CCN-CERT

BP/05

Internet of Things

BEST PRACTICES REPORT

JUNE **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Index

1. **About CCN-CERT** 4
2. **Introduction** 5
   - 2.1 Trends in the internet of things 8
   - 2.2 Relations with the cloud 11
   - 2.3 Critical infrastructures and the internet of things 13
3. **Visibility on the internet** 15
4. **When devices are the target** 18
   - 4.1 Recommendations 20
5. **When you are the target** 22
   - 5.1 Recommendations 24
6. **Attack surfaces** 25
7. **Measures to protect and/or reduce the attack surface** 29
   - 7.1 Secure configuration 29
   - 7.2 Update 30
   - 7.3 Genuine updates 31
   - 7.4 Firewall and harmful code detection 32
   - 7.5 Authenticity and integrity of commands 33
   - 7.6 Internet connectivity 34
   - 7.7 Security settings 36
   - 7.8 Software/firmware integrity 39
   - 7.9 Physical security 42
8. **Conclusions** 44
9. **Decalogue of recommendations** 47

1. About CCN-CERT

The **CCN-CERT** is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

Its mission, therefore, is to **contribute to the improvement of Spanish cybersecurity,** by being the national alert and response center that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively confront cyber-threats, including the coordination at state public level of the different Incident Response Capabilities or Cybersecurity Operations Centers

Its ultimate aim is to **make cyberspace more secure and reliable,** preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose

In accordance with these regulations and Law 40/2015 on the the Public Sector Legal System, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incidents will be managed by the CCN-CERT in coordination with the CNPIC.

The CCN-CERT is the Information Security Incident Response Capability of the National Cryptologic Center.

2. Introduction

The term "Internet of Things" refers to networks of physical objects: artefacts, vehicles, buildings, household appliances, clothing, implants, software... in short, sensors with network connectivity which allows them to collect information of all kinds.

A study by IOT Analytics[1] shows that by the end of 2019 there were 9.5 billion connected IoT devices in the world excluding mobiles and computers. Over the next few years, demand is set to soar to 28 billion by 2024 and 40 billion by 2027. It is not hard to imagine how such a vast number of objects represents a huge area of social and industrial exposure never seen before.

In the same report, a graph showing the number of IoT platforms in the world from 2015 to 2019 shows that by the end of 2019 there were 620 Internet of Things (IoT) platforms worldwide, more than double the number counted in 2015.

While the media and security experts are constantly warning about the risk of cyber attacks, the risks associated with the Internet of Things are rarely mentioned.

IoT security is not yet in the spotlight, even for companies that have a lot to lose if a security breach occurs. In a 2017 survey conducted by US consulting firm Altman Vilandrie & Company, nearly half (48%) of US companies using an IoT network had experienced at least one security incident.

The Internet has gone through four (4) distinct phases over the last 30 years (academic, commercial, transactional and social phases), and has maintained a stable implementation and improvement over many years, but nevertheless, it cannot be said it changed much from an

1. https://iot-analytics.com/iot-2020-in-review/

architectural point of view. In fact, it is essentially the same entity that was designed in the ARPANET era[2].

In this context, IoT is the first real evolution of the Internet, a leap that could lead to very significant changes in the way we live, learn, work, entertain and socialize. The most transcendent thing about IoT is that it gives sensors and sentience to the Internet, allowing a reality to exist autonomously beyond itself, the physical world, us and what is ours within it

IoT refers to all those adapted everyday objects or devices that are connected to each other or to the internet. The IoT is a relatively new

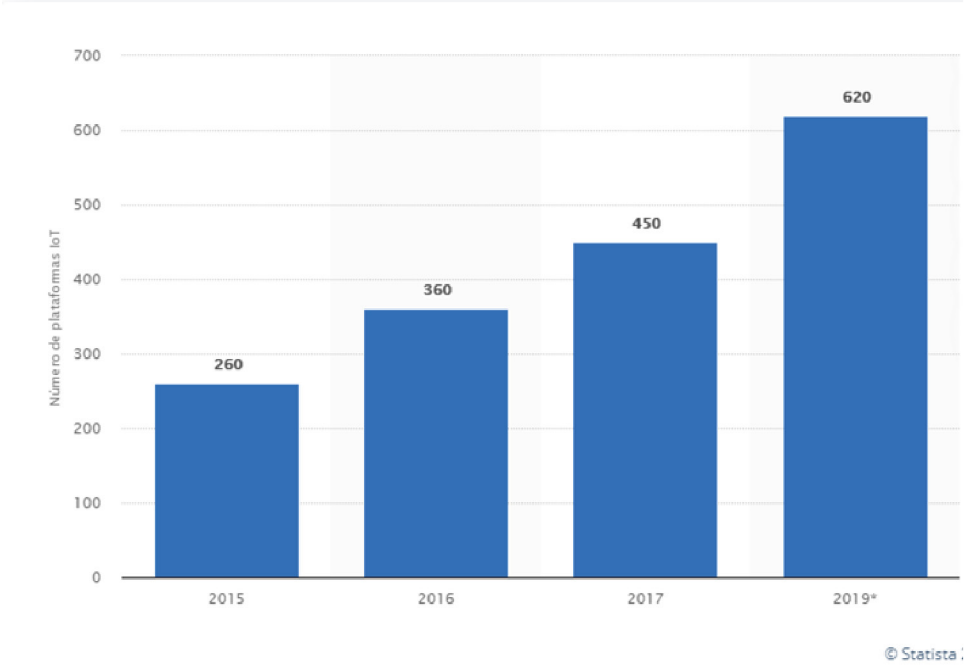


Figure 1.- Number of IoT platforms in the world 2015-2019

While the media and security experts are constantly warning about the risk of cyber attacks, the risks associated with the Internet of Things are rarely mentioned.

