Internet of Things and Alarm Systems: From the Perspective of Security

Santosh Sharman
Kiwa, Apeldoorn, Netherlands

Abstract

At this point, it's a mere obvious observation that the increasing digitalization of our world will, and is, stretch(ing) its tentacles to most if not all aspects of our lives. Meaning, all current forms of technology at our service will be enhanced and evolved by utilizing the possibilities digitalisation offers. In turn, this means that these possibilities need to be anticipated and exploited efficiently. Moreover, the previously mentioned tentacles all need to be addressed adequately to keep all the different challenges such at bay. One of the main challenges that needs constant and relentless attention is (cyber)security. On an abstract level cybersecurity of IoT products (and cybersecurity in general for that matter) is dependent on the balance of technology, processes and (human) interactions. These three pillars can be found back in in one way or another at different levels in the Internet of Things (IoT). For alarm systems the paradigm of the internet of things will undoubtedly be important as well. The alarm chain will and is already making use of digital possibilities such as mobile and web applications for enhanced functionality. This results in a complex chain of entities which narrowly work together to deliver the functionalities that are expected from modern alarm systems.

This paper is by no means an in-depth technical elaboration on digital fire detection and smoke alarm systems. On the contrary it intends to paint of the so called "helicopter view" of the general architecture involved in data driven alarm systems or IoT alarm systems. This maps the important stakeholders and entities that need to be addressed if standardization, testing, certification and inspection were to be performed. First the general architecture is elaborated on. After that a few challenges, varying in type and degree, that will arise are addressed to create context to accentuate the task that is at hand for the certification and standardization world to tackle the challenges of the internet of things.

Keywords: Internet of Things, IoT, chain, data, digitalisation

General Architecture

The architecture consists of different parts with each differing in role, complexity, types of technologies used and importance. Every part is involved in one or more processes. These processes are more often than not part of larger processes. Additionally, in these processes interactions made by us humans come in the mix which complicate and add extra dimension creating an amalgamation of processes, technology and interactions. These three are the pillars on which IoT rests and need to be considered in anything that has to do with solving the challenges of the IoT.

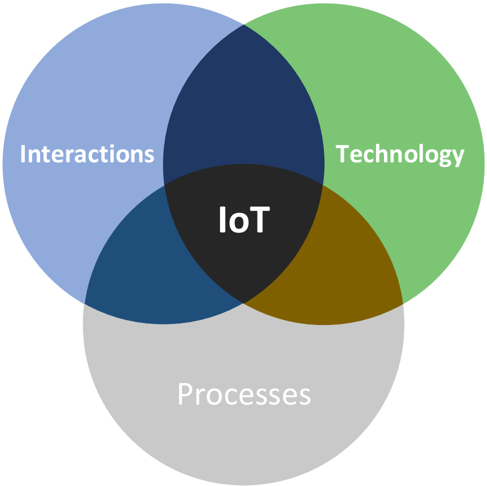

Figure 1. The three main pillars of the security of Internet of Things.

- (Human) Interactions: Human beings interact with the IoT systems. This can either be an end-user, an administrator, a developer, an independent supervisor etc. Point being, different interactions are made with the systems depending on whom is performing the actions. These interactions have their impact and create room for vulnerabilities to creep in. For example: Leaving the computer unlocked while fetching a cup of water.

- Technology: Technology is the cause of the severe advancement of our world regarding industries, day to day life, transport etc. It is a broad term but technology covers, among other things, every single standalone technology that is part of the IoT. There are various types of technologies involved which also differ in complexity, role and importance. Every type of technology requires a different approach and has its own hassles and challenges. Every type of technology also offers its own type of opportunities and possibilities.

Some examples of different technologies are: radio technology, encryption technology and user interface logistics.

- Processes: Interactions and Technologies are combined and create elaborate processes. The processes are build-up of small steps that have to be taken in particular orders, to ultimately offer (smart) services or functionality as an output to end-users. Some steps are sequential while some happen simultaneously. Overall, processes are made up of a mix of both sequential and simultaneous steps. Some processes are loops while other processes have a beginning and an end. Receiving and acting upon an alarm message, continuous monitoring of suspicious activity by sensors and updating software on edge devices are some examples that could come to mind for processes.

Generally speaking, digitalization has data utilization at its core and one of its goals is delivering efficient functionality. The functionality is delivered by a chain of entities, also called an ecosystem of entities, that work together. The data which is at the core of digitalization is either stored, manipulated, transported or interacted with depending on which part of the chain is being addressed. These are the driving forces behind the IoT and its different applications, which in our case are alarm systems. The entities that make up the chain are each different and can be anything from a simple sensor to a person viewing a dashboard with graphs of information. Still however, regardless of the difference between each single entity they all are either connected directly or indirectly working in unison which translates itself into the combination of processes, technology and human interactions which in their respective turn allow for smarter and more efficient services.

