. However, of the one weather stations reported its location to be in the Boston area, and the other reported its location to be in London.

![Figure 1: Dust sensor readings for two weather stations. The y-axis is the dust reading, which briefly reaches unusually high values, and the x-axis is time, with units in minutes.](image)

Later, the latitude and longitude readings for the weather station apparently in London changed to (Lat -71.086502, Long 42.342751) - which is in Antarctica. A possible explanation for this can be given by the fact that the location given by swapping these latitude and longitude coordinates, (Lat 42.342751, Long -71.086502), is in Boston. It seems likely that the weather station that apparently jumped from London to Antarctica was in Boston all along. It was given an initial configuration with a location value in London, to be updated with the correct latitude and longitude once these readings became available, but in the updating process the latitude was incorrectly recorded as longitude and vice versa.

Example 4: Figure 2 shows strange behaviour by one malfunctioning pollution sensor. It is one of only two pollution sensors in the data set that give a reading of over 600mV; as can be seen, it gives a reading over 900mV for most of the 2-hour time interval plotted. A possible cause is that the sensor has become choked with dust.
Example 5: A final example is that one weather station travelled 5 km from the research institution where it initially was. This seems more likely to have been caused by a curious researcher checking out sensor readings at a different location than a security issue, as the weather station returned to its origin after three hours. However, theft is a common threat for IoT devices. An enterprise IoT device may be stolen either as an end in itself, or potentially to hamper its sensing abilities so as to make an attack easier to carry out; so the ability to detect devices going walkabout may be very useful.

5 Conclusion

The rise of the Internet of Things, which has inherent security challenges, means that IoT security will be increasingly important for enterprises. There is an opportunity to build a partly-centralized security analytics system that uses the large memory capacity of future hardware to give it capabilities particularly suited to detecting attacks on IoT systems, producing more effective results than traditional network security tools. This article has suggested indicators by which such a system could detect substantial real-life attacks.

Acknowledgements

Thanks to Yolanta Beres, Sagi Schein, Philipp Reinecke, Martin Arlitt and Amip Shah for their input to this article, and particular thanks to Pratyusa Manadhata.

References


Verizon (2015) State of the Market: The Internet of Things 2015. [online] http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf (Accessed 8 August 2016). Note: a suggested tweet on p.2 of the report says that leading adopters of IoT will be “up to 10% more profitable”, which is the opposite of the prediction in the main body of the text (p.4) that they will be “at least 10% more profitable”. From context, the prediction in the main body appears to be the one intended.
