Horizon Scanning Series

The Internet of Things

Cyber Security Risks in IoT Systems and Techniques for their Mitigation

This input paper was prepared by Vijay Varadharajan

Suggested Citation

Varadharajan, V (2019). Cyber Security Risks in IoT Systems and Techniques for their Mitigation. Input paper for the Horizon Scanning Project "The Internet of Things" on behalf of the Australian Council of Learned Academies, www.acola.org.

What cyber security implications may arise from IoT deployment in smart cities? How can risks be mitigated?

1. Smart City and Internet of Things (IoT)

A smart city can be loosely defined as a city connecting physical and information and communications infrastructures together with social and business infrastructures to leverage the collective intelligence of the city [15]. In the provision of services in a smart city, the large-scale deployment of the Internet of Things (IoT) plays a significant role. For instance, IoT introduces new capabilities such as the ability to monitor and manage devices remotely, and then analyze and take actions based on the information received from various real-time data streams. IoT helps to leverage several ubiquitous services in smart cities such as enhancing infrastructures, creating more effective and cost-efficient municipal services, improving transportation services by decreasing road traffic congestion, and improving citizens' safety. It is clear that such smart city services need to be secure and trustworthy as well as scalable and efficient.

Consider an example of IoT enabled solar farm in a smart city. IoT provides the infrastructure to control the positioning of the panels as well as perform acquisition of the physical sensor data such as temperature, humidity, time, angle, and position logs from the solar panels. These sensed data are then transmitted to the cloud where they can be stored and analysed. The data in the cloud can then be made available to other users or applications. For example, a power distributing company can analyse the solar panel logs and find the optimum panel angle respective to sun's position throughout the day. The panels can be remotely programmed to rotate in a particular manner to provide maximum efficiency.

2. IoT Architecture Overview

The IoT infrastructure is not the result of a single novel technology, instead consists of several complementary technical developments providing capabilities that added together, help to bridge the gap between the virtual and physical world. Typically, an IoT device can consist of sensor, actuator, communication infrastructure and a processing unit with some software (firmware). A typical function of an IoT device is to sense data and send it to a remote location or to receive data and perform some limited actions on it. The IoT devices can be small and often resource constrained and typically embedded in other real world objects. The behaviour of the IoT devices are controlled by the applications.

One can think of the IoT architecture consisting of four basic layers namely the Perception Layer, Network Layer, Middleware Layer, and the Application Layer [1]. The Table below shows the components in each of these layers and the associated tasks.

Layer	Components	Tasks
Application Layer	Third Party Application, Websites, Consoles, and Touch panel.	Machine Learning, Business Models, Graphs, and Flow charts.
Service Layer	Vendor Specific Third Party Application	Machine Learning, Processing, Pre-processing, and Real time action.

Network Layer	Nodes, Gateways, Firmware	Device Management, Processing and Secure Routing
Perception Layer	Sensors (Temperature, and Humidity) and Actuators (Motor, and Relays)	Identify, Monitor, Acquisition and Action.

There are different services, networks and protocols involved in these different IoT architecture layers.

Layer Name	Protocol Used
Application Layer	HTTP, CoAP, DDS, AMQP, MQTT, MQTT-SN, XMPP, HTTP REST
Network Layer	MDNS, DNS-SD, RPL, 6LoWPAN, IPv4/IPv6
Perception Layer	LTE-A, EPCGlobal, IEEE 802.15.4, Z-Wave.

3. Security and Privacy Challenges in IoT Systems

One of the biggest security challenges with IoT systems is the substantial increase in the security attack surface giving rise to new threats. This is due to the large-scale deployment and heterogeneity of IoT devices. IoT devices often have different operating systems and work with a variety of networks and associated protocols. The devices can be connected to networks via different providers and can involve wireless as well as mobile networks. IoT devices may use a range of wireless protocols such as Bluetooth, 802.11, WiMAX, Zigbee and UMTS, making them susceptible to a range of security vulnerabilities and threats.

