IoT-related risk: prevention and management

Vidar Hedtjärn Swaling

1. Introduction

Internet of Things (IoT) is a concept that describes how more and more objects are being designed with the capability to be connected to internet and other networks, both for private and industrial use. Being connected can provide numerous advantages, but also entails many challenges. For example, such solutions often have a low level of security and are inadequately protected against unauthorised use. The incentive to sell IoT devices in large volumes at relatively low acquisition cost also limits the possibilities for ensuring good security.

Attacks against IoT devices can result in consequences at the societal level, since the proper functioning of all critical infrastructure sectors depends on both information technology (IT) and control systems. Such systems are often connected to internet and rely at least in part on IoT products, which exposes them to the risk of cyberattack.

IoT is developing extremely rapidly and there is a need to acquire a much deeper understanding of the complex of problems that accompany it. This memo summarises the risks associated with the advances in IoT and provides recommendations concerning a procedure for dealing with them.[1]

***Threat** is defined as the potential for an undesired event with negative consequences.*

***Risk** is the combination of the probability that a given threat is accomplished and its resultant consequences. Risk can be said to be a measure of the expected cost of doing nothing, and is thus the natural basis for developing strategies.*

2. What is IoT?

The example of the interactive or communicative refrigerator is used so often that for many it may be the very symbol of IoT. Other frequently highlighted applications are self-driving cars and various healthcare solutions. Since there probably is not any ultimate limit for how and in what context IoT can be implemented, at the same time as progress is continually being made, it is more important to understand what it is that makes something an IoT item than to be able to present numerous examples of them. One of the more generally applicable and unambiguous definitions can be found in a publication by the U.S. Department of Homeland Security, which describes IoT as, "*the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the internet) via interoperable protocols, often built into embedded systems.*"

3. Architecture

To be able to discuss the risks of IoT, it is fundamental to consider its architecture. This can be done in a variety of ways, but often one speaks of three layers. In the **perception layer**, data about the surrounding environment is collected with the help of sensors, cameras, GPS, laser scanners, and RFID tags, among other things. The **transmission layer** is where data is exchanged between the perception and application layers and processed. In the **application layer**, the information received is processed and commands are issued to the physical devices. This is where the connected devices are controlled.

4. Analytical framework

This memo is based on a study in the form of a literature review that included both academic articles as well as publications from the industry and relevant organisations such as NIST and ENISA. The study had its point of departure in the risks identified in the review. The analytical framework proceeds from a generic risk analysis model that describes the following logic:

- Considering something to be a risk requires a consequence with regard to something *worth protecting*, an *asset.*
- Risk also emerges in the presence of a *threat* and an *attack vector,* that is, a means by which the threat can be accomplished.
- The potential for accomplishing an antagonistic threat to a technical system depends on the system's inherent vulnerabilities.

In other words, the most interesting consequences are those that arise when a threat, by means of an attack vector combined with a vulnerability, affects any of the protected assets. Table 1 describes the elements of the framework's model and the categorisation that the analysis is based on.

[1] This memo summarizes the main reasoning and conclusions of the FOI report, "IoT-relaterade risker och strategier" [IoT-related risks and strategies] (Swaling & Johansson, 2016). The study was conducted by the Swedish Defence Research Agency (FOI), on behalf of the Swedish Civil Contingencies Agency (MSB), at the National Centre for Security in Control Systems for Critical Infrastructure (NCS3).

FOI Memo 6503
Project number: E13631
Approved by: Karin Mossberg Sonnek

October 2018

MSB Swedish Civil Contingencies Agency

FOI

Table 1: The analytical framework and its components, derived from risk analysis methodology, and the categories into which its components are broken down, or that are used in analysing them.