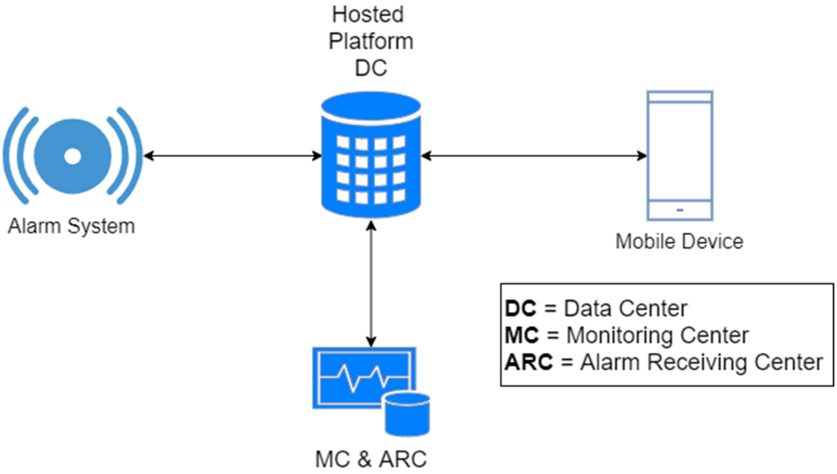

Figure 2. Abstract overview of some important entities involved in an alarm system that is accessible and operable through a mobile application.

Regardless of which type of IoT alarm system is being looked at, the general architecture remains similar. Using figure 3 as a reference, the part of the alarm system which is physical installed at a location (e.g. camera system in the building) is connected through a wireless connection to the internet which is the medium through which it is connected to “the rest of the world”. The hosted platform data centre is through which all the data flows. This can be considered a storage where all types are stored in orderly an orderly manner. Here the data comes in, stored according to a certain type of structure and goes out again. Through the datacentre all other entities such as the mobile device and the Monitoring and Alarm Receiving centre get their data to fuel their own functionality.

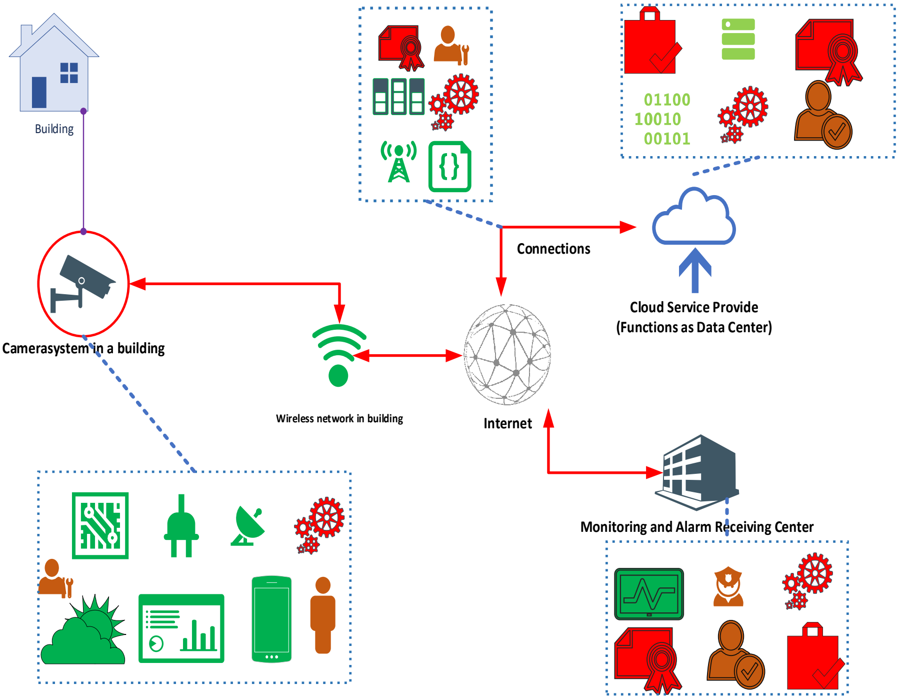
Building
01100
10010
00101
Connections
Cloud Service Provide
(Functions as Data Center)
Camerasystem in a building
Wireless network in building
Internet
Monitoring and Alarm Receiving Center

Figure 3. A more elaborate architecture of a surveillance system. In this figure connections are red arrows and the blue dotted boxes detail the different entities working together and are part of a part of a “larger” entity. Certificates, weather, certified personnel, processes, data etc. can be seen.

