Authenticated Component Event Reporting in VOGUE.

Nicolai Kuntze, Roland Rieke (Fraunhofer SIT),
Kai-Oliver Detken (DECOIT),Adrian Nowak (Otaris), Karsten Sohr (MRC)

March 12, 2010

Context: Collaboration between ADiWa and VOGUE

Motivation of the VOGUE project. In the last years, mobile phones and other mobile devices have become more and more our companions and belong to the working equipment of many people. In many areas of our business and private life, various activities are not possible any more without mobile phones. With this trend, a stronger complexity of systems goes along, which influences the security and trustworthiness of mobile systems. The end user expects that data and communications channels are protected from unauthorized access. Such security requirements can only be satisfied if the mobile device makes available prerequisites for securing such a channel appropriately.

However, from the perspective of service providers, operators, and manufacturers, mobile phones operate in "hostile" environments. Under some circumstances, the end users, for example, may be interested in manipulating the functionality of the device in order to commit fraud, depending on the their intentions. For example, stolen devices may copy data encrypted via SSL or VPN technology trustworthily and securely, but these data may be forwarded to an attacker by manipulated software. This way, an attack, which is interesting for industrial espionage, might be possible.

The market demands increasingly integrated solutions, which are more complex due to the challenges to be addressed. On the other hand, these solutions are subject to a strong cost pressure. Flexibility and reuse of applications and modules is an important factor here. In particular, this applies to IT security. Security as a service is an important prerequisite for reuse and quality.

VOGUE concentrates on the development of an integrated security platform which allows mobile devices to access different IT systems in a trustworthy manner such as applications spanning whole supply chains and enterprise networks. Such a platform consists of soft- and hardware. The

solutions to be implemented shall use the standards of Trusted Computing, which describe at their heart a trust anchor. VOGUE is based on the hardware properties of Trusted Computing and mobile devices and makes available a software architecture, which helps to achieve stronger trust in the devices by the service providers. The security mechanisms can be used on different mobile platforms. In particular, SMEs will have methods and tools at hand which sustainably increase trust of possible customers in novel sensitive applications by means of the results of the VOGUE project. With the help of the scenario "Mobile access of an external to an enterprise network", the increased security provided by the VOGUE solution will be proven.

Main focus and common objectives of VOGUE. The use of mobile devices (smartphones, mobile phones, PDAs) expands further and they become more frequently integrated in corporate networks. Especially security relevant business processes are operated with mobile devices (M-Business, M-Commerce) and these devices manage more often sensitive data, too. The introduction of new platforms for smartphones, like iPhone or Android Mobile Phone G1, enlarges the range of functions for mobile phones, which are now comparable to PCs. Both platforms provide the opportunity to download plenty of new applications. This increased complexity of end devices, which is at the same time linked to a higher mobility and an increased demand of greater connectivity enlarges the risk of compromising malware and targeted attack, without knowledge of the user. This can affect the availability and safety of IT-infrastructures, because security policies of various companies can be circumvented in this way. More than ever the combination of telephone and PC functionalities can cause safety risks that aren't yet adequately studied and understood. This especially applies to software of mobile devices that leads to security gaps like buffer overflows. Lately, a series of security problems has just became known in new platforms like attacks on iPhone, symbian end devices and recently even on Andriod Mobile Phone G1.

Therefore, a secured access to the IT-infrastructure through a suitable authentication is required. Furthermore the device has to be in a trustworthy condition to ensure that no malware is transferred to the network. To enforce the corresponding security rules for devices, suitable safety mechanisms have to be implemented.

In addition, supply chains and general organization scenarios are also interesting. In this context, e.g., a modern federated identity management system (IdM) can be named, in which digital identities are represented by mobile devices and where supply chain partners will automatically be announced. These "portable identity" have to be trustworthy to prevent an unauthorized user access to safety-critical applications such as ERP systems. On the other hand, a mobile device is exposed in organizational scenarios

to external attacks.

