Information Governance

Paul Wang, Kang Wei Woo, Jens-Matthias Bohli, Joao Girao, Ghassan Karame, Wenting Li

Abstract

Many of the challenges that city planners face require the cooperation of different government agencies. The scope of the problems requires the involvement of diverse groups -who may have conflicting practices or agendas. In order to launch a coordinated response, different arms of the government, with different security clearance, must contribute seamlessly, without the hindrance of such administrative overheads. In NEC's Inter-Agency Collaboration solution, the MAG1C (Multi-AGencies, 1 Concert) Suite, we provide a platform where resources and information owned by individual agencies can be shared without compromising the security model. In order to make this happen, a mechanism for a proper Information Governance is needed. This paper talks about the technologies used in our Information Governance Suite. Minimally, it enables various agencies to access information they require, while protecting it using access rights. This means various agencies collaborating on a situation can have access to a set of data on a "need to know" basis. The value of Mag1c Authorization is the flexibility to apply many dimensions of control to cater to various operational demands.

Keywords
e-Evidence, Information Governance, user authorization, Inter-Agency Collaboration, device integrity

1. Introduction

As public security and safety agencies and city planners around the world continue to advance in their plans for making cities safer, the sharing of devices and information among different agencies becomes essential. Agencies such as police, emergency services and authorities for land transport, environment and water working together in a city-wide monitoring project, will look for various signs of threat, from urban surveillance to the monitoring for possible fire and floods. The ability to share the resources expediently will enable the government agencies to have crucial situation awareness to better respond and even pre-empt implausible incidents.

However, with this sharing of resources comes the issue of information governance. In NEC's Inter-Agency Collaboration solution, the MAG1C Suite (Multi-AGencies, 1 Concert), we provide device integrity and authorization features. The device integrity feature ensures that an appliance to be installed by various agencies is not compromised and therefore, the information accessed from the appliance is reliable. Users would only receive information on a need-to-know basis. In addition, the authorization feature enables various agencies to access information they require, while protecting it using multi-dimension access rights. This means various agencies collaborating on a situation can enforce their respective security policies, to ensure access to a set of data by the right users, at the right place and on a right occasion with the "need to know" criteria.

2. Device Integrity feature

2.1 Device Integrity for mobile devices

Remote attestation of untrusted devices is gaining increasing popularity nowadays. The literature includes various proposals to establish a static root of trust and/or a dynamic root of trust in various computing environments. Most existing solutions rely on embedding TPM chips within mobile devices and establishing a root of trust within the mobile device[1) 2)]. However, while there are several architectures for standard PC platforms that can support the establishment of a root of trust, this technology is rather immature for mobile or embedded devices.

NEC Laboratories Europe's IMASC technology addresses the shortcomings of existing solutions by enabling secure and authenticated boot within mobile devices without relying on TPM chips. The key features of IMASC are as follows. IMASC leverages software-based integrity measurement

software (e.g., IBM IMA[2)]), so that all executable code on the device is measured before it is loaded. Moreover, IMASC launches a new service whose sole role is to interface between the kernel and a smart card located on the device. As soon as the kernel intercepts the system calls to measure the executing binary, the measurement result is sent to the smart card to authenticate it. IMASC additionally relies on specifically designed Java applets on the smart card that emulate the extend-only functionality provided initially by TPMs solely using lightweight cryptography and counters. This ensures security in spite of an adversary who is able to corrupt/delete/modify the measurement logs stored on the device (**Fig. 1**).

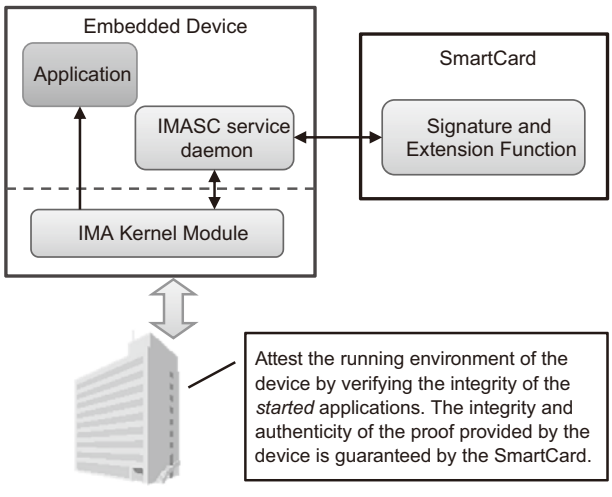

Fig. 1 Architectural sketch of IMASC.

2.2 Video Non-Repudiation

Video surveillance cameras are already widely deployed in private and public places to detect physical threats and support the investigation of criminal acts. Consequently, in legal trials, proofs of authenticity and integrity, known as non-repudiation proofs, will be required to accept the data from video surveillance as evidence. However, most existing solutions focus on verifying the digital signatures of the video stream at the network layer to authenticate the source of the video. This complicates the verification process in storage size and computation.