2. See https://sistemas.com/arpanet.php

concept and for this reason, the cybersecurity field is not yet ready to deal with all the threats it represents, the ones that have already emerged and those that will undoubtedly emerge in the near future.

One of the greatest recognized advantages of these devices is their connection to the Internet, but this capability is also one of their greatest weaknesses, as such connectivity can threaten the security of the entire system by significantly increasing its exposure to cyber-attacks.

For example, if there was no access control on the device or if it had any flaw, an attacker could remotely access the device and alter its configuration and even all of its functionality. Such access could occur at any time and from anywhere, so the integrity and functionality of the IoT device that was originally installed and used on a daily basis on a regular basis could not be trusted.

The growing attack surface is dominated by non-traditional control points, ranging from something as innocuous as an internet-connected toy to something as critical as the connected sensors that control energy production in a nuclear plant.

2.1 Trends in the internet of things

Unprecedented connectivity is both the best and the worst of the Internet of Things as it creates both great opportunities and considerable risks. In an environment that extends from sensors to cloud applications and services, an end-to-end IoT ecosystem is essential to seize opportunities without compromising security, manageability and interoperability.

For example, Microsoft is developing kitchen worktops that can recognize food and display recipes that include those foods. There are smart mattresses that monitor the user's sleep patterns by measuring their breathing and heart rate and a great number of smart locks that open when you approach the door and can be remotely programmed to eventually let in friends or guests.

There is some restrained enthusiasm about the potential for 'assisted daily life', which is especially important for elderly or dependent people. There are several projects underway that include large IoT deployments for better management of cities and systems.

The potential applications of the Internet of Things cover a wide spectrum of multi-billion dollar industries ranging from security and health to lifestyle and gaming.

2.1 Trends in the internet of things

One example is Songdo[3] in South Korea, which is the first example of a fully equipped **Smart City**. Virtually everything in the city is wired, connected and turned into a continuous source of data that can be monitored and analyzed by a multitude of computers with little or no human intervention.

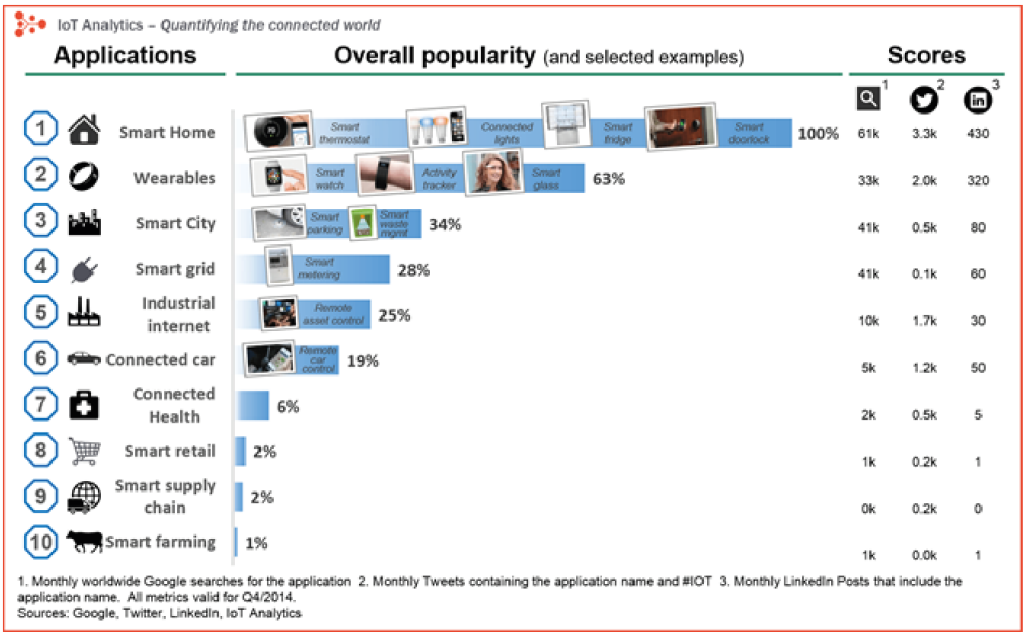


Figure 2.- Popularity of IoT devices.

Another aspect to take into account is the rapid **update and obsolescence cycles** that are common in the world of information technologies. If these technologies are to be integrated with building and architecture, we could end up with buildings, houses and factories riddled with completely obsolete elements, with no support and no possible maintenance.

With the IoT, our homes are becoming more *hackable* as the number of connected devices increases. Cybersecurity experts' nightmares are armies of *botnets* using smart toasters to develop distributed denial of service (DDoS) attacks or to hide code and executables away from the view of researchers.

3. See https://www.bbc.com/mundo/noticias-57030345

2.1 Trends in the internet of things

With the Internet of Things, the home and other smart environments become an extension of our work. Just as a *wearable* device counts our steps, heart rate or breathing, our homes will monitor and measure everything else.

The most obvious concerns have to do with **privacy**. The mass collection of our data and metadata may be the same as installing surveillance cameras, but it is a form of digital surveillance even more dangerous to our privacy and freedom than mere visual observation.

In the future, the Internet of Things may be a huge open network in which virtual entities and objects (avatars) will interact with each other independently according to context, circumstances and environment.

Enterprises will need to adapt their risk management practices and broaden the scope of risk assessments to include all connected devices. In this context, one of the main challenges for organizations will be how to store, track, analyze and make sense of the vast amount of data generated by including IoT in the risk assessment process.