Components of the model	Categorisation	Comments
Protection values	Confidentiality	Categorised according to components in the CIA triad.
	Integrity	
	Availability	
Vulnerabilities	Complexity	Categorised according to general characteristics of the influence of risk.
	Design requirements	
	Exposure	
Attack vectors	Perception layer	Categorised according to the different layers in the architectural model.
	Transmission layer	
	Application layer	
Risks	Confidentiality	Categorised according to components in the CIA triad.
	Integrity	
	Availability	
Strategies	Manufacturers and integrators	Categorised according to types of actors.
	System developers	
	Importers and distributers	
	System owners and users	
	Government authorities	

5. Vulnerabilities

If a risk is to arise, there must be a threat and a way for the threat to be accomplished. The possibility that an antagonistic threat to a technical system will be accomplished depends in part on the attack vector (the way the system is attacked), and in part on the system's inherent vulnerabilities and flaws, as well as its exposure. Identifying and eliminating vulnerabilities is therefore a major part of working with information security. As far as IoT as a technology is concerned, it is not possible to point to any specific, concrete vulnerabilities. On the other hand, general characteristics of IoT devices can be identified, which can in turn lead to vulnerabilities.

Complexity: The number of connected IoT devices, along with their associated risks, is going to increase rapidly in the next few years. Their heterogeneity is also going to increase, which implies compatibility challenges and makes it more difficult to uphold the system expertise that is necessary to retain the system's security.

Design requirements: IoT devices are often small and battery-driven, so that access to electricity will thus be a strongly limiting factor. They also generally have small processor power and memory compared to conventional network devices, which makes it difficult to apply adequate security and anonymization solutions. IoT devices are not often designed with security in mind, which not only means that they may contain numerous vulnerabilities, but also that it may not always be possible to "patch" those software errors, retroactively, that is, to correct retroactively any software errors that have been discovered.

Exposure: The components that comprise an IoT network may be located in unguarded places and also may "come and go," which makes physical protection difficult. Combined with the fact that IoT is characterised by communication over several different protocols, weak (often factory-installed) passwords, and devices that in many cases are never turned off, traditional IT security solutions are inadequate. IoT is going to be carried by us and surround us and collect data without our permission, often without our being aware of it. Factory-installed passwords, which in practice are intended to protect information, are often known or simple to break, and are seldom changed by the user.

6. Attack Vectors

In table 2 examples of possible attacks are presented in accordance with the architectural model.

Table 2: Overview of IoT-related attacks and attack vectors.

Attacks against	Attack vectors
Perception layer Attacks in the perception layer direct themselves against computing nodes, RFID tags, directly against the communication or against edge computing.	Hardware trojans Non-network side-channel attacks Invasive attacks and hardware tampering Node replication and tag cloning Denial of Service (DoS) Injecting fraudulent packages Integrity attacks against machine-learning Jamming
Transmission layer Attacks in the transmission layer often involve some form of data leakage. An attacker can capture a message, modify and then forward it, or else take advantage of remote access in a network with many connected network nodes to generate overloading.	Loops Wormhole Sinkhole Jamming Denial of Service (DoS) Eavesdropping Passive monitoring Identity theft Injecting false information
Application layer Large quantities of user information are collected in this layer, so that attacks here can result in damaged data and information arriving in the wrong hands.	Buffer overflow Malicious code Information fusion Phishing Denial of Service (DoS) Social engineering

7. Risks

The assessment of the risks associated with IoT was conducted according to the CIA model, beginning with the consequences that jeopardise one or more protection values: *confidentiality, integrity,* and *availability.* Traditionally, IT security has been very much focused on confidentiality. It has been argued, however, that integrity and availability will become more important with regard to IoT.

With regard to *confidentiality,* the risks involve information ending up in the wrong hands. This may mean information that allows access to technical systems, personal data, or corporate secrets. Information theft may be a first move in an attack that results in information that is changed or made inaccessible, or to disruption or destruction of hardware or processors. Via eavesdropping or phishing, for example, unauthorised persons can obtain access to such information as user names, encryption keys, and passwords. With the help of this information, an attacker can infiltrate a computer system and carry out several different kinds of attacks, everything from changing or deleting information to disseminating damaging code. Persons with important social positions can be exposed to targeted attacks that among other things take advantage of IoT devices, including computers, smartphones, and smartwatches. These types of attacks are most often conducted with the help of sophisticated social manipulation combined with technical attack. The increasing use of IoT devices within companies and government departments also creates new opportunities for example, for industrial espionage and intelligence-gathering.