To create context more closely consider the example in Figure 3. In this figure a surveillance system is installed in a building. This system is connected to the internet and can be accessed and operated through the internet by the end-user in the same manner as can be seen in Figure 2.

Figure 3 gives insight in how complex and multi-layered a simple chain, that provides functionality as expected from the internet of things, is. Every part in Figure 3 is fuelled by several processes, technologies and interactions of persons. Not all entities are depicted in this simplified example. However, the following entities are all somehow involved in the chain and ecosystem of technology, processes and interactions of alarm systems that utilize the internet of things:

- Radio Technology
- Weather proof hardware
- Power supply
- Encrypted connections
- Quality systems
- Electronics
- Business Processes
- Technical Processes
- Independent Supervisory Parties
- Mobile Devices
- Data
- Algorithms
- Privacy preserving processes
- Transparency
- Sensors
- Networks
- Data Centre Sorting Algorithms
- Mobile Application
- Access Levels
- The administrators monitoring the alarm systems
- The act of operating the alarm system through the mobile application
- Data in all forms and types
- Processes concerned with translating data to adequate formats which are dependent on the entity that will make use of it.

Challenges

The aforementioned list can go on endlessly however matter of fact is that there countless entities to take into account for the Internet of Things. Therefore, it is very important that all stakeholders, entities and involved parts need to be mapped out and addressed to get a as clear as possible picture of everything to ultimately anticipate the challenges that may come about. This also applies to IoT alarm systems.

Some challenges that could arise are:

- Tackling privacy related issues is very important since IoT alarm systems will be fuelled by data. This data in turn is collected for increasing efficiency and developing alarm systems to run increasingly smoother in all aspects. However, this data will be generated, either directly or indirectly, by persons and could potentially be subject of abuse. Privacy is a basic human right, protecting it and treating it with utmost care will be a challenge that needs to be addressed properly and continuously. Developing standards and guidelines that aim to preserve privacy in alarm systems will be key in handling privacy preservation correctly. Privacy threats such as profiling, linkage, localization etc. all will need to be included in rigid standards that put personal privacy as the most important thing. The GDPR is one regulation that takes aim at privacy threats. However, there is much more work to be done. Especially on more detailed levels work is still pending as to be of support of an overarching regulation such as the GDPR.

- IoT alarm systems will become an amalgamation of numerous standalone services (provided by third parties which can potentially be independent of each other) and will be offered as integral solutions. For example: the mobile application of an alarm system, the hosting of its web application and the storage its data can all be provided by standalone vendors which are contracted by one single manufacturer. Meaning, manufacturers will become more and more of a service provider that bring together several smaller services such as cloud, monitoring, networking and hosting services to offer their end users an all-in-one alarm system package. This blurs the lines for, among other things, responsibility and liability. Rules, regulations, standards and tests need therefore be aimed at covering this new paradigm efficiently and will perhaps even require a total new approach. On top of this, technology keeps evolving rapidly so having a flexible basis to create stringent rules, regulations and standards is a challenge on its own. One option is to accept the inherent characteristics of IoT alarm systems and approach standardisation with a modular solution. In this way modules can be put together in a variation of different ways to solve various different problems and challenges. However, the synergy of the modules is also a challenge that is not one that is very easy to solve.

- The personnel that will be involved with IoT alarm systems need also be trained in such a way that they can comprehend the new dynamics of IoT alarm systems. A proper example is a comparing a fire detection system from the past with one that utilizes digitalization. Previously, when installing, servicing and maintaining such an alarm system, the person in charge for this usually was trained to do these things correctly. With a digital fire detection system, the personnel need also be digitally trained to perform their duty adequately. This means that training needs to be additionally geared towards digitalisation.

In conclusion it can be safely stated that the internet of things is going to have an impact on alarm systems as well. Complex and multi-layered chain of entities, also referred to as ecosystems, will be at the basis of IoT alarm systems. This will allow for a lot of opportunities but will also bring about novel challenges. Striking a good balance between human interactions, technology and processes will be the first step into taking on these challenges.

References

[1] M. A. a. G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, 2014.

[2] J. M. C. Mohammad Al-Rubaie, "Privacy Preserving Machine Learning: Threats and Solutions," IEEE, 2019.

[3] Remote Access for Remote Services, Kiwa FSS Products

[4] P. &. S. C. &. K. P. &. G. A. &. Y. M. &. V. A. orambage, "The Quest for Privacy in the Internet of Things," IEEE Cloud Computing, 2016.

[5] Intersoft Consulting, "www.gdpr-info.eu," [Online]. Available: https://gdpr-info.eu/chapter-1/. [Accessed 7 3 2019]