At present, many IoT devices do not have any security functionality, and even the ones that have are often primitive and hence can be easily subjected to attacks. Compromising one of more devices in the infrastructure can lead to proliferation of malware and attacks, potentially leading to the compromise of the whole network system.

For instance, the well-publicized Mirai attack in 2016 compromised a number of IoT devices (such as Internet camera, routers and printers, having default administrative passwords), creating a large IoT botnet to perform distributed denial of service attacks against Internet services. The susceptibility of IoT devices to attacks is further aggravated as the devices become smarter; smarter devices have more functionality which increases the possibilities for attacks. Furthermore, it is just not the external attacks that one needs to be concerned with; insiders in a large organization can both inadvertently or maliciously expose the infrastructure to attacks.

Another major security challenge with the deployment of IoT devices in smart city applications is concerned with the secure access to devices. As many of these devices have limited computational resources, there is a need for novel IoT security solutions that are light weight and can achieve fined-grained access control with efficient policy management for billions of devices in a heterogeneous environment. Smart city applications such as monitoring the health of buildings or the environment for water leakage involve accessing data from a number of different types of IoT devices. The issue of authorized access to data is critical as the data is used to make sensitive decisions. The authorization service needs to be secure and efficient and needs to be able to deal with large scale heterogeneous IoT devices.

Identification and authentication of IoT devices is often a pre-requisite to authorized access. This involves secure provisioning of IoT devices to ensure that appropriate registration and authentication of IoT devices are achieved at the set up time. Once again, there is a need for lightweight protocols and key management schemes when it comes to large scale deployment of resource constrained IoT devices.

Secure identification of IoT devices plays a key role in the establishment of trust. Trust is a major security challenge when it comes to large scale deployment of IoT devices in smart city applications. Here the fundamental question is what it means to trust a device, and more specifically, what functionalities are required in a device to achieve trust, and how can trust on IoT devices be evaluated and managed in distributed IoT infrastructures. The issue of trust associated with a device is not just dependent on its identity (or its identifier) but also on its behaviour over a period of time. It is necessary to take into account both static and dynamic characteristics of a device in evaluating trust. The IoT trust issue becomes even more important when the devices are mobile, moving from one jurisdiction to another, where they are not known in advance.

Another security risk that arises when collecting data from an IoT environment is concerned with the attacker inserting or manipulating data from the IoT device, which are being used by decision making applications. For instance, if machine learning algorithms are being trained at the backend using the data collected from the IoT devices, then tampering of data can fool or cheat the machine learning algorithms used in the decision making. Such attacks are referred to as data poisoning attacks in the machine learning context, which can enable the attackers to affect adversely the overall performance, or cause targeted misclassification as well as insert backdoors and Trojans.

A related issue when it comes to data from IoT devices is that of data breaches. The data breaches involving IoT devices can have a serious impact on the end users, because the data may not only be sensitive but also linked with personal devices, such as their door locks, cars, baby monitors, security cameras or even healthcare devices such as heart pacemakers. Such information, in the hands of a cybercriminal, can have a direct devastating impact on the users. Attacks on medical IoT devices such as heart pacemakers and implants can enable an attacker to change settings leading to adverse effects, potentially even death. Attacks on smart electricity infrastructures can lead to malicious attackers stealing electricity or even potentially causing blackouts to large parts of a city. Attacks on smart vehicles (such as a smart car) can lead to loss of control, causing accidents and serious injury.

Often the preferred solution for dealing with software vulnerabilities is to regularly patch them; however, with IoT devices, device manufacturers may be unable to do this, as users often do not to register their devices with the manufacturers. IoT users may even forget unattended IoT devices previously installed in their networks, leaving them with outdated software. Furthermore, due to small cost/profit margin associated with the consumer IoT devices, it may not be worthwhile for the device manufacturers to provide the required software patches in a timely and regular manner. Hence security solutions will need to cater for an ecosystem where IoT devices with unpatched vulnerabilities will often be present in the network infrastructure, co-existing with other devices during the device lifetime. This means that a different approach to deal with attacks and patch management in IoT systems is required.

