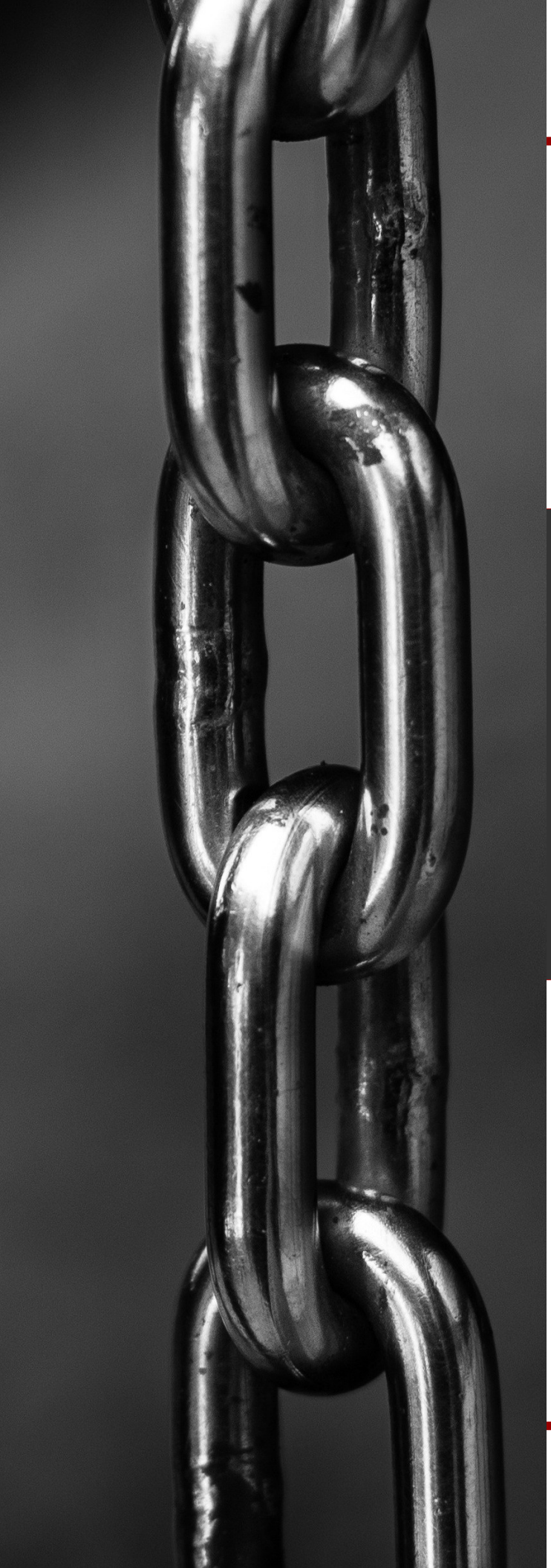

IoT Security: Everyone's Business

IoT has become one of the most important trends in the last years. With a huge projected impact in the world -both economic and social-, IoT is in the radar for most companies due to the potential benefit it could mean for these companies. But IoT is also in the mind of people expecting to simplify their lives with all kind of devices.

But not everything is bright with IoT. Security risks have been exposed by experts, especially after several incidents such as the Mirai attack and the Foscam cameras leak. Some people blame customers for not securing their devices; others blame manufacturers for not implementing good security policies. At then end, no action is taken because it's not clear who needs to do what.

And, as expected, many vendors claim to have the solution to all these problems. They promise that by using their products, customers can be confident that their devices and systems will be secure and free of risks of getting affected by an attack.

The problem with these claims is that each vendor focus on their specific field of expertise (e.g. Cisco claims that all security risks can be solved with their network devices) and none of them provides an integral solution that covers all the vulnerabilities that could be present in an IoT system, or it's very hard to integrate a bunch of products from different vendors, making the problem worse because customers would believe they are protected when in reality they are not, thanks to a bad configuration/integration among devices.

If this is the current scenario, what customers could do to secure their IoT deployments? First of all, don't believe the hype some vendors are creating. Don't get me wrong, the security threats are real, and will increase both in size and impact in the future. However, heeding just one vendor's perspective could be a costly error.

The right approach to securing an IoT deployment is to analyze each specific case and decide which solutions are the best ones for each component of the system, including operations and maintenance. It's not the same thing to secure a phone app than a database, or to secure a communication channel than to secure a sensor. And also, the response to an incident should be different if the source of the issue is internal or external.

The following sections describe the main components of a typical IoT deployment, the main threats for each one them, and suggestions about how to secure them.

Applications and User Interfaces (UI)

Applications are one of the entry points to the system. An application could be a smartphone app, a web page or a desktop app. Since these applications are generally just a nice way to collect and display information, developers tend to think that security is not relevant since they are not processing or storing information. Thinking like this is a big mistake since attacks are not just an exploit of one vulnerability. Most successful attacks are a combination of exploits that the attacker follows in order to reach the valuable data. For example, a lousy coded web page could give hints to the attacker about the system, the technologies used, the name of the components, and so on.

One of the main components of the app is the user interface (UI) and it should take in account security practices to help making the whole system more secure. For example, let's say that a database have a bug when strings are used instead of numbers. If the UI validates the data the vulnerability won't be exploited even if the bug is not fixed, because the harmful data never reaches the database. This kind of vulnerabilities, called Injection Attacks, are very old (described first in 1998) but are still the number 1 attack according to the 2017 ranking by the OWASP (Open Web Application Security Project).

