Digital Witness: Digital Evidence Management Framework for the Internet of Things

by Ana Nieto, Rodrigo Roman and Javier Lopez (University of Malaga)

We define the concept of 'digital witness'; personal devices able to actively acquire, store and transmit digital evidence to an authorised entity, reliably and securely.

The growing density of networks formed by devices with heterogeneous capabilities and users with different profiles poses new challenges to cybersecurity. One clear example of this is the Internet of Things (IoT) paradigm, where cyberoffenses – not only cyberattacks – take place in very dynamic, polymorphic and even isolated scenarios [1]. There are too many devices to be controlled, and any device with minimal computing and communications capabilities can perpetrate cyber-attacks without leaving a trace. In such a scenario, and in order to clarify the facts of a cyber-crime scene, it is essential to collect and handle electronic evidence within a Chain of Custody (CoC). Yet this is a problem that is impossible to solve only with existing tools.

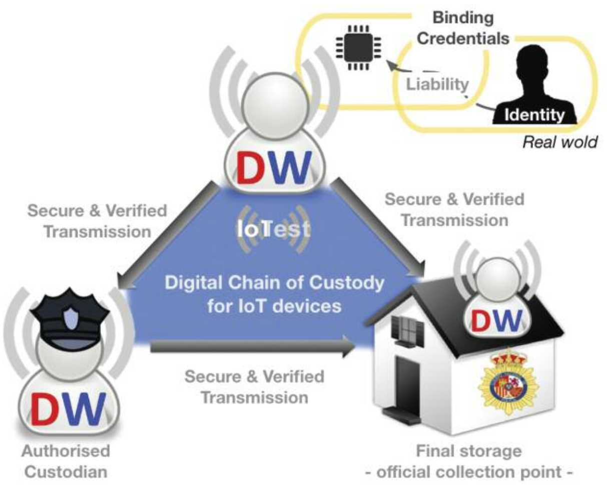
Binding Credentials
Liability
Identity
Real wold
DW
Secure & Verified Transmission
IoTest
Digital Chain of Custody for IoT devices
Secure & Verified Transmission
DW
DW
Secure & Verified Transmission
Authorised Custodian
Final storage
- official collection point -

Figure 1: Digital Witness for Cybersecurity in IoT.

The IoTest project [L1] aims to help solve this problem by introducing a security solution that is drastically different from those that have been used to date. This project proposes the design and development of the 'digital witness', a trusted electronic device capable of obtaining and safeguarding electronic evidence. More specifically, a digital witness: (i) binds the user's identity to his/her personal device, (ii) has a core of trust that is able to protect the integrity of one or more electronic pieces of evidence according to the law, within a trusted execution environment, (iii) ensures that only authorised entities have access to the evidence, and (iv) is able to witness the traceability of the evidence.

Furthermore, a digital witness (v) is able to send digital evidence to other digital witnesses or any other entity with the authority to safeguard the electronic evidence. The user's identity and the capabilities of his device determine the type and role of a digital witness, which opens the door to the creation of digital witnesses with different profiles (e.g., police cars as mobile custodians). These and other properties enable the creation of a digital chain of custody in IoT (IoT-DCoC) environments (see Figure 1). IoTest defines and works with this natural evolution to digital chains of custody [2].

These five basic requirements help to define a robust digital witness, and comply with several existing challenges in the emerging IoT-forensics paradigm [3]. In order to fulfil these requirements, the project will explore various novel concepts, such as the notion of binding credentials (BC). In this context, a BC is defined as any mechanism that provides a link between a user and a device, based on the user's identity. In addition, BCs can be used in conjunction with biometric capabilities in personal devices to ensure the presence of the user at the key moments within the lifecycle of the digital evidence.

IoTest is a novel project recently funded by the Spanish Ministry of Economy and Competitiveness under the EXPLORA Programme, a complementary action that encourages frontier research. Precisely, this project also will investigate the viability of more radical ideas in the context of future network environments, such as the implementation of the concept of digital witness in local clouds of personal IoT devices, the deployment of virtual digital witnesses that are linked to the identity of a privileged digital witness device, and the implementation of binding credentials associated to these virtual witnesses.

By using digital witnesses as a foundation for the creation of a digital chain of custody within IoT scenarios, the IoTest project aims to offer a dynamic solution that will record events on heterogeneous, unpredictable and uncertain scenarios. Moreover, since existing digital evidence processes and regulations are not prepared to deal with the new cybersecurity issues created by these highly dynamic and distributed scenarios, we expect that the deployment of digital witnesses will result in a qualitative advancement in the evolution of electronic evidence management systems, improving their ability to detect attacks and identify cybercriminals.

Links:
[L1] https://www.nics.uma.es/projects/iotest

References:

[1] A. Kasper, E. Laurits: "Challenges in Collecting Digital Evidence: A Legal Perspective", The Future of Law and eTechnologies, 195–233, 2016.
[2] Y. Prayudi, S. Azhari: "Digital chain of custody: State of the art", International Journal of Computer Applications, 114 (5), 1–9, 2015.
[3] E. Oriwoh et al.: "Internet of things forensics: Challenges and approaches", 9th IEEE Collaboratecom, 608–615, 2013.

Please contact:

Ana Nieto, University of Malaga, Spain
+34 951 952914
nieto@lcc.uma.es