4. Security Attacks in IoT Systems

Based on the risks identified above, let us categorize the attacks in IoT systems into five areas, namely communications, device/services, users, mobility and integration of resources. Note that, we use the term 'services' in a low level sense, whereas the term 'integration of resources' covers applications which draw on multiple devices and services to meet end-user requirements. Communications category covers the possible attacks in wired and wireless medium (e.g. routing channels and data transmission etc.). Device/services category encompasses physical IoT devices and their associated low-level services (e.g. battery, memory, data provision, etc.). User category covers attacks such as privacy and identity disclosures of IoT users. Mobility category includes attacks on location such as tracking, and integration of resources category includes attacks arising from composition or cascading of diverse services.

- *Communications*: Communication lies at the heart of the IoT, with the connections between users and devices. Attacks on IoT communications can be broadly categorised into routing attacks, active data attacks, passive data attacks and flooding. In a routing attack, attackers target routing protocols and network traffic to either disrupt the flow of information or redirect the routing path to an unsecure destination. They neither alter the contents of nor attempt to gain information from the transmitted packets. Common forms of these attacks include blackhole, wormhole, and pharming. Active data attacks alter or delete information by targeting valid data packets directly rather than via subverting network routing. Examples of these attacks include channel jamming and various forms of data tampering (modification, manipulation etc.) which may or may not result in valid packets. Active data attacks may target the payload, header or both of a packet. Passive data attacks attempt to gain information without altering the contents of communications. Examples here include eavesdropping and traffic analysis. Examples of flooding attacks include SYN flooding and denial of service (DoS) attacks. DoS attacks are of particular concern for IoT systems due to the resource-constrained nature of many IoT devices. It may only take a limited amount of bogus traffic before an IoT device is compromised by resource and bandwidth consumption.
- *Device/Services:* Threats on the devices and services of an IoT system can be broadly categorised into physical attacks, device subversion attack, and device data access and device degradation. The vast majority of IoT devices operate in open environments, where common security issues include device damage and disconnection. For instance, an attacker can physically disconnect an IoT device (e.g. a computer, mobile phone, even an air-conditioner) from the Internet, damage it beyond the point of serviceability or even destroy it completely. In a device subversion attack, an attacker assumes full or partial control over a device. This can then be used to actively cause the device to either cease functioning or to provide incorrect outputs. Taking control over IoT devices can be divided into two categories i.e. controlling a single device and controlling many devices. In the former case, an attacker may, for example, penetrate a user's home network (either physically or virtually) and take control of a single device (e.g. smart LEDs, refrigerator etc.). This can lead to its functionality being unavailable, or even restricted or misused. The low power of IoT devices make them more vulnerable due in part to the minimal (or non-existent) security protections that are embedded in such devices. Moreover, these devices are often incapable of updating to the latest software and security patches even when they have embedded security functionality. In the latter case, an attacker may assume control of many IoT devices and manipulate services, e.g. an attacker may disrupt a traffic monitoring service by controlling large numbers of the underlying sensors. In a device data access attack, an attacker infects one or more IoT devices which are then used by the attackers to perform malevolent activities on sensitive data without the user's knowledge. For instance, stealing medical information by gaining unauthorised access to a patient's mobile device. The device appears to be functioning normally, but the data held by the device is available to the attacker. Device degradation is a form of DoS attack intended to prevent access

to a service by attacking the functioning of the devices themselves rather than the network's ability to handle traffic. In a typical DoS attack, the service is over-whelmed by having to process bogus traffic but the individual nodes are unharmed. With their limited memory space and battery capacity, IoT devices can be attacked by memory exhaustion and battery corruption. Thus, a device degradation attack on these resource-constrained devices in mass-scale can potentially collapse the entire system's operations.

