Leveraging Trusted Network Connect for Secure Connection of Mobile Devices to Corporate Networks

Prof. Dr. Kai-Oliver Detken[1], Hervais Simo Fhom[2], Prof. Dr. Richard Sethmann[3], Günther Diederich[3]

[1] DECOIT GmbH, Fahrenheitstraße 9, 28359 Bremen, Germany, detken@decoit.de

[2] Fraunhofer Institute for Secure Information Technology, Rheinstrasse 75, 64295 Darmstadt, Germany, hervais.simo@sit.fraunhofer.de

[3] University of Applied Science of Bremen, Flughafenallee 10, 28199 Bremen, Germany, {sethmann, guenther.diederich}@hs-bremen.de

Abstract. The approach described in this paper is part of the German national research project VOGUE. VOGUE leverages trusted network connect concepts as a key to implement/design a holistic and vendor neutral network access system while addressing shortcomings of traditional network access control mechanisms. The rest of the paper is organized as follows: Section 2 provides the motivation that outlines the importance of validating mobile devices state of health before allowing access to the enterprise network and gives a brief overview of the background on Trusted Network Connect (TNC). Furthermore, the section describes the security risks, challenges and requirements that are relevant to interoperable network access control and authorization. Next, we discuss in section 4 existing solutions and other industry standards and specifications that have had an influence on our work. The paper concludes with section 5.

Keywords: Network Access Protection (NAP), Network Access Control (NAC), Trusted Computing Group (TCG), Trusted Network Connect (TNC), Trusted Platform Module (TPM), SIMOIT, TNC@FHH, VOGUE.

1 Introduction

Wired and wireless communication networks grow together and service access is becoming more and more ubiquitous, multimodal and standardized solutions are necessary. However, mobile devices and systems pose specific requirements and because of the diversity of network access technologies, the increasing numbers of services, mobile devices are more vulnerable with respect to IT-security. Reliable identification of both the user and the device itself is mandatory for authorization and authentication when requesting access to networks or services. In general, IT-based business processes demand administration and control of access privileges with automated and role-based allocation/withdrawal of user privileges – the so called “user-provisioning” und “de-provisioning”.

The Trusted Network Connect (TNC) approach addresses this issue, specified by the Trusted Computing Group (TCG) with the aim to define a common standard. Besides the more significant authentication (user and device identification), a quarantine-zone for unsecured equipment has been introduced. TNC avoids any modifications of devices and thus excludes security lacks caused by weak device configuration, security breaches in software applications and operating systems. With this framework the configuration state of devices are communicated to a dedicated server, which decides upon its trustworthiness.

The core specification has been completed and some products such as switches, routers, and VPN-gateways are already available in the market. However, a seamless integration of mobile users into an enterprise user-centric identity management system is still far from being a reality. Platform-independent solutions do not exist in the market. Authentication mechanisms and synchronization of user identities and rights are not compatible.

Especially for SMEs identity management and access is a complex issue and challenge. This target group cannot afford dedicated departments for IT-security and has to face restricted budgets and personnel resources. As mobile networking and communications becomes more complex, administration is tedious and error-prone, demanding mechanisms for central administration and configuration. The German R&D project VOGUE (http://www.vogue-project.de) has identified this problem and implemented the TNC approach partly in the form of a vendor-neutral prototype. [1]

2 Motivation and Background

Let us consider an enterprise that provides its employee, named Bob, with a mobile communication device (e.g. smartphone) running several critical business applications that he require for carrying out his job responsibilities. As mobile employee, Bob uses the firm-owned mobile device to remotely access critical components of his enterprise's network and retrieve sensitive business information remotely. In order to limit access for non-authorized users and devices, Bob's enterprise relies on a traditional network access control approach deployed as a combination of 802.1X, EAP/EAoP, IPsec and RADIUS. That scenario will lead us to the motivation of the project VOGUE, the security risks/challenges, and requirements, described in the next sub-chapters.

2.1 Motivation scenario

In order to enter his employer network, Bob first connect his mobile device to a wireless access point (AP). The latter can be either a public hotspot or one located at a foreign[1] enterprise network perimeter. By applying the foreign enterprise's and public hotspot's operator routing policy respectively, the AP relays Bob and his device through a potentially unsecured network, i.e. Internet, to his home security gateway.