2.2 Relations with the cloud

Today, many of these home devices use cloud-based backup services to monitor their usage and allow users to remotely control these systems. These allow users to access data and control the device through a mobile app or via a web portal.

Given the importance that cloud service providers will have in the various phases of IoT development, there is a strong need to check the security of their interface:

Determine whether the default user and password can be changed during the initial installation process of the product.

Determine whether accounts are locked after multiple login failures[4].

Determine whether valid accounts can be identified using password recovery mechanisms.

Check the resilience of the web interface against cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection (SQLi) and similar attacks.

Review interfaces in the cloud for any potential vulnerabilities (API interfaces and web interfaces of cloud systems).

4. For example, see: https://bitacoralinux.es/fail2ban-o-como-prevenir-ataques-de-fuerza-bruta/

2.2 Relations with the cloud

Securing the interface with the cloud requires:

- Changing the password and even the user name during the installation of the IoT product.
- Ensuring that users' accounts cannot be found out using functionalities such as password recovery.
- Ensuring that access to the account is temporarily blocked after several access failures.
- Ensuring that credentials (user names, passwords, access tokens, cookies, etc.) are not exposed to the Internet while transiting through it. Always use encrypted connections with TLS authentication.
- Implementing, if possible, authentication using two-factor or multi-factor verification.
- Detecting and blocking anomalous requests or attempts to gain access to the system/device.

2.3 Critical infrastructures and the internet of things

In recent years, industrial electronics and its computing were very specific and only present in closed domains. SCADA[5] systems are a type of Industrial Control System (ICS)[6] as are the so-called Distributed Control Systems (DCS)[7].

In industrial systems, data is received from remote stations and these generate reactions that, automatically or with the help of operators, are translated into executive actions that are sent to field devices, thus controlling the entire system. These devices are the ones that actually control local operations (opening or closing valves, setting or removing brakes, collecting data from sensors, monitoring the environment, setting the alarm level, etc.).

SCADA technologies are those that control industrial processes and all these installations have the essential characteristic that they cannot be shut down without causing great harm to the populations and systems they serve, nor without causing great economic losses that are difficult to bear.

SCADA communication protocols are manufacturer-specific, but many of them are widely used over TCP/IP networks thanks to later extensions of the original protocols. This dangerously blurs the boundary between industrial networks and general purpose networks such as the Internet. In any case, this migration to TCP/IP networks is a risk in itself, as it does not take into account the important differences between an industrial and a general purpose network.

5. SCADA (Supervisory Control And Data Acquisition). Ver https://www.wonderware.es/hi-scada/que-es-scada/
6. See https://www.industriasgsl.com/blog/post/que-es-un-sistema-de-control-industrial
7. See https://www.cursosaula21.com/que-es-un-sistema-de-control-distribuido/

2.3 Critical infrastructures and the internet of things

All these scenarios and many more, which make up the **Critical Infrastructure** catalogue, depend, to a greater or lesser extent, on control and monitoring networks that are being migrated to operate over TCP/IP networks and thus use the same network electronics as the Internet, all without prior assessment as to their effective security.

Consideration of SCADA security has changed dramatically since the Stuxnet attack[8] on the industrial control systems of an Iranian uranium enrichment plant in Natanz[9]. As a result, it has become clear to industrialized society what the threat of malicious code can mean for sabotage operations[10].

8. See https://www.businessinsider.es/10-anos-stuxnet-primer-ciberataque-mundo-fisico-657755
9. See https://www.bbc.com/news/world-middle-east-56722181
10. Kim Zetter: "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon" Crown Publisher, ISBN-13: 978-0770436179

3. Visibility on the internet

Thanks to the rapid growth of the Internet, more and more tools are becoming available to everyone, and one of them is the famous search engines.

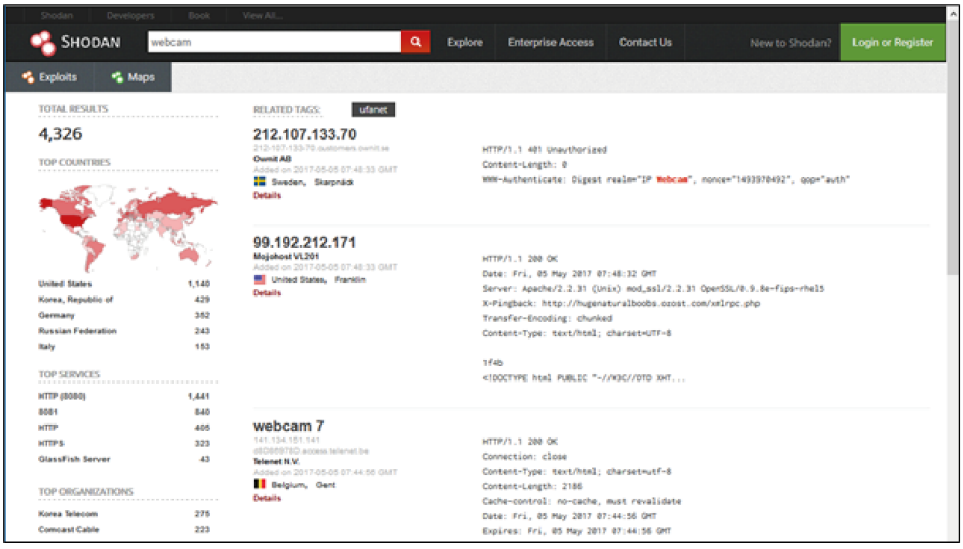


Figure 3.- Search for IoT devices in Shodan.