- *Users:* We divide potential security attacks associated with users into four broad categories, namely trust, data confidentiality, identity management and behavioural threats. With the potential scale of the IoT, trust is an even more pressing issue than is traditionally the case. Interactions may be fleeting and devices will interact with a high number of previously unknown other devices. Trust related attacks include self- promoting (a malicious device providing good recommendation for itself), bad mouthing (an attacker providing bad recommendation against a good device) and good mouthing (bad devices providing good recommendations for other compromised devices) attacks. The potential utility of the IoT lies in the richness of the data that it contains. This may include extremely sensitive user data, e.g. age, address and medical data. A user's privacy can be breached by any attack that accesses the personal information. Attackers may manipulate or disclose such data or use it to impersonate the user. User impersonation in the IoT is a critical issue due to the combination of heterogeneous data sources coming from various IoT devices, contexts and locations. This can be done via identity spoofing, where attackers gain unauthorised access to IoT systems.
  With the IoT's scale and heterogeneity and a user desire for privacy, it is likely that users will maintain multiple identities. This also multiplies the normal vulnerabilities that attackers can exploit, due to the range of interactions of the systems supporting these identities. In IoT systems, management of identities is a major concern for authenticating and authorising a legitimate device (e.g. who and what is connecting to), where the service provider and the service consumer may both try to keep their identities hidden. Attackers may exploit the heterogeneous and multi-domain nature of the systems supporting identity management in the IoT to subvert these systems. In personal and social domains, users' malicious or selfish behaviours can also be used to create attacks through social engineering. For example, by downloading malicious software or being tricked into revealing private information through phishing attacks.

- *Mobility*: We divide the various mobility related security issues into three categories i.e. dynamic topology/infrastructure, tracking and location privacy, and multiple jurisdictions. As noted above, some threats can be viewed from multiple perspectives, for example users' mobility may increase the possibility of active and passive data attacks (communications) and location tracking (mobility). In the IoT, nodes do not necessarily need to connect over the Internet; they can connect via any network e.g.
  - Wireless Sensor Network (WSN), Personal Area Network (PAN) or Wireless Local Area Network (WLAN). In such an environment, when users and devices move (i.e. joining and leaving the network), the network topology is dynamically modified. This could generate security challenges of interdependencies (e.g. attacks on networked-car, electronic medical devices and power stations) for the end-users. This could further evolve into 'sinkhole' attacks by updating the network topology by the attackers and gaining illegal access to a user's data in a real-time situation. In tracking and location privacy, location-based information (e.g. user's current position or daily routine) in an IoT system could be inherently vulnerable and a possible target for attackers to breach personal privacy.
  - It may also possible that several disjointed networks of things join to form inter-domain collaborations and co-ordinations. It is likely that such collaborations will use heterogeneous technology. Attackers may seek to exploit any mismatch in policy

settings, identity management or security technologies. For instance, in a traffic accident, police officers can communicate with emergency services to coordinate well-being of the driver or passengers. However, the management of this information over the jurisdictions possess several challenges of data privacy.

- *Integration of Resources*: In the IoT systems, from data collection to data processing, storage and usage are highly dependent on diverse infrastructures. We divide the attacks in this area into three broad categories i.e. cross domain administration, cascading resources and interoperability. The components which co-operate and interact to provide end-user results may be controlled by multiple different domains. Even when control resides within a single domain, there are challenges in ensuring security at each stage of the composition. In such cases, attackers may seek to exploit any mismatch in policy settings, identity management or security technologies. End-user applications in the IoT systems can potentially draw upon a vast range of devices and services. Any security breach at the low level may cascade up and affect higher level services and applications that depend on the compromised component. For instance, an attacker can penetrate a user's mobile network and make a modification to their home automation system and compromise a motion sensor. If the system is set to open windows or doors when motion is detected, the attacker may be able to gain access to the building. As another example, an attacker may introduce malicious code into a poorly protected device. The code is then passed up as data through applications and used to infect user devices. Furthermore, the large volume of data can create threats to the user's privacy and information security. In such attacks, the attacker gathers a large amount of information (of service, user and resources) and can perform automated data- mining without being noticed by the user and service provider. Interoperability relates to attacks based on the need for multiple systems to work together and the ability of attackers to exploit any potential issues in an IoT system can include cloud computing, fog computing, social networks, mobile computing and industrial networks. For instance, in a smart healthcare system, a patient's data (e.g. blood pressure) is collected, analysed and transferred to the patients by the doctors, which may depend upon several of these dynamic networks. Therefore, in any of these stages' attackers can breach patient's personal (and sensitive) information by penetrating any of these networks between the infrastructures.