[1] Any network other than Bob's employer network to which Bob's mobile device may be connected.

The AP's network control policy as well as related processes is for simplicity reasons not further discussed. The security gateway, which is designed to enforce Bob's employer network access policy blocks, by default, all traffics form devices that have not yet been authenticated. It basically blocks all traffic towards back-end components like for instance critical database servers and other services provisioning servers, except those traffics towards entities needed to establish trust, e.g. AAA server. The mobile device then authenticates to the security gateway by sending it all necessary security parameters including Bob's identity attribute (user name and correct password) as well as his smartphone credentials. These security parameters are then relayed to relevant back-end validator entities (e.g. AAA server), which proceed to determine whether Bob and his smartphone are compliant with the enterprise's policy requirements. If the compliance check is successful, i.e. if user and device along with their respective attributes (e.g. identity and role in the company) are authentic and allowed to access company critical servers, then the back-end validators instruct the security gateway about access rules and conditions to be enforced. Finally, the gateway provides the smartphone with the enforced access decision. An example of such a decision might be the establishment of a secure VPN-connection between Bob's mobile device and one of his company critical services provisioning servers.

However, since the employer, being the owner of the smartphone, might also allows Bob to use the device in foreign networks (e.g. while working from a partner's premise) and perhaps install applications that he need for his daily use, it wants to be able to validate access to its network based on the smartphone's state of health and security. It thereby wants to mitigate potential threats posed to his network infrastructure by getting assurance about the mobile device integrity and the fact that there is no malware-infected application running on it.

2.2 Security risks and challenges

Regarding the described scenario we have the following security risks and challenges:

a. **Endpoints misconfiguration**: Traditionally, enterprises deployed NAC solutions relying on strong isolation of network segments by means of firewalls and routers. Dedicated routers are configured to perform simple network packet filtering while the firewalls deployed as proxies performed more fine-grained filtering or allow the setting of a "demilitarized zone" (DMZ). However, firewalls configuration might contain errors and even well configured firewalls can be circumvented. On the other hand, vulnerable networked devices (incl. smartphones) posing huge security threats to the overall enterprise information and communication technology are typically secured by means of patching of their OS, update or by installation of latest versions of security software. The challenge here is related to the difficulty and cost of patching, updating and managing security patches manually, especially when non-security aware employees (re-)introduce infected mobile devices into the enterprise network. Moreover, the ubiquitous nature of smartphones makes it hard the kind of automatic, continuous and

centralized management required for a broader and secure adoption of smartphones as endpoints in enterprise network infrastructures.

b. **Open and ubiquitous nature of mobile endpoints**: the growing popularity of smartphones is attracting more and more enterprises to deploy them as integrated components of their enterprise network. Designed as open and programmable-networked embedded devices, smartphones are used by mobile and external employees to access and manage critical business data in a ubiquitous way (see section 2.1). This fact has introduced new technologies and new security challenges to the urgent need for machine-to-machine identification and authentication, and cross-layer network access authorization. Machine level platform-authentication is crucial for the security and authorization of network-access requests at both layer-2 and layer-3. Furthermore, due to recent attacks at the higher layers (e.g. attributable to the increasing number of smartphones malwares) a major problem that needs to be addressed is that of achieving integrity of mobile endpoints. The problem of endpoint integrity concerns in our case the trustworthiness of the smartphones and that of enterprise servers with regard to their respective integrity states, including their identities. By the term integrity, we understand relative purity of the smartphone platform from software (and hardware) that are considered harmful to the phone itself and others with whom it interacts. The growing number of smartphone malwares best exemplifies this problem for corporate networks. As illustrated in the motivation scenario, today employees connect their mobile devices to unsecured networks, at home or when they are away on business, often resulting in malware being inadvertently downloaded onto the smartphone. When (re-) connected to the corporate network, the device becomes a distributor of the malware to other devices on the enterprise network. [2]