3. Visibility on the internet

As the services offered on the web have increased, so have the search engines, with the emergence of some engines such as **Shodan**[11], which makes it very easy to find IoT devices connected directly to the internet.

This search engine provides the user with a wealth of details about the device itself and allows the user to search by device type, such as "webcams". As shown in Figure 3, this simple search can find up to 4,326 webcams directly connected to the Internet at that time.

You can also filter searches by other terms such as the port they have exposed to the network. For example, you can find all devices that allow connections to port 22, which is the port for SSH terminals, and the search result returns up to 8,860,281 items directly accessible remotely with this type of communication on the Internet.

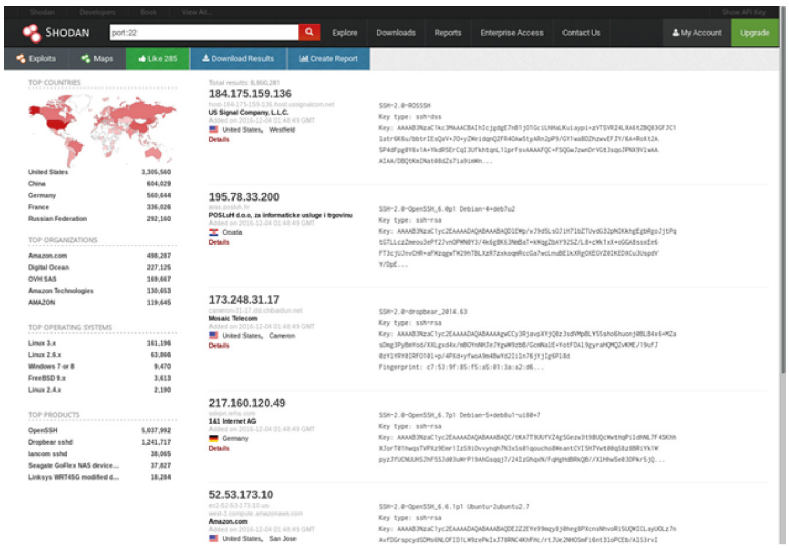
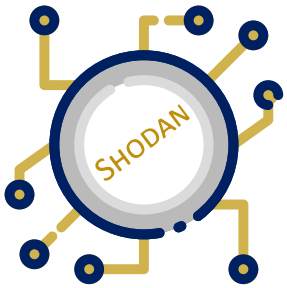


Figure 4.- Search for IoT devices in Shodan by port.

11. https://shodan.io

3. Visibility on the internet

In addition to Shodan, there are many other machine search methods that are directly connected to the Internet. Some of the best known are Scans.io[12] and ZMap[13].



It should not be forgotten that IoT devices can also be connected to each other or to other devices via radio connections[14], including Wi-Fi, BlueTooth (BT) or even NFC connections. In these cases, control of the devices is also susceptible to fall into the hands of malicious users.

In the report "Combatting the Ransomware Blitzkreig" there is a chapter dedicated to medical-related IoT devices that are connected to other devices via Bluetooth links, such as pacemakers implanted in patients, which highlights the security risks involved.

In any case, users are advised to search for their devices in the aforementioned search engines, as they are one of the main sources of information for attackers seeking to locate vulnerable devices.

12. https://scans.io/
13. https://zmap.io/
14. https://www.postscapes.com/internet-of-things-protocols/

4. When devices are the target

Once attackers find a way to automate the search for potential targets that they can access and manage remotely, all that remains is for them to do so and gain full control of the systems to carry out the illicit activities of their interest.

This network of machines and devices under the control of a single person is known as a “botnet”, which is made up by nodes known as “bots” or “zombies”.

When an attacker has access to a device, he usually installs malware on it that allows him to control it synchronously with other devices, even to launch commands simultaneously, so that all infected computers act in the same way, or in a coordinated way, against the same target.

The most popular attack of this type in recent years is the **Distributed Denial of Service (DDoS**) attack, which, by making massive and simultaneous connections from different sources, seeks to disable a service or a website so that nobody can access the attacked site.

It is interesting to note that compromised IoT devices are increasingly being used for such attacks, mostly digital video recorders (DVRs) and IP cameras.

4. When devices are the target

The reasons for launching DDoS campaigns are manifold, some of them are clearly politically motivated, others are protests or activism, etc. In other cases, their aim is simply to demonstrate the power of a group of cybercriminals when it comes to disabling a website. Sometimes the attacker threatens to disable the company's servers, which will seriously affect business activities, unless an extortion demand is paid.

Botnets are also used to carry out **spam** campaigns, which consist of sending unsolicited mass e-mails, or to alter the results of online polls and surveys. These botnets are usually rented to third parties as a platform to carry out activities of the customer's choice, which are usually illegal.

Currently, one of the most famous and widely used botnets is the Mirai[15] botnet. This botnet is widely used since, in mid-October 2016, its source code was published in the form of free code for anyone to use. In addition, it should be emphasized that this malicious code makes it very easy to infect devices and to grow as a botnet.

First, Mirai scans the Internet, mainly looking for cameras and routers. It then tries to access the device's administration panel using a list of **default users and passwords**. When it gains access to the device, it hosts itself on it and checks that it is not already infected by other malicious code and, if that is the case, it ejects it. It then tries to increase the infection, and thus the botnet, from that device by looking for new vulnerable machines.

Once the infection process on a machine is complete, it becomes a zombie machine which is continuously ready to be used in the distributed attacks indicated by its command and control servers'.
A new version of Mirai[16] has recently been discovered, equipped with more exploits, which makes it more dangerous and easier to spread. Moreover, this new version does not only target its usual victims (IP cameras, routers, etc.), but also corporate IoT devices.