5. Security Techniques for Mitigation of Attacks in IoT Systems

An effective approach to securing IoT systems requires not only efficient attack detection and prevention, but also containment and recovery from attacks.

Although the security techniques that can be deployed to mitigate the attacks fall under the traditional categories of authentication, authorisation, secure communication and trust management, these techniques need to be addressed within the *specific context of IoT* and integrated with different services and protocols in the IoT architecture. This can pose some significant challenges in practice. Let us briefly look at some of these challenges.

- Identity and Authentication: Identity is a fundamental notion which represents "who the entity or device is" it is. Identity is important when it comes to determining what a particular device can access and who can access that device. It is also necessary when it comes to detecting which device has become malicious or attacking the system, and how to provide security software (e.g. patches) to counteract the malicious device. There are various representations of identity, such as using identifiers and/or using attributes. Authentication provides reliable verification of the identity of the device. In the case of large scale IoT systems with millions of IoT devices and sensors, a major practical challenge is how to achieve authentication of IoT devices in an efficient manner using lightweight security protocols, as the devices are computationally constrained. Another major challenge in practice is how to achieve secure registration of IoT

devices in large scale at the set up time, which requires protocols for secure provisioning of IoT devices. As indicated earlier with consumer IoT devices, lack of suitable registration procedures can potentially lead to a significant increase in the attack surface.

- Secure Authorization: The main challenge in the design of secure authorization service in IoT systems arises not only due to the large scale but also due to the different jurisdictions the IoT devices reside in (and the associated security policies). For instance, it is not realistic to assume in dynamic IoT systems that the identities of all users who will need access are known beforehand. For example, a retail shop may not know the identities of its customers until they walk through the door. Hence the design of authorization service in IoT systems needs to be not only light weight but also have the flexibility to deal with dynamic situations with fine-grained policy decisions capabilities and a decentralised architecture for real-time decision making to achieve the desired performance in distributed environments spanning multiple jurisdictions.
- Secure Communication: Secure communication techniques typically involve the use of cryptographic mechanisms for the provision of services such as data confidentiality, data integrity, non-repudiation as well as data origin authentication. The aspects addressed by these security services include: who is able to view the data from an IoT device (data confidentiality), how does the receiver ensure that the data from the sender has not been tampered (data integrity), how can one prove that a particular device did send a specific data (non-repudiation) and is the data coming from the claimed device (data origin authentication).
  In terms of practical challenges associated with these services, they arise due to the resource restrained nature of IoT devices as well as due to large scale. Cryptographic algorithms can involve sophisticated computations requiring computational power and adequate memory, which may be difficult to achieve in resource restrained IoT sensors and devices. Crypto based security services require management of suitable attributes such as keys. In large scale IoT systems with multiple jurisdictions, key management can pose practical challenges, especially if devices are constantly added and removed in a dynamic manner.
- Trust Management: With IoT systems involving many devices, the services provided to the end users and applications often relies on the data from these devices and cooperation between them. The compromise of one or more devices can have serious consequences on the service being provided. For instance, if an attacker succeeds to compromise or add one or more devices in the network, the attacker can provide fake or erroneous information, which can subsequently affect the cooperation of nodes, data treatment and the service provided to the end user. Thus, the credibility and reputation of devices is key to ensuring accurate and reliable network service delivery. There are two classes of techniques, namely hard trust and soft trust, which can be used to achieve trust management. Hard trust techniques involve the use of mechanisms that monitor and evaluate the state of a device, thereby helping to assess whether a device has been compromised. Soft trust techniques involve the use of reputation mechanisms to assess the behaviour of a device based on its past actions. The combination of hard and soft trust mechanisms can lead to suitable trust management schemes especially for large IoT systems that are dynamic.
- Privacy Management: Privacy management in the context of IoT systems primarily address the data privacy aspects. That is, certain data from IoT devices should not be revealed to unauthorised users and more importantly, the level of control that a user has on his or her own data being collected by the IoT devices. Consider for instance smart buildings or smart retail spaces in the city that track individuals' location and activity to provide customized experience based on users' context. Such services could include customized heating/air conditioning (HVAC) control based on user's preference, services to help locate nearby resources, and/or deliver customized coupons/incentives in the retail setting. Capturing fine-grained sensor data besides enabling customized services, also raises significant concerns about building owners