Due to the new and growing requirements that are provided for the trustworthiness of mobile devices, a platform is being developed in this project to secure these devices. In particular this safety platform will provide mechanisms for trustworthy equipment authentication.

Android - an open platform. Google Android offers an open, Linux based platform for the development of applications in the mobile domain. This, based together with the existing emulation environment, allows for an efficient development on the client side with respect to security mechanisms like TNC or the integration of Trusted Computing. The aspect of security means on the client side will form the focus of VOGUE. Through the TCG a mobile version of the TPM is specified for the mobile market, taking into account the special requirements of this particular market share. VOGUE will provide for an emulation of the expected features of such a hardware based security device to allow for the development of business cases and their demonstration.

VOGUE addresses the existing questions on security in the context of mobile and autonomous devices and will provide for a demonstration to show the potentials of security and trust enhanced devices.

Security Information and Event Management. The management of incidents and events is one of the cornerstone for any service, and is formally accepted as part of best practices in information communication and technology frameworks such as ITIL and COBIT. These frameworks are largely reactionary in nature, and one of the crucial differences to specific Security Information and Event Management (SIEM) solutions, is the ability for SIEM solutions to provide near-real time notification and the possibility for these solutions to provide proactive management of incidents and events.

SIEM frameworks collect and examine relevant events about an infrastructure and provide a unifying view about the security status of the monitored systems. Since the framework running environment is highly dynamic and potentially hostile, it can become the target of an attack, as the adversary attempts to neutralize the "sentinel" before proceeding to compromise the actual system. Therefore, resilience methods that allow the framework to operate with a high level of trustworthiness with functional and non-functional properties, depending on the operations to be supported (data collection, abstraction, aggregation, correlation, etc) are required. Some of the anticipated aspects that will have to be taken into consideration at the architecture level are: data acquisition from greatly diverse computational nodes (e.g. from small sensors); huge amounts of events requiring distributed aggregation and processing for scalability; unpredictable operational conditions due to network loading conditions, reliability and security problems;

highly resilience requirements even under attack.

Information flow defense mechanisms. Information flow defense mechanisms target at event data protection while it travels from the place where it is captured (e.g., sensor) until it arrives to the processing site. By interposing itself in the path between generation and consumption of events, the adversary can delete and corrupt passing data, disturbing and/or forging the perceived status. To address this problem, a secure and dependable event distribution, preserving temporal consistency and causal order among events, despite accidents and attacks (e.g. clock skew, timing attacks) is required. In order to support resource constraint nodes this has to be highly adaptable, and therefore employ a number of techniques such as trustworthy event tagging and event re-ordering prevention mechanisms.

Trusted Network Connect - a base for securing the events. One aim of VOGUE is, to integrate industry approaches to the attestation of event reporter states and how to integrate these measurements to gain a certain degree of trustworthiness and non-repudiation for events collected.

Using existing technologies like the upcoming Trusted Network Connect (TNC) protocol family will allow to build up the base to establish SIM data exchange. TNC is an open architecture for Network Access Control, promulgated by the Trusted Network Connect Work Group (TNC-WG) of the Trusted Computing Group (TCG). It aims at enabling network operators to provide endpoint integrity at every network connection, thus enabling interoperability among multi-vendor network endpoints.

Transfer of TNC technology to mobile phone platforms is a new aspect approached by the VOGUE project.

Authenticated Component Event Reporting. Various equipment, including the sources of event data, relevant for the operation of the overall infrastructure is placed in non-protected environments. This recent development can be observed for example in smart grids for energy distribution or approaches in the area of facility management.

It is therefore possible for attackers to acquire access to equipment with relative ease; and then initiate fake event reporting. This attack possibility is not new and well documented; but perhaps best showcased in movies featuring heists in casinos. In these movies, the robbers divert the feed of security cameras to a fake camera source thus convincing the monitoring agents that there is nothing wrong in the environment.

The aim is, to integrate industry approaches to the attestation of event reporter states and to analyse how to integrate these measurements to gain a certain degree of trustworthiness and non-repudiation for events collected.