15. https://www.akamai.com/es/es/multimedia/documents/white-paper/akamai-mirai-botnet-and-attacks-against-dns-servers-white-paper.pdf
16. https://www.kaspersky.es/blog/mirai-enterprise/18065/

4. When devices are the target

Botnets can easily be created in a matter of hours based on the growing number of insecure IoT devices that are connected to the internet.

Planning for DDoS attack mitigation shall consider attack rates of up to 1.5 Tbps (Terabit per second).

4.1 Recommendations

The first step to be taken with all devices, particularly IoT devices, should be to **change the password, choosing one that is truly secure** for all your profiles, especially those who manage **that device. If for some reason this is not possible, that device should never be connected to any other device and, as far as possible, should not be used.**

Another possibility would be to change the default TCP connection ports in order not to give browsers information about the service offered by the device through them.

If possible, it is also advisable to use an element that acts as an intermediary separating the IoT device network from the rest of the Internet. Such a device could be the router used to access the internet, in which case it should be **properly configured and security and access control measures activated** to secure the IoT device networks to which it provides connectivity.

Use an intermediary element that separates the IoT device network from the rest of the Internet.

The first step on all devices is to change the password and choose one that is really secure.

5. When you are the target

Although the concept of ransomware is currently more oriented towards the kidnapping of information and the payment of the corresponding ransom, there is no doubt that with the expansion of IoT, new forms of extortion of users will emerge.

While the effectiveness of ransomware on personal computers is based on taking advantage of the sentimental value of the private files captured and the value of that information (business environment) for the operation of the company, in the case of IoT devices, the objective will not be, in principle, the information that may be stored on them, but the permanent denial of service while waiting for a ransom.

For some devices, reinstalling the original firmware and resetting the system to factory settings may be sufficient to respond to the attack and restore its original operation, but depending on the device, this could be a complicated task and in some cases, given the nature of the service provided, the disruption to usual operation could be crucial and even life-threatening.

Take the example of a **pacemaker**. This device could be used to force the victim to pay a ransom under threat of deactivation, or to force the victim to perform battery-draining operations at an accelerated rate until payment is received.

In cases of denial of service of IoT devices or IoT installations, the cost of restoring service could far exceed the value of the ransom demanded, and the ransom would eventually be paid.

Depending on the device, disruption of proper operation could be crucial and even life-threatening.

5. When you are the target

It should also be borne in mind that, on some occasions, the process of restoring factory settings may be impossible to carry out in the short space of time set by the attacker. In these cases, paying the ransom may become the only viable option that does not put the affected person's life at risk.

Another example of an attack could be the infection of the general control system of a **home automation system**. By taking over the home's central controller, the attacker could determine at any time what the operation and behavior of all connected devices in the house should be, and enable various actions against its inhabitants.

For example, the actions the attacker could take could range from manipulating clock's alarm so that it goes on when it shouldn't and stays silent when it should activate, to telling a device's temperature regulator to go to extreme levels that could endanger its integrity. The attacker could also, for example, access surveillance cameras to obtain compromised images of the home's inhabitants and then use them to blackmail their victims.

It could also be a covert operation, where the attacker simply wants to know the victim's habits and schedule in order to plan the best time for a robbery or kidnapping.

In the case of IoT devices, the target will not, in principle, be the information that may be stored on them, but the permanent denial of service while waiting for ransomware.

5.1 Recommendations

This situation poses a new set of threats that the user has no means to combat. Therefore, the main recommendation is to **disable internet access on IoT devices**, thus avoiding the possibility of remote attacks and the theft of private information that could cause serious problems in the future.

In the event that such access from the Internet is absolutely necessary, it is essential to exercise extreme caution and security measures when establishing **who can connect (access control), from which device** (mobile, tablet, etc.) and a**t what time** of the day, week or year.

The inertia as users of information technologies makes us think that the increase in the number of functionalities of systems and devices is always good and welcome, but in the case of IoT it is necessary to think about whether these functionalities are necessary and are really going to be used and, above all, whether they compensate for the risks they entail.

Any functionality that is not disabled is one more opportunity for the attacker to take control of the entire system.

The main recommendation is to dispense with internet access on IoT devices; if this happens, extreme caution and security measures are essential: who can connect, from which device and at what time.

6. Attack Surfaces

Given the broad spectrum of IoT solutions that the industry is proposing, which is likely to increase in the coming years, it is interesting to identify early on the spaces or windows through which attacks can occur.

Below are some of the vulnerabilities on each of the fronts through which an attacker can gain access to an IoT infrastructure or the data it collects.

Attack Surface	Vulnerability
Ecosystem Access Control	Implicit trust among all components of the system. (In)Security in component registration (enrollment). The removal or retirement of equipment (decommissioning). Loss of access credentials and procedures.
Device memory	Clear usernames and passwords. Third-party credentials in clear. Encryption keys in clear.

Attack Surface	Vulnerability
Physical interfaces of the device	Firmware extraction. Command line interface for users and Administrator. Possibilities for privilege escalation. Reset to an insecure state. Removal of storage media. (No)Resistance to physical manipulation of the device. Presence of debug ports (e.g. JTAG[17]). Exposure of serial number or the identity of the device.
Device Web interface	SQL injection, Cross-site scripting y Cross-site Request Forgery. Extracción y listado de nombres de usuarios válidos. La presencia de contraseñas débiles. Posibilidad de bloquear cuentas. Existencia de credenciales por defecto.
The device firmware	*Hardcoded credentials*. Disclosure of URLs and sensitive information. Presence of clear encryption keys. Alteration of the cipher itself (symmetric and asymmetric). Show the firmware version and/or the date of the last update. Forgotten user accounts acting as backdoors. Active vulnerable services (web, ssh, tftp, etc.). Exposure of the security APIs of the device. Possibility to revert to an insecure previous version.
Device network services	Dissemination of information. Line interface for users and for the Administrator. Code injection possibilities. Denial of service. The existence of unencrypted services. The use of poorly implemented encryption. Presence of test and/or development services not removed or not disabled in production scenarios. Buffer overflow problems in software. UPnP[18] and vulnerable UDP services. The chances of success in DoS (Denial of Service) attacks. The On The Air (OTA) update of the device's firmware. The chances of successful Replay attacks. Lack of verification of data or code uploads. Lack of verification of the integrity of messages, whether they are data or commands.

