Security in IoT Process in Uruguay

September 2019

Internet Society
Capítulo Uruguay

Uruguay
Digital

PRESIDENCIA
República Oriental del Uruguay

I. Content

II. INTRODUCTION

The open nature of the Internet creates the ability to connect multiple devices, systems, applications and services at a scale that transforms the way in which we interact with the environment and our society. The Internet of Things (IoT) has an enormous potential to improve the world. The projections of the impact of IoT on the Internet and on the global economy are impressive. It is estimated that in 2020, there will be 38.5 billion devices of this kind, which can be used for a wide variety of activities.

Definition of the Internet of Things (IoT)

According to the International Telecommunication Union (ITU), IoT can broadly be considered as a notion with technological and social repercussions. It can be seen as a global infrastructure at the service of the Information Society, which is conducive to the provision of advanced services through the interconnection (physical and virtual) of things, thanks to the interoperability of present and future Information and Communication Technologies. In addition, thanks to the identification, acquisition and processing of data as well as to its communication capabilities, IoT uses things to offer services to all types of applications while guaranteeing total compliance with safety and privacy requirements.

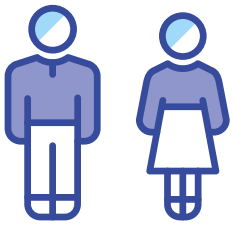
Importance of working on the security of IoT

IoT provides endless opportunities for individuals and companies. However, with billions of IoT systems and/or devices in use, a number that is continuously on the rise, working on security is even more critical because non-secure systems and/or devices may serve as access points for cyberattacks, affect trust and result in damages. Understanding the growing impact that security has on the Internet, the devices themselves and the various types of consumers is necessary to protect the future of IoT.

In this regard, the purpose of this document is to generate recommendations that will help IoT systems and/or devices to be secure from the moment they are designed, by default, making it easier for people to be more informed and secure in the digital world.

Starting point

To generate this document, a process was carried out at the national level where over 60 people from the most diverse sectors of activity participated in in-person meetings and collaborative work online to collect contributions from all interested actors.



The work was based on the following premises:

- People must be at the center of every possible solutions.
- Responsibility must be shared between everyone involved.
- The protection of privacy and personal data must be considered since the design and by default.
- Awareness campaigns must be implemented to specific audiences considering the most vulnerable group of people.
- There are many challenges that must be worked out, global cooperation is essential for a truly effective security of the network and consumers.
- It is necessary to focus on the entire life cycle of systems and/or devices.
- New actors involved in the IoT ecosystem may have little or no prior experience in cybersecurity.
- It is essential to promote a culture of cooperation among the various actors involved.

III. GENERAL CONSIDERATIONS

IoT encompasses a rapidly changing area in terms of new abilities and new security issues that are constantly being discovered. Best practices and standards for the security of IoT systems and/or devices are still emerging and are being analyzed by various organizations at a global level.

IoT is a series of interconnected systems and/or devices, including software and hardware, such as sensors and platforms. They provide several types of services. All parts must be protected, and this requires a layered approach to security.

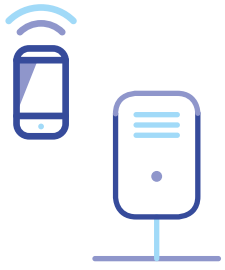
Internal and external security must be addressed. IoT systems and/or devices may be attacked, affecting the privacy and security of the consumer, but third parties may also be affected, as well as other systems and/or devices.

The security of IoT systems and/or devices is a global concern and the security of one person impacts on the security of everyone else.

Security should start at the design stage and continued throughout the whole life cycle of the system and/or device. Security is more effective when it is included in the process from the start till the end of the life cycle.

Timely, verifiable and effective patches and updates are a critical factor for addressing security vulnerabilities throughout the life cycle of these systems and/or devices.

It is paramount to investigate, report and communicate the vulnerabilities. Investigators have a very important role to play in testing security and warning about any weaknesses that are discovered.



The systems and/or devices vary in their privacy practices. Some are more recommendable than others, and it is crucial to adopt security measures in all layers.

IV. CHALLENGES

The various challenges present should be identified in order to work toward mitigating them.

