

DIGITAL WITNESS: SECURE MANAGEMENT OF INFORMATION ON ELECTRONIC DEVICES

Description:

In a world in which users increasingly depend on their devices, they store a large amount of information and are a very valuable source of knowledge about their environment. However, the heterogeneity and density of connected objects, characteristics of the Internet of Things (IoT), serve as a veil to hide malicious behaviors that affect these devices, without leaving a trace of such actions. The use of embedded security architectures in mobile devices and other personal items is below its potential. Currently the purpose of these architectures is either to protect user data or to facilitate electronic payment. Recent advances allow the signature through the mobile phone using the latest version of DNIe that incorporates NFC. However, these architectures can offer much more. The technology that is the subject of the patent developed defines the concept and architecture of the digital witness, which allows personal devices and other devices with embedded security architectures to collaborate with each other to alert and record malicious behavior. This architecture makes it possible to implement a digital chain of custody in the IoT.

Keywords:

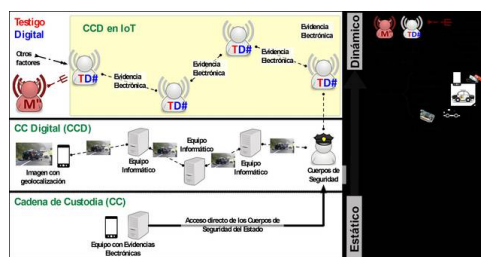
[Evidences](#), [Iot](#), [Anti-Tampering](#), [Security Architecture](#), [Security Of The Information](#), [Safe Element](#)

Sectors:

[ICT](#), [Security](#), [Protection and Defense](#)

Areas:

[Telecommunications](#), [Hardware / Devices / Components](#), [Internet and Networks](#), [Protection and security](#)



Advantages:

Some advantages that a digital witness provides compared to what already exists are listed below: - Binding identity between devices and users, in objects that use the security architecture described in the patent. - Necessary adaptation of electronic evidence management to the IoT. - Non-repudiation in mobile terminals and other objects restricted in resources. - Binding role-based delegation. Submitting electronic evidence takes advantage of the connectivity benefits of the IoT. - The digital witness will help detect attacks from their source and establish responsibilities. - Adds a new functionality to the use of personal devices. - Clarifies the architectural requirements necessary to improve the security performance of a personal device or other IoT objects.

Uses and Applications:

This technology is framed in the ICT sector applied to Information Security. The most direct application is the early detection of attacks that use objects that have the technology described in the patent, and its most direct use and simpler implementation could fall on objects used by state security forces (from mobile terminals to cars. patrol with on-board computer and TPM). Users with this technology could report cyber acts using the digital witness to report electronic evidence to the authorities. It should be noted that it can also be applied to IoT objects with few computational resources. This type of device can range from industrial sensors to wearables, as long as they implement the components of the architecture described in the patent.

Patent Number: ES2587584B2

Applicants: Universidad De Málaga

Inventors: Ana Nieto Jiménez, Rodrigo Román Castro, Francisco Javier Lopez Muñoz

Filing Date: 22/10/2015

Protection Level: National (Spain)

Processing Status: Spanish patent