17. See https://study.com/academy/lesson/joint-test-action-group-jtag-definition-uses-process.html
18. See https://www.redeszone.net/tutoriales/internet/upnp-problema-seguridad-red/

6. Attack Surfaces

Attack Surface	Vulnerability
Administrative Interface	SQL injection, Cross-site scripting and Cross-site Request Forgery. Mechanisms to discover valid usernames. Presence of weak passwords and known default credentials. Option to block accounts. Absence of Security/Encryption and secure logging options. No two-factor authentication. Inability to securely wipe the device.
Local storage of data	Presence of unencrypted data and/or encryption with compromised keys. Lack of data integrity checks. The use of the same encryption/decryption key for all data.
Web Interface of the Cloud	SQL injection, Cross-site scripting and Cross-site Request Forgery. Discovery of valid usernames. Presence of weak passwords and default credentials. Option to block accounts. The non-encryption of what is transported or communicated. The presence of an insecure key and password recovery mechanism. Lack of two-factor authentication.
Third-party backend API	Unencrypted transmission of personal or identifying information. Means of encryption of personal and identifying information. Disclosure of internal device information. Disclosure of the location of the device.
Updating mechanism	Updates that are sent unencrypted. Updates that are not properly signed. URL of the updates can be modified. No or ineffective verification of updates, or lack of authentication of updates. The possibility of installing malicious updates. The temporary or permanent loss of the updating mechanism. The absence of a manual updating mechanism.
Mobile application	The existence of default credentials and/or the acceptance or use of weak passwords. Insecure data storage. Absent or inadequate encryption of what is being transported. An insecure password and key recovery mechanism. The absence of two-factor authentication.
Vendors' API backend	Accept the trust in cloud or mobile applications as inherent. Weak authentication mechanisms. Weak or non-existent access controls. The likelihood of successful injection attacks. The presence of hidden services and undocumented functionalities.

6. Attack Surfaces

Attack Surface	Vulnerability
Ecosystem communication	The absence or abuse of system-wide health status checks. Tests for the correct functioning (Heartbeats) of the system. The (in)security of the commands that operate the ecosystem. De-provisioning of resources or capabilities. The forcing of updates.
Network traffic	The Local Area Network (LAN) itself. The hop from the LAN to the Internet (router, proxy, firewall, etc.). Short-haul air connections. Non-standardization of protocols and/or procedures. The wireless networks themselves (Wi-Fi, Z-wave, Zigbee, Bluetooth). The possibility to analyze devices with Protocol fuzzing[19] techniques.
Authentication and Authorization	Disclosure of values related to Authentication/Authorization of session keys, tokens, cookies, etc. Re-use of session keys, tokens, etc. The absence of device-to-device authentication. No or weak authentication of the device to the application and between the device and the cloud, and vice versa. Non-authentication of the application with the cloud, and vice versa. Lack of authentication of web applications with the cloud system. Lack of dynamic authentication techniques.
Privacy	Disclosure of user data. Publication of the user's location through the tracking of the device. The possibility of systems with differential privacy, where a few monitor everyone and no one monitors them.

Security of IoT infrastructure against the above attacks will be enhanced by any measures that serve to mitigate the effects of each of the exposure surfaces. Before adopting any technology or implementing an IoT-based architecture, it is advisable to ask yourself the questions listed in the table above.

19. See https://www.owasp.org/index.php/Fuzzing

7. Measures to protect and/or reduce the attack surface

In the case of IoT architectures, it will rarely be possible to use the same security measures that are recommended for ICT systems, with which the user is most familiar (antivirus, firewalls, malware scanners, etc.). However, there are others measures that need to be taken into account if you intend to work, travel, live, etc. with a secure IoT infrastructure.

7.1 Secure configuration

In general, the characteristics of each IoT device vary greatly from one to another, and in some cases it is possible to install security applications (mini firewalls, anti-malware, etc.) or at least modify the behavior of the device (configuration) to make it more secure. However, in many other cases the **physical and logical limitations of the device itself will make this protection process impossible**, and in many cases this impossibility is imposed by the manufacturer, in which case the only possible recommendation is to **abandon the use of this type of technology.**

7.2 Update

The main security measure to follow with any computing device, be it IoT or not, is to **keep all its software and firmware permanently updated**, as this is the only way to implement the latest fixes for detected vulnerabilities. The decrease in the number of vulnerabilities always decreases the risk and effectiveness of possible tools developed by attackers.

The timely updating of the systems, in addition to promoting their proper functioning, makes available new features offered by the manufacturers.

In general, the update process depends on the device in question. Some devices allow automatic updates by means of periodic connections and checks on the servers that the manufacturer has active for this purpose, while in other cases, updates can only be performed manually and therefore require the user to follow the instructions provided by the manufacturer.

7.3 Genuine updates

In any case, the quality of the IoT device is also related to the security measures implemented by the manufacturer so that the device can only install genuine updates authorized by itself.