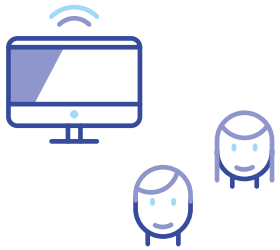
Economy favors weak security. Competitive pressures to reduce market release times for systems and/or devices and to lower costs has resulted in fewer resources being assigned to security. In addition, the commercial value of data encourages its accumulation, which goes in contradiction of good practices and against the protection of privacy and personal data.

There are currently very few mechanisms to signal and compare the security level of the different systems and/or devices (for example, through classifications), as there are no internationally accepted standards for labeling levels of security.

IoT systems and/or devices are complex and each part must be secure. Different components can be under the control of several actors and in various jurisdictions, making it difficult to achieve a unique and coordinated solution.

The security support should be maintained. Devices and/or systems require security updates to be protected against vulnerabilities.

Consumers tend to have little knowledge of the security of IoT systems and/or devices, which affect their ability to take security into account in their purchasing habits and to configure and maintain the security of their systems and/or devices.



Security incidents can be difficult to detect and address by consumers. In many cases, the effects are not obvious.

Existing legal responsibility mechanisms are unclear or are not adapted to the needs that IoT demands. If this is not addressed, it will be final consumers who are ultimately the most damaged.

V. COURSES OF ACTION

All actors have a very important role in the IoT security.

Many challenges must be worked out. Looking for global solutions and cooperation are essential for the security of the network and consumers to be truly effective.

In this regard, as the main courses of action, it is proposed to work toward protecting consumers and network resiliency.

Consumer protection

Generating trust and clear rules in the IoT ecosystem facilitates development and innovation, produces benefits and clarity, and promotes the universalization and mass production of IoT systems and/or devices in a secure context.

Main lines of action identified

Possible actions are proposed below on which it would be desirable to work to protect consumers of IoT systems and/or devices.

Consumer education and awareness. Development of capabilities and specific awareness-building on the topic. Understanding the importance of addressing certain aspects in order to be able to evaluate the security in their IoT systems and/or devices.

Risks. Ability to identify and understand current or potential risks.

Good practices guide. Understanding of good security practices.

Management of updates and patches. Knowing the measures that should be adopted so that the system and/or device is updated correctly and in a timely manner.

Data privacy policy. Comprehensible and easy to access.

Security starting with the design and by default. Ability to use them confidently. Robust access control, use of security protocols for communications and the possibility to block ports.

Consumer data protection. Protection of data throughout the entire chain and in all the layers.

Minimization of data. Limit the amount of data obtained by the systems and/or devices to those that are necessary for their operation.

Consumer service. Access to sites where consumers can find information and assistance for addressing any issues that may arise.

Consumer prevention. Mitigate any threats that are detected.

Terms and conditions. Easy to access and easy to understand.

Connection of IoT systems and/or devices to the Internet. Understand whether or not it is necessary for the system and/or device to be permanently connected to the network.

Accountability. Understand the specific responsibility of each one of the actors of the chain.

Classification system. Consumers must be able to easily identify the degree of security of the IoT system and/or device.

Network resiliency

The number of IoT systems and/or devices is constantly growing at a rapid pace, which makes them more attractive as the target of cyberattacks or as a means to execute them.

These systems and/or devices may have a presence in several areas of activity, requiring specific attention and measures, depending on the degree of experience of whoever is using them, as well as the potential risks.

In this regard, it is important to protect network infrastructure against new and potential threats, given that the systems and/or devices can affect: (i) consumers, if they breach privacy, security and even if they interfere in their use; (ii) other devices that are connected to the network; (iii) the network itself, if they affect trust and discourage its use; and (iv) the stability, security and resiliency of networks in general.

The most vulnerable systems and/or devices are those that are continuously connected to the Internet. In addition, people generally don't have the technical knowledge necessary to know how to protect them properly, and this generates an eventual access point that might result in a breach of other systems and/or devices.

Main lines of action identified

Possible actions are proposed below on which it would be desirable to work in order to protect network resiliency.

Risks. Identify the threats and vulnerabilities that may be associated with IoT systems and/or devices. Search for ways of mitigating the various risks that are identified.

Communication with the user. Inform and communicate, adapting the message to the target audience.

Passwords. Avoid using universal passwords by default. Attempt to make an initial password modification mandatory in order to perform and to use secure passwords.

Manage vulnerabilities. Report any vulnerabilities that are detected, promoting points of contact where they can be informed. Perform audits and monitor security events. Share knowledge and promote communication of the findings. Act in a timely manner and in coordination, as this helps to reduce vulnerabilities.