being empowered to use the data captured to infer properties such as personal habits of individuals, e.g., smoker/non-smoker, gender, religious beliefs, etc. – properties that individuals may not be comfortable sharing without explicit consent. To address such concerns, there should be mechanisms for informing the users about the policies related to collection of data in smart spaces as well as mechanisms for obtaining user consent. Such mechanisms should be designed to protect users from malicious IoT spaces that may capture data other than what it has been agreed to in the policy. They can help to empower the users to retroactively attest policy compliance by the IoT space.

6. Concluding Remarks

IoT is one of the fundamental technologies' businesses are using for digital transformation efforts. Each one of us now manages multiple IoT devices. Increasingly the expectation is that we will configure securely the variety of devices from a connected fridge, smart TV to watch to meet our own specific requirements. As the deployment of IoT devices in smart systems continues to increase in different sectors such as smart cities, transportation, agriculture and healthcare, there is a need to ensure that the devices meet certain minimum security standards. For instance, in healthcare, with the increase in the use of devices such as medical implants, there is a greater reliance on the part of the healthcare practitioners on the manufacturers to guarantee security. Hence it is critical that there are proper regulatory guidelines and even legislation to ensure that every IoT device (in particular in sectors such as healthcare) complies with a set of minimum security standards.

The US Congress has recently passed the Internet of Things (IoT) Cybersecurity Improvement Act (in 2019)
[2] which prescribes that government agencies can only procure and use IoT devices that adhere to a minimum set of security standards. From the Australian perspective, it would be useful to introduce guidelines (and regulations) not only with respect to secure government use of IoT technology but also expanding it further to include business and consumer IoT devices.

Furthermore, regulatory process will need to include some form of independent penetration testing of products that contain software as part of the approval process (not solely relying on the manufacturers' guarantees). However, this is not that simple. In the world of IoT systems, inevitably there will be issues around the interaction between devices and systems. It will not be enough for the manufacturers of individual products such as a car's emergency braking or stability control to maintain and patch their components independently. It will not be sufficient to certify components; we will have to certify and monitor whole systems, which can pose some formidable challenges.

References

1. L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial Informatics, Vol. 10, No. 4, pp. 2233-2243, 2014.
2. US Congress, Internet of Things Cyber Security Improvement Act of 2019, Mar 2019.

Professor Vijay Varadharajan FIEE, FIEAust, FACS, FBCS, FIMA, FIETE
Global Innovation Chair Professor in Cyber Security
Advanced Cyber Security Engineering Research
Centre (ACSRC) The University of Newcastle
Australia
Email: vijay.varadharajan@newcastle.edu.au
https://www.newcastle.edu.au/research-and-innovation/centre/advanced-cyber-security-research- centre/people/professor-vijay-varadharajan-biography