NEC Laboratories Europe's technology for ensuring video non-repudiation is based on the actual encoding of the video and can be recomputed easily from the data source with a minimum amount of additional meta-data. Meanwhile, our technology relies on an adapted hash tree so that the non-repudiation proof can be easily reduced to blocks, single frames, or short segments of the video according to the quality of the transmission channel (**Fig. 2**). Moreover, our technology tolerates the loss of partial data from the video; that is, even if parts

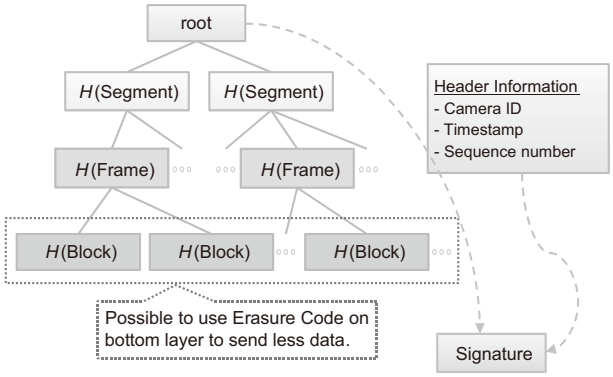

Fig. 2 Adapted hash tree on semantic video data.

of the data are lost, the authenticity of the remaining parts of the video frames can still be verified.

As an additional feature, our technology utilizes the IMASC solution deployed in the camera module to ensure that the software at the time of the creation of the video was not compromised. This provides an extra guarantee to the non-repudiation proof that the video couldn't be undetectably tampered and the digital signature was generated at a subsequent time.

3. Authorization Features

With sensors and cameras connected to a broad Internet of Things, it was important to ensure that the surveillance infrastructure was used efficiently by the various agencies. Could a camera be used by both a security agency as well as an environmental agency? Who could access the video footage and who could view an analysis of suspicious persons in an area, such as a train station?

The answer to this is in Information Governance, a key component in future safe city solutions. The Authorization Feature in the MAG1C suite is more than just a simple authentication server, but it maps out the access policy for the whole safe city system, empowering authorized government users while safeguarding the privacy of citizens.

A central server controlling access can enable users who are authorized to access more sensitive information to have it instantly, while keeping it away from users who are not allowed to see it. The key is in giving access to those who need it, and only those who need it (**Fig. 3**). The data is effectively enforced with role based access control (RBAC) for authorized access to data and information.

On a live city map, for example, only those with access can track certain persons or vehicles of interest, while others who don't have access are not even shown any content that is out of bounds. Again, the key is in giving access to those who need it, and only those who need it.

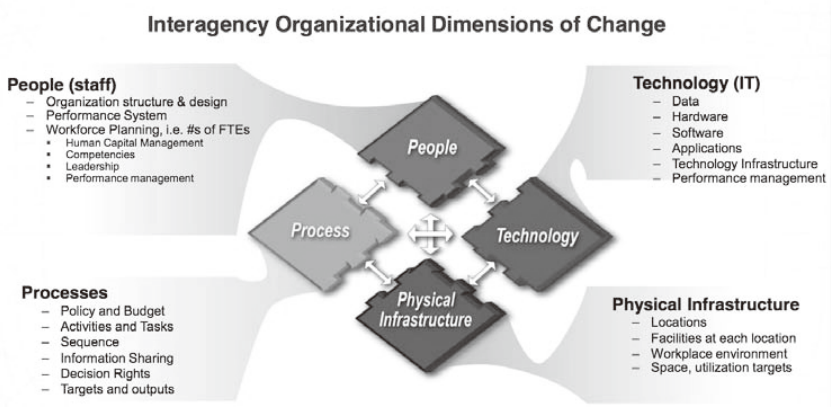

Fig. 3 Authorization and Control.

4. Conclusion

Through the secure sharing of information and raw data through the authorization and execution of governance policies, the information can be used as e-Evidence and be presented in courts. Digitally Signed Sensors' content ensures non-repudiation as device and node integrity is enforced. The integrity status of the servers, nodes, and various sensors spread around the city, whether they be fixed, mobile or ad hoc, can be monitored.

With the Information Governance in place, the different resources and information can be utilized securely. NEC's Inter-Agency collaboration solution, the MAG1C (Multi-AGencies, 1 Concert) Suite, can help the different agencies to overcome infrastructural and technical barriers, and optimize the use of manpower, and improve situational awareness and anticipation of security threats.

Reference

1) B. Parno, et al.: Bootstrapping Trust in Commodity computers In Proceedings of the IEEE Symposium on security and Privacy, 2010
2) IBM IBM 4758 Basic Services Manual Release2.45 http://www- 0 3.ibm.com/security/cryptocards/pdfs/IBM_4758_Basic_Services_Manual_Release_2_54.pdf

Authors' Profiles

Paul Wang
CTO, Head of Strategy & Management
Global Safety Division

Kang Wei Woo
Technical Director
Global Safety Division

Jens-Matthias Bohli
Chief Researcher
NEC Laboratories Europe
NEC Europe Ltd.

Joao Girao
Manager
NEC Laboratories Europe
NEC Europe Ltd.

Ghassan Karame
Senior Researcher
NEC Laboratories Europe
NEC Europe Ltd.

Wenting Li
Research Scientist
NEC Laboratories Europe
NEC Europe Ltd.

The details about this paper can be seen at the following.

Related URL:

NEC Public Safety Portal
http://www.nec.com/safety

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.9 No.1 Special Issue on Solutions for Society - Creating a Safer and More Secure Society

Vol.9 No.1
January, 2015

Special Issue TOP

NEC Information