Update. Keep the software updated.

Data protection. Properly store login credentials and information. Activate the encryption of information and/or systems whenever it could be possible.

Security by design. Design and implement mechanisms to test the levels of security and protection, minimizing the exposure to attacks. Design the systems to be resilient against network faults.

Data storage. Pay attention to the information that is collected and limit it to what is strictly necessary. Facilitate the elimination of data, system updates and system and/or device maintenance.

Fault reporting. Configure or enable rules for detecting anomalies, which should notify the administrator and/or user and/or the manufacturer, when possible.

Predetermined configuration. Recommend to manufacturers that they adopt certain measures or security checks to accredit the security of the device. Be capable of correctly and securely configuring the systems and/or devices.

Backup. Allow security events to be stored in external repositories and avoid the loss of events.

Global cooperation. Global cooperation, given that digitalization and network security involve and might affect everyone. It is essential to develop global standards that facilitate technical interoperability and regulatory coherence, providing clear rules, predictability and transparency.

VI. FINAL CONSIDERATIONS

IoT provides endless opportunities to everyone. It presents potential risks that should be identified in order to work toward mitigating them.

The number of IoT systems and/or devices is constantly growing at a rapid pace. Therefore, multistakeholder work is essential in order to fully understand and consider the growing impact of IoT security.

To protect the future of IoT, it is essential for the different stakeholders to coordinate actions and constructively contribute to achieving solutions at a global level that will protect the network and people against potential threats. In this regard, it is recommended to closely follow other national, regional and global processes that may serve to replicate collaborative and joint actions.

Trust is essential for the sustainability and global drive of the Internet and networks in general. Building secure ecosystems that reduce risks and generate safeguards, as well as providing different information mechanisms so that consumers can make informed decisions when purchasing equipment or systems, are crucial for their proper development.

In light of the above and considering international standards and recommendations , it is desirable to work on a security framework and to develop tools and processes that will allow integration and support, placing people at the center.

VII. BIBLIOGRAPHY

Code of Consumer Security Practices in Relation to the Internet of Things. DCMS, 2018, 'Secure by Design: Improving the cyber security of consumer Internet of Things: Report', https://www.gov.uk/government/publications/secure-by-design. October 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/490114566519 Viewed July 12, 2019.

ENISA: "IoT Security Standards Gap Analysis". Mapping of existing standards against requirements on security and privacy in the area of IoT. V1. O. December 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/490100936575 Viewed July 12, 2019.

ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures". November 2017. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/498759112229 Viewed July 29, 2019.

ETSI TS 103 645 V1.1.1(2019): CYBER: Cyber Security for Consumer Internet of Things. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/499603848486 Viewed July 31, 2019.

GLOBAL CITY TEAMS CHALLENGE: "Smart and secure cities and communities challenge (SC3). A Risk Management Approach to Smart City Cybersecurity and Privacy. A Guidebook from the Cybersecurity and Privacy Advisory Committee (CPAC) Public Working Group. July 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495945984537. Viewed July 24, 2019.

GSMA: "IoT Security Assessment". CLP.17 V.3.0. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495964815061. Viewed July 24, 2019.

IEEE STANDARDS ASSOCIATION. IEEE Standards Activities in the Internet of Things (IoT). November 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/498755786979 Viewed July 29, 2019.

INDUSTRIAL INTERNET CONSORTIUM: "The Industrial Internet of Things: Managing and Assessing Trustworthiness for IoT in Practice". An Industrial Internet Consortium White Paper. Version 1.0. July 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/502051557200 Viewed August 5, 2019.

INTERNET SOCIETY: CANADIAN MULTISTAKEHOLDER PROCESS: Enhancing IoT Security. Final Outcomes and Recommendations Report. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/490100106034 Viewed July 12, 2019.

INTERNET SOCIETY: Top tips for Internet of Things security and privacy. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/491209777648 Consulted July 15, 2019.

INTERNET SOCIETY: "IoT Security for Policymakers". April 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/490319556578 Viewed July 12, 2019.

IOT-NOW: "New vulnerability found in internet building automation devices" https://www.iot-now.com/2019/08/13/98154-new-vulnerability-found-internet-connected-building-automation-devices/ Viewed August 29, 2019.

IOT SECURITY FOUNDATION: "IoT Cybersecurity: Regulation Ready". 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495957218652. Viewed July 24, 2019.