Even small things, such as session time outs and locking after several failed login attempts, help to make the system more secure. And even when designing the interface, the designers should pay attention to little details such as error messages, field names and the information exposed in source files.

Network and communication channels

Unless the system is isolated (which is very uncommon these days), all the data travels through a network. This is, a combination of devices doing routing, switching, access control, monitoring, etc., and communication channels between those devices. All of these components are exposed to security threats, since they are generally public infrastructure. This is why many times security is associated just to those network devices and communication channels, and even if it's true that not all security efforts should be focused in securing the network, it's also true that an insecure network would translate into a successful attack. Therefore, securing the network and the communication channels should be one of the first steps in any security design.

There a hundreds of network security solutions out there and most of the times is very hard to choose the best ones for each specific case. In this case, it's better to stick to the fundamental principles of information security and start from there:

- ✔ ***Avoid unauthorized access and unauthorized command execution:*** access control and policies are the most used tools for this.
- ✔ ***Confidentiality:*** Data should not be exposed to unauthorized individuals or entities. Encryption is the best answer for achieving this.
- ✔ ***Integrity:*** Data should not be modified by unauthorized individuals or entities, or modified in a wrong way by authorized ones. A combination of encryption -to avoid data tampering in a communication channel- and a mechanism to grant integrity -such as a digital signature- could be needed.

- ✔ ***Availability*:** The network must be available for users as much as possible. There are several practices used to mitigate the risk of this kind of attacks, but it's hard and expensive to achieve a good level of availability, as demonstrated by the DDoS attacks.

Once the needs and the impact for each of these principles are identified, the products and solutions could be selected.

Data Center

The attractive cost structure and functionality offered by data centers providers as Amazon AWS and Microsoft Azure, has lead companies to move their critical systems to the cloud. From an operations point of view, this is an excellent choice -no maintenance team, no energy bills, no hardware failures, etc.- however, companies don't realize that they are moving their critical information outside their full control and that the cloud providers are exposed to attacks and security incidents as any other company. Some of them even hide the security incidents from the public to avoid getting a bad reputation.

Some actions the companies could do to avoid issues with the cloud providers are to consider data stored in data center as exposed to the public and therefore applying mechanisms to protect them, such as encryption, access control, etc. Also, the companies should have very clear what are the responsibilities of the cloud provider and define an action plan in case of a security incident which includes data migration, system shutdown, and even fines to the provider.

Sensors and end devices

Sensors and end devices are probably the most insecure elements in the system. This is due to a combination of elements: not enough resources to implement security mechanism, bad out-of-the-factory configurations, not enough functionality such as an updating mechanism, physically

exposed in insecure environments, and so on. And since every IoT company is running to deliver something to the market, security is not part of the Minimum Viable Product (MVP). Even some of the protocols used by sensors, such as MQTT, don't provide security out-of-the-box and relies on installers to enable the security mechanisms.

IoT users should select carefully the sensors they would install on their deployments, the security mechanisms they offer, and how to use them. If the sensors don't provide the desired level of security, this flaw has to be compensated with a higher level of security in one of the other components of the system, such as the network devices (e.g. gateways) or the communication channel.

Tools

Many of the current security efforts are focused on developing tools that could detect and even predict attacks. Machine learning is the last trend used for these purposes.

These tools are a great way to protect and monitor the system. However they are usually very expensive and hard to configure and use. Also, companies must be aware that a tool is useful only if they know how to take advantage of the data it generates. A tool can be very accurate predicting an attack, but if the company doesn't know how to react to them the tool is mostly useless.
Also, this tools are not free of suffering attacks themselves. There is potential attack where the attackers tamper the information sent to the tool and even the algorithm and the rules it follows to classify an event as an attack. By doing this, the attackers has a back door entry in the system that could be used later.

Policies

All the cybersecurity professionals agree that no system is 100% secure. They are so complex and with so many components -including humans- that it's practically impossible to secure the whole system.
Having this in mind, one of the key components of a security design is to define how the company will react in case one of the attacks is successful. This set of policies should define actions such as isolate compromised components, audit tracks reviews, disclose the impact of the security breach to customers, fine any vendor which didn't follow the company's policies, and the most important one: learn what happened and take the needed measures to protect the network against these kind of attacks.

Policies are so important that security experts say that's it is the only way to force IoT companies to secure their devices. For example, a home device with a security vulnerability could be used to start a distributed attack (e.g. DdoS). When this happen, the vendor doesn't face any consequence for not securing appropriately its device. If companies -and even governments- establish consequences for the vendors, these vendors will be more careful about shipping an insecure product.

People

Everything described above must be defined around the most important component of the IoT ecosystem: the people.
An IoT solution must improve the life of the citizens, the way a person works, or the life quality of a patient. And companies can benefit from IoT solutions if they keep in mind the customers.
For example, one could think that an IoT system improving the logistics of a transportation company would benefit only such company because it could cut the costs. However, at the end, such cost reduction and the improvement in the system's efficiency will benefit the customers

because they will get their goods faster, and with more reliability and visibility. The success of an IoT solution can be measured by the benefit percieve by both the company and the customer.

Said that, it’s clear that a good security design must be aligned with this win-win scenario. One company could implement a very expensive security solution just to avoid legal issues and then translate this cost to customers. This is not the best scenario. A company should implement a security solution to protect their customers. If it implies a higher cost, the company should be honest and explain why it’s implementing such security mechanism. In the current world, where most of the people are aware of the cybersecurity concerns, customers will understand and even prefer a company with such degree of transparency and concern for the customer’s valuable data.

Securing an IoT system is everyone’s business, and all the members of this ecosystem should be part of the security efforts.