One of the most effective attack procedures on IoT devices is fake updates, suitably modified by the attacker. **The integrity and authenticity of updates is an important consideration when purchasing electronic devices** of any kind.

In any case, **updates must be signed, and these signatures must be properly verified before** installation. It should be noted that **downgrade to earlier, more insecure versions should not be allowed,** so the update should always be subsequent to the version being updated.

7.4 Firewall and harmful code detection

Since it is not possible to install anti-malware or firewall software on the IoT device itself, intrusion prevention must be done at other layers in between to manage the security of the entire architecture.

The most recommended measure is to **properly configure the router providing internet access to the device** so that it filters connections to and from the IoT devices to which it provides connectivity.

The aim should be to restrict access to the device from external networks so that, for example, device settings can only be accessed from a computer connected to the same local network, or that connections to and from the Internet are made to specific and verified trusted IP addresses.

In this scenario, the **router must be properly configured** and **lists of allowed access (whitelists)** must be established for specific users, domains and/or IP addresses.

7.5 Authenticity and integrity of commands

If external connectivity for IoT devices and infrastructures needs to be maintained, it is appropriate that the system has a digital signature mechanism that allows cryptographic verification of the authenticity of the commands and communications that are established.

The IoT system should always establish whether a remote (Internet) connection to the IoT device is genuine or not, and if it is not, simply disregard the request.

7.6 Internet connectivity

It is highly advisable to disable any remote connectivity to the IoT device if it is not going to be used immediately. Both Bluetooth devices, which can be located by other nearby devices, and internet-connected devices, which can appear in specific search engines, are easy to discover, and the best way to prevent an attack is to limit access to them.

There are cases where it may seem necessary to access an IoT device from the outside, from any corner of the Internet, but it is always worth answering the question of whether it is really necessary to access “my fridge” from anywhere in the world. The answer is almost always not a resounding yes.

A risk mitigation solution is to establish what exactly are the conditions under which this connection needs to be allowed: from where, at what time, by whom, for what purpose, what exactly is it going to be allowed to do, and so on.

7.6 Internet connectivity

For example, if what is needed is to be able to turn on the heating in a second home so that the temperature is comfortable on arrival, the connection with the boiler is perfectly defined (command to turn the boiler on or off), it will be done from very specific devices (IP address of the main residence, telephones of the owner or authorized persons), probably on weekends and holiday periods (calendar), at certain times more likely than others (schedule) and in the event that the outside temperature is below a given value, etc. With this information, the time window and the origin of that remote operation in the IoT infrastructure can be limited.

7.7 Security settings

Due to the requirements of serving a wider market, in most cases, IoT systems include functionalities that are necessary at a given point in time for commissioning or for subsequent maintenance. In this case, all unnecessary functionalities must be deactivated in the exploitation scenario.

In order to make this possible, there are **configuration mechanisms** by means of which the functionality to be developed by the device in each scenario is determined. It is very important to check that the degrees of freedom available in the configuration process are sufficient. This verification includes:

7.7 Security settings

- Reviewing the device's administrative interface for options to strengthen system security, such as **forcing strong passwords.**
- Finding a way in the administrative interface to **separate administrator profiles from normal user profiles.**
- Reviewing the administrative interface for **encryption options.**
- Reviewing the management console for options to **enable the secure logging of various security events.**
- Reviewing whether there is a way to **activate alerts and notifications** to the end-user of all security-related events in the system.

7.7 Security settings

Making the configuration of a device sufficiently secure requires:

- Ensuring that **normal users** can be **isolated from administrators**.
- Ensuring the ability to **encrypt data at rest and in transit**.
- Ensuring that the use of **strong password policies** can be enforced.
- Ensuring the ability to activate **security event logging**.
- Ensuring the ability to **notify end-users of the occurrence of** security-related **events**.

7.8 Software/firmware integrity

The fact that the rules of the microelectronics market require huge volumes of sales of a single item to be economically viable, implies the emergence of IoT scenarios that are plagued by general-purpose hardware devices, whose specific operational functionality is dictated by the software or firmware they run.

It is very important that these universal devices, from the beginning (boot) and onwards (run), **can check the integrity of the software elements they run** and cannot be altered in such a way that they end up doing things they were not designed to do.

The control of any IoT architecture inevitably depends, firstly, on the ability to update the software and, secondly, on the possibility of physically changing the operation of the hardware itself (*firmware*).

7.8 Software/firmware integrity

Checking for the presence of insecure software/firmware updates includes:

- Reviewing the update file for sensitive information that may be exposed, even if it is obfuscated.
- Reviewing the production of update files so that they implement correct encryption using approved algorithms and procedures.
- Reviewing the output of the update file and checking that it is always correctly signed.
- Reviewing the security and robustness of the communication method used to transmit updates and publicize their existence. Systems should be prevented from not being updated due to unawareness of available updates.
- Checking the update server on the network to ensure that the communication encryption methods are up to date and correctly configured, and that the update server itself is not vulnerable.
- Checking the device for correct validation or signing of the update files.

7.8 Software/firmware integrity

Securing the software/firmware running on a device requires:

- Ensuring that the device is capable of updating itself. In IoT it is very important that everything has a secure updating mechanism.
- Ensuring that the update file is encrypted using methods and algorithms accepted as secure.
- Ensuring that the update file is transmitted over an encrypted connection and that the installation or configuration process ends with a positive **self-diagnostic phase**. If not positive, the update process should be completely reversed.
- Ensuring that the update file does not expose sensitive data.
- Ensuring that the update file is signed and verified before the update is published, distributed and applied.
- Ensuring that the update server is complete and secure.
- mplementing **secure boot** of the device if possible and its chain of trust.

