

Location-Based Security (LBS)

Location as
a security factor



Introduction	03
Towards the new trends of cybersecurity ...	03
Geolocation and security	04
Location-Based security	05
How it works	06

index

Introduction

Digitalization, Industry 4.0 and teleworking are increasingly present in our environment, causing many companies and institutions to open their systems to the Internet, increasing the risk of having their security compromised. This digitization process has accelerated in 2020 with the arrival of the pandemic caused by the COVID-19 virus, which has caused an **increase of 125%¹ in cyber-attacks in Spain in the last year, reaching 40,000 attacks per day.**

Towards the new trends of cybersecurity

In a context in which digitalization and interconnectivity are more present than ever and, as a consequence, there has been a notable increase in cyber-attacks, seeking and betting on alternative and innovative cybersecurity solutions is more important than ever.

“People are at the center of all business, and they need digitalized processes to function in today’s environment.” **Major technology companies such as Gartner are already talking about new cybersecurity trends that include, among others, the Internet of Behaviors or IoB, “anywhere operations” or remote operations and Artificial Intelligence.**

The Internet or security of behaviours aims to capture, analyze, understand and respond to all kinds of digital representations of human behavior and interpret them using innovative technologies and machine learning algorithms.

Learning from human behavior could in many cases put an end to security breaches by identifying, eliminating and preventing anomalous or risky behavior, such as the identification and detection of false identities or credential theft, which can be used to gain access to devices or services of various kinds and thus jeopardize the security of systems.

In addition, the most common attack in digital environments is the **theft of credentials or passwords, which is the cause of 81% of security incidents.** For this reason, **Microsoft is already talking about “replacing passwords with biometrics or authentication on a device which you own”.**

If it was already vital to **ensure the security of “anywhere operations”** before, Gartner is already talking about this cybersecurity trend as something primordial after the digital acceleration and teleworking produced by the pandemic.

With teleworking, millions of companies have been forced to use remote access tools, and in **March 2020 alone, Spain recorded more than 19 million² attacks on RDP (Remote Desktop Protocol), one of the most used tools.**

However, remote operations do not only apply to telecommuting. To close the systems security gap, it is necessary **to implement methods to ensure all types of secure operations from any location,** and therefore it is necessary to verify that, the location from which an operation or attempt is made to access information or services, is an authorized or usual location for the user.

¹ <https://www.interempresas.net/Ciberseguridad/Articulos/346890-Los-ciberataques-en-Espana-han-crecido-un-125-por-ciento-en-el-ultimo-ano-hasta-los-40000.html>

² <https://www.itdigitalsecurity.es/endpoint/2020/05/espana-registro-mas-de-19-millones-de-ataques-al-rdp-solo-en-marzo>



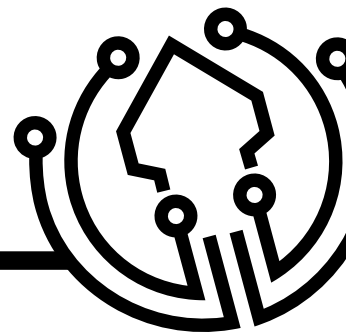
Geolocation and security

Geolocation presents several security and usability problems, reason why it has not been present in security systems until now. The main problems can be summarized in the following two points:

- 1. Most ge positioning systems are based on coordinates**, that is, using a GPS sensor the device obtains a latitude and a longitude with which you can locate a position on a map. Although it is useful for most applications, it is not for cyber security since any user with Google Maps can obtain coordinates and send a false location. Not only that, but there are hundreds of applications for mobile devices that allow you to send false coordinates, making it very easy for an attacker to steal, for example, the location of our house.
- 2. Geolocation requires a GPS sensor**, something that not every device includes, preventing its use in certain equipments, such as laptops or desktops.

How do we put an end to all these problems?

The best way is to add innovative security layers that take into account the identity of the device from which the service is accessed, using secure communication channels and factors that are more difficult to spoof. That is why at Ironchip we are launching a unique technology in the market, Location-Based Security, our AI that uses wave based location as a security factor.