IOT SECURITY FOUNDATION: Make it safe to connect. "Establishing principles for Internet of Things Security". URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495971368874 Viewed July 24, 2019.

IOT SECURITY FOUNDATION: White Paper: Mapping the IoT Security Foundation's Compliance Framework to ETSI TS 103 645 Standard. February 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/499587357470. Viewed July 31, 2019.

ISACA: "Managing the Risk of IoT: Regulations, Frameworks, Security, Risk and Analytics". URL: https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/managing-the-risk-of-iot.aspx Viewed August 29, 2019.

ISTR: Internet Security Threat Report. Volume 23. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/497646535147 Viewed July 26, 2019.

ITU-T: Telecommunication Standarization Sector of ITU. Y4806 (11/2017). URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/498757025611 Viewed July 29, 2019.

LACNOG – M3AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition LAC-BCOP-1. May 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495302212082 Viewed July 23, 2019.

NRIA IoT Security Upgradability and Patching. Existing Standards, Tools and Initiatives Working Group (WG1). Catalog of Existing IoT Security Standards. Version 0.01. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/498758824895 Viewed July 29, 2019.

Organización de los Estados Americanos (Organization of American States) (OEA): "Ciberseguridad. Marco NIST". Un abordaje integral de la Ciberseguridad (Cybersecurity. NIST Framework: An Integral Approach to Cybersecurity). Edition 5. 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/517046329645 Viewed September 1, 2019.

ONEM2M: Facing the Challenges of M2M Security and Privacy. Phil Hawkers. 2014. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/511801089415 Viewed August 22, 2019.

OTA – Online Trust Alliance an Internet Society Initiative. IoT Confianza por Diseño. El marco de Confianza IoT de OTA (IoT Trust by Design. The framework of the IoT Trust of OTA). URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/493760516548 Viewed August 22, 2019.

OTA – Online Trust Alliance. Smart Home Checklist. Maximizing Security, Privacy & Personal Safety. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/511799261039 Viewed August 22, 2019.

OTA – Online Trust Alliance an Internet Society Initiative. The Enterprise IoT Security Checklist. Best Practices for Securing Consumer-Grade IoT in the Enterprise. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/511800322567 Viewed August 22, 2019.

OTA – Online Trust Alliance an Internet Society Initiative. IOT Security & Privacy Trust Framework v2.5. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/511797067111 Viewed August 22, 2019.

SENSORS: "The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey". URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/515507947386 Viewed August 29, 2019.

VII. REFERENCES

Juniper Research: "Internet of Things connected devices to almost triple to over 38 billion units by 2020". URL: https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020. Viewed July 31, 2019.

Recommendation ITU-T Y.4000/Y.2060 (06/2012) of the International Telecommunication Union. General Description of the Internet of Things. URL: https://www.itu.int/rec/T-REC-Y.2060-201206-I/es Viewed July 30, 2019.

With the participation of the following organizations: Agencia de Gobierno Electrónico y Sociedad de la Información (Agesic), Administración Nacional de Combustibles, Alcoholes y Portland (ANCAP), Administración Nacional de Telecomunicaciones (Antel), Claro, Dativa, Dirección Nacional de Telecomunicaciones y Servicios de Comunicación Audiovisual (Dinatel – Miem), Fundación Ceibal, IEEE, Intendencia de Montevideo, Internet Society Uruguay, Isbel, LACNIC, Laboratorio Tecnológico del Uruguay (LATU), Liga de Defensa Comercial (Lideco), Observatic, Seciu, Sigfox, Tib, Universidad de la República - Facultad de Derecho y Facultad de Ingeniería, Universidad Católica del Uruguay, Universidad ORT, Universidad de Montevideo, Universidad Tecnológica del Uruguay (UTEC), Unidad Reguladora de Servicios de Comunicaciones (URSEC), Administración Nacional de Usinas y Transmisiones Eléctricas (UTE), Youth Uruguay

Internet Society. URL: https://www.internetsociety.org/blog/2014/04/permissionless-innovation-openness-not-anarchy/ Viewed August 5, 2019.

In order for the degree of security of the systems and/or devices to be easily identifiable, the Working Group considers that it would be positive to encourage standardization institutes to agree on criteria or recommendations that allow classifying the security of IoT systems and/or devices, thus making it easier for the industry to comply and for consumers to understand them. It is recognized that an in-depth study is required that considers international standards, which is why conducting a specific and concrete study on the topic is recommended.