7.9 Physical security

Certain attacks require physical access to the device, so they cannot be executed remotely. This will be especially easy in the IoT, as devices will be next to what they measure or operate, so they will generally have no physical protection.

Since the attacker will be able to access the device, or get as close to it as he wants, it is necessary to check whether the measures taken by each manufacturer are sufficient to provide **physical security for** the device:

- Reviewing the ease with which the device could be disassembled and **its storage media accessed or removed.**
- Reviewing the use of **external ports**, such as USB, to determine if the data contained within the device can be accessed without disassembly.
- Checking whether all external physical ports **are necessary** for the operation of the device.
- Checking the administration interface to determine if external ports, such as USB ports, **can be disabled.**
- Reviewing the administrative interface to determine whether the administrator's capabilities can be **limited to the local level**.

7.9 Physical security

Adequate **physical protection** requires:

- Ensuring that storage media cannot be easily removed.
- Ensuring that stored data is **encrypted at rest.**
- Ensuring that USB and other external ports cannot be used for harmful access to the device.
- Ensuring that the device **cannot be easily disassembled.**
- Ensuring that only those external ports, such as USB ports, that are really necessary for the proper functioning of the device are allowed.
- Ensuring that the product has the **ability to limit administrative capacities**.

8. Conclusions

Cybersecurity is facing a new challenge stemming from the everyday objects around us, the Internet of Things (IoT). From coffee machines and fridges to virtual assistants and video cameras, consumers are using a new wave of connected devices, although they rarely consider the vulnerabilities associated.

IoT attacks expose businesses to loss of data and services, and can make connected devices dangerous for customers, employees and the general public. Potential vulnerabilities will continue to grow as the number of internet-dependent devices increases.

With little regulation in place to hold manufacturers of connected objects accountable, these devices offer a **direct route to access personal, industrial or corporate data, often highly sensitive.**

Meanwhile, security teams are struggling to cope with an increasingly **complex threat landscape,** where any device could be the target of sophisticated attacks.

The design of most **IoT devices does not focus on the security of the devices themselves and others**, it rather focus on functionality, ease of use and quick time to market. These devices are generally cheap, useful and, if necessary, simple to configure, which often comes at a cost to security.

The nascent nature of this new paradigm, and the fact that most IoT attacks have been mere proofs of concept without serious consequences, does not mean that attackers in cyberspace will not focus on this market in the future.

A Hewlett-Packard study found that 70% of the most widely used IoT

Potential vulnerabilities will continue to grow as the number of Internet-dependent devices increases.

devices contain a wealth of vulnerabilities that can be exploited[20] by attackers. Moreover, 80% of these devices present serious privacy concerns, as they **collect particular,** mostly unnecessary **data about the user and their circumstances.**

For the time being, only the **demand for security on the part of the end user and society as a whole** will be able to impose on manufacturers and the market the need to consider all these aspects **before launching a product to the market**. This demand will force the authorities and the various professional sectors to opt for **regulatory measures to protect both citizens and society in general** from the consequences of populating the planet with billions of insecure devices.

Unlike traditional cyberattacks, IoT-related incidents do not limit to the extraction of information, but can also be used to **cause physical harm** or could be exploited by state-sponsored cyberattackers to cause serious damage.

Securing the 'thing' may not be the answer, as there will always be too many elements to manage. Instead, observation and monitoring will increase visibility, which together with analysis and timely response, will provide a pragmatic approach to reducing the risks inherent in the growth of IoT devices. This way, the aspects to consider would be:

The devices offer a direct access route to personal, industrial or corporate data, often highly sensitive.

15. See http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

8. Conclusions

Focus on what you can see. IoT devices often have a point of control, whether it's a router, firewall or proxy at the network perimeter or in the cloud. It is necessary to obtain visibility and, where possible, control it.

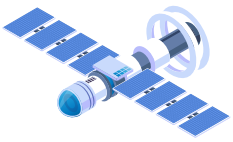
Analytics as a best friend. IoT devices share an often overlooked characteristic: their behavior is predictable. The application of machine learning for behavioral modelling is extremely effective in profiling risk, detecting anomalies and responding.

Dedicated security staff. Monitoring, investigation and remediation should never stop, and there should be staff to analyze the situation and articulate an appropriate response.

Success comes down to establishing a monitoring and control base to reduce risk exposure and apply smart techniques to the growing population of IoT devices.

9. Decalogue of recommendations

Then are ten (10) security recommendations for *IoT Architecture*



Security Decalogue for IoT Architecture

1. **Avoid using IoT** devices whenever they are not strictly necessary.
2. **Do not use**, as far as possible, **IoT devices that transmit information to external servers** (the Cloud), even if they are owned by the manufacturer.
3. **Change default passwords** on devices and use strong passwords that are not in any dictionary, that are sufficiently long and therefore difficult to guess.
4. Keep devices up to date with the **latest available software and firmware versions.**
5. **Disable all remote** (Internet) connectivity of devices when **not strictly necessary.**
6. **Keep open only those communication ports** that are really necessary and modify the listening ports if possible.
7. If IoT devices do not allow security configuration, always **operate them on a local area network (LAN)** behind a properly configured device (router) that does provide such security.
8. As far as possible, **ensure authenticity, confidentiality and integrity in all local (LAN)** communications, especially if these are made via radio links (Wi-Fi, Bluetooth, etc.).
9. **Periodically** and without prior notice, **check the security configuration** of all elements of the IoT architecture and of its communication devices with the outside world.
10. **Check the visibility of your own devices in IoT device search engines such as Shodan.**

CCN centro criptológico nacional

CCN cert centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es