Location- Based Security, “Security based on wave-based location”

In order to achieve a truly secure location that is difficult to falsify, we have replaced the typical latitude and longitude with other more advanced geo-location methods, based on Artificial Intelligence and Big Data processes.

Instead of using the GPS sensor, we are able to determine whether the device is in a secure location from the radio waves that surround it, that is, we analyze wifi signals, signals from mobile devices such as 2G, 3G and 4G, or even from IoT signals like Sigfox or Lora.

Our Artificial Intelligence process analyzes the radio waves found at the location, and creates a unique wave signature from them. This fingerprint must be sent again when the user wants to access the system.

1. Replacing the coordinates for the set of waves, we prevent any remote attacker from falsifying our location. To do this, the attacker would have to be physically in the safe location, which makes the attack extremely difficult and makes automated attacks impossible.
2. Any device with a Wifi card can be geolocated.

In addition, this geolocation technology is the first totally anonymous alternative, since by not knowing the coordinates of the location, only the waves, it is not possible to locate this location on a map.

Ironchip’s unique location technology also has the following characteristics:

- **Secure and difficult to falsify**

Replacing the coordinates for the set of waves, we prevent any remote attacker from falsifying our location. To do this, the attacker would have to be physically in the safe location, which makes the attack extremely difficult and makes automated attacks impossible.

- **Totally anonymous**

Ironchip’s wave based location technology is the first totally anonymous alternative to other systems that use location as a security factor since, as we do not know the coordinates of the location, only the waves, it is not possible to place this location on a map.

- **Encrypted information**

We do not store the wave information anywhere, neither on the server nor on the client. Our artificial intelligence learns, and then immediately destroys the wavelet information, so we only store the predictive mathematical algorithm that, when it receives the wave information, will determine whether it is valid or not.



How it works

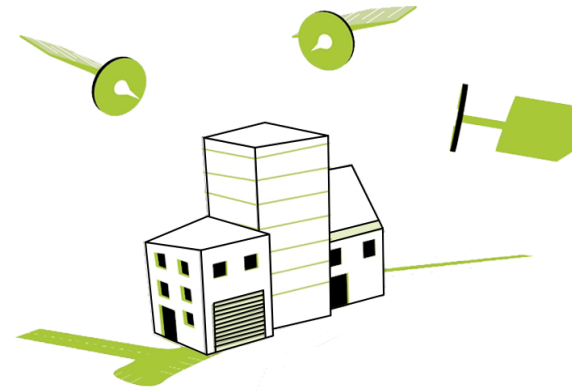
Analyzes the location waves

Ironchip's Location-Based Security technology analyzes the waves detected by a mobile/desktop device to create a digital identity associated with that location. In this way, it identifies whether the device from which the operation is performed is a recognized device and, by analyzing the waves in that location, it also verifies whether the operation has been performed from a secure location or area.



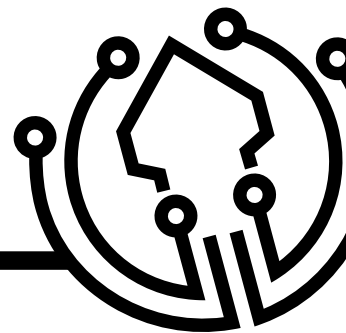
Sending signature to validate access

The device analyzes the waves of the location and then sends a signature associated with that location to verify that the user is in a secure area. In this way, Ironchip's technology has many uses or applications, ranging from using location as a security and authentication factor, to identifying and learning what a user's usual places of operation are and thus using location as an extra layer of security.



A unique signature of the waves is created


By replacing the coordinates with a set of waves, Location-Based Security technology creates a secure signature associated with a specific and secure location. This makes it the first fully anonymous alternative to other systems that use location as a security factor, since it is not possible to place this location on a map.



**Contact Ironchip's
sales team**

Aitor Zaballa

 aitor.zaballa@ironchip.com

 617 898 342