Risks with regard to *integrity* imply that important information is manipulated in unauthorised ways. The attacker can penetrate a system to modify its function, which for IoT devices means that the system is changed so that it functions differently than it was intended to. The consequence of attacks on data and code is that trust in the system is damaged. Using a *botnet,* an attacker can obtain large quantities of computing power. The attack occurs secretly and most often the user doesn't even notice. The bot spreads itself on internet by searching for vulnerable and unprotected computers to infect. IoT devices are often easy targets, since they often have factory-installed passwords, are difficult or impossible to update and are running continuously. Botnets can circumvent spam and overload filters and incur massive attacks that can create serious access problems and strike critical systems.

Risks involving availability imply that important information or systems are in practice rendered inaccessible for authorised users. Typically, a botnet is used for overload attacks, *DoD* or *DDoS attacks*, or in blackmail attacks so-called *ransomware.* Just as in attacks against system integrity, attacks on availability usually begin with some form of initial trespass of confidentiality to recruit a botnet, or for infiltrating the computer or system that is to be taken hostage.

8. Strategies

There is a wide range of measures that manufacturers and integrators can take to increase the security of their products. An important principle is security by design; this means that in the design phase security measures are already being applied. Such measures can involve support for encryption and anonymity of the hardware, trustworthy security updates of software and password protection requirements. It is also important that the software has been designed to a certain degree of tolerance against disruptions or errors in other devices, or to disturbances in connections to internet and various cloud services. In order to limit the attack surface, the functionality of IoT devices can be restricted so that they can only perform what they were intended for, without unnecessary peripheral functions. The devices must also be delivered with strong, default password protection. Instead of supplying a factory-installed standard password that is so weak that the user will have to replace it with a stronger one, products can be delivered with a unique and secure password that the user can intentionally change, as required.

On the system developer side, it is important that a security mindset suffuses all steps in the process, including the choice of platforms, programme language, and tools. If open source code is used, it is important to choose software that is continually updated and in a version where known security flaws have been fixed. Developers should also have a lifecycle strategy for the system and communicate reasonable expectations to both manufacturers and users. This includes informing about the risks involved in using the solution past the date of its supported lifetime.

Importers and sellers can demand that IoT products maintain an acceptable level of security. Distributors should also provide users with information about the purpose of various network connections. All connections should be made consciously and with a knowledge of the risks that being connected carries with it. Connecting directly with internet should not be necessary for critical functions in an IoT device, especially not in industrial contexts.

Even if attention to security has been paid in the design phase, many flaws and vulnerabilities are not going to be discovered until the equipment has come into use. As a starting point, IoT equipment must be installed in a secure way. If it is also placed in a public place or an unmonitored space, then the ability to physically manipulate it must be minimised. Through security updates, surveillance, and maintenance, such vulnerabilities can be managed, and thereby limit the potential consequences of an attack. Devices should not be connected to internet unnecessarily, either. Instead, it may suffice if devices can communicate locally, or, alternatively, that they don't communicate at all.

Measures must also be taken on the more overarching level of government authorities and branch organisations, for example through joint activities among actors, and common policies and standards, as well as compilations of reports on vulnerabilities. Awareness-raising measures may also need to be directed at consumers, to increase their knowledge of how the risks with IoT can be minimised. These actors should also work for stronger incentives for other actors to contribute to increasing the security of IoT. It is today often unclear who is responsible for the security of a certain product or system. The cost of inadequate security is seldom borne by those who have the best possibilities to increase security. Mechanisms that can both increase security and support path-breaking innovations include, for example, indemnity liability, cyber risk insurance, and voluntary certification, as well as laws and regulations, in general.

9. What can MSB do?

The strategies mentioned above indicate that, as a government authority, MSB should act by:

1. Striving to attain risk management that directs preventative efforts against:
   a. vulnerabilities such as poor password management as well as physical exposure;
   b. information theft and other breaches of confidentiality, since these may be the first steps in an attack sequence that in the worst case threatens critical societal functions;
2. Recommending a conservative attitude, in terms of "security by design", so that products are delivered with secure passwords, and that units should not be connected unnecessarily;
3. Prioritising ordinary IT and ICS security work, because it is in these domains that the relevant consequences are manifested;
4. Striving for transparency within IoT, where the purpose of being connected is communicated, and where information about incidents and vulnerabilities is shared, without jeopardising commercial incentives.

Reference

Swaling, V. H., Johansson, J. (2018), *NCS3 Studie – IoT-relaterade risker och strategier – Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem*, ISSN 1650-1942, FOI-R—4591—SE, MSB 2017-1554.