2.3 Security requirements

For the aforementioned scenario and with regard to the security risks and challenges described above, we define the following requirements:

a. **Backward compatibility and scalability:** it is not reasonable to build an entirely new NAC solution that does not interwork with already existing solutions, industry standards and open specifications. Therefore, proposals for a new NAC system have to be interoperable systems leveraging a number of existing and emerging standards, products, or techniques such as IEEE 802.1X and/or others. Moreover, a new NAC system should provides features required to guarantee good scalability and performance especially for large-scale enterprise environments, e.g. centralized configuration and policy management. The complexity of maintaining such a deployed NAC system should be reasonable.

b. **Enterprise's network security policy should be reliably enforced**: additionally to user and device credentials, the mobile endpoint's state of health and security should be considered for validation during the access

control and authorization process. Validation rules and conditions specified as technical security/ integrity policy have to be reliably enforced. Such a policy might require the presence, status, and software version of mandated applications, and the OS patch level of the mobile device. Reassessment methods are required to enforce post-admission control, i.e. revalidation, at regular time interval, of mobile device platforms that are already admitted to the enterprise network.

c. **Isolation and automatic remediation:** in order to provide flexibility with regard to the isolation of critical enterprise networked resources from less critical ones, mobile devices should be reliably isolated and quarantined from the rest of the network if they fail to meet the security policy requirements for endpoint compliance. If allowed, smartphones and employees redirected to a quarantine zone should be provided with necessary security updates, helping them becoming compliant. In order to reduce the effort for performing such a strategy, especially in large-scale enterprise, the remediation process has to be automatic.
d. **Endpoints platform authentication:** NAC mechanisms should enable mobile devices and employees to reliably detect rogue access requestors and rogue security gateways respectively. Furthermore, the proof of identity of communication endpoint (smartphones, access point or back-end servers) and the assessment of platform integrity of those devices have to be reliably verified.
e. **Support of federation of trust:** since corporations defined different network access control and authorization policies, methods are required for exchanging security attributes and integrity information about a mobile device and about the employee associated with it across enterprises' security domains. This is an important requirement considering corporation boundaries becoming more elastic and mobile devices roaming between different corporations' networks.
f. **Usability:** NAC solutions should be designed while keeping both network administrators and end users' (employees) conveniences in mind.

2.4 Trusted Network Connect (TNC)

With the TNC specification, the TCG developed an open and vendor-neutral specification for the integrity check of communication endpoints, which requests access to a resource. The architecture supports existing and well-established security technologies such as VPN, 802.1X, Extensible Authentication Protocol (EAP) and RADIUS. The TCG's TNC offers hardware support by means of the Trusted Platform Module (TPM), so that e.g. the accuracy of the platform integrity information used in the network access control process is guaranteed. Built in desktop PCs and notebooks this integrated chip protects data on a hardware level. Together with 802.1X, it guarantees the TNC architecture, so that solely certificated (digitally signed) application software may be used. Furthermore, this technology uses an authorization token (e.g. a X.509 certificate), which is communicated together with the client status

information. These are being validated at the target system against policy conformity. Access management relies on client identity and system status.

The architecture of TNC should be divided into three main areas:

a. **Access Requestor (AR):** contains a Network Access Requestor, the software that is used by the client to connect to the network – an 802.1X supplicant, a VPN client, or similar. The Access Requestor also contains a TNC Client (software that manages the overall NAC process) and Integrity Measurement Collectors (IMCs, plug-in software modules specialized for reporting the status of anti-virus software, patches, or other things).

b. **Policy Decision Point (PDP):** contains a Network Access Authority, software that makes the final decision on whether network access should be granted. The Policy Decision Point also contains a TNC Server (software that manages the NAC process on the server) and Integrity Measurement Verifiers (IMVs, plug-in software modules that compare reports from IMCs against policy, supply access recommendations to the TNC Server, and send remediation instructions to the IMCs).

c. **Policy Enforcement Point (PEP)**: PEP is responsible for the assessment of the Integrity Measurement Collectors (IMC) and the TNC client measurement data. PEP doesn't have any internal components. The TNC server will do this work.

The following diagram illustrates the TNC architecture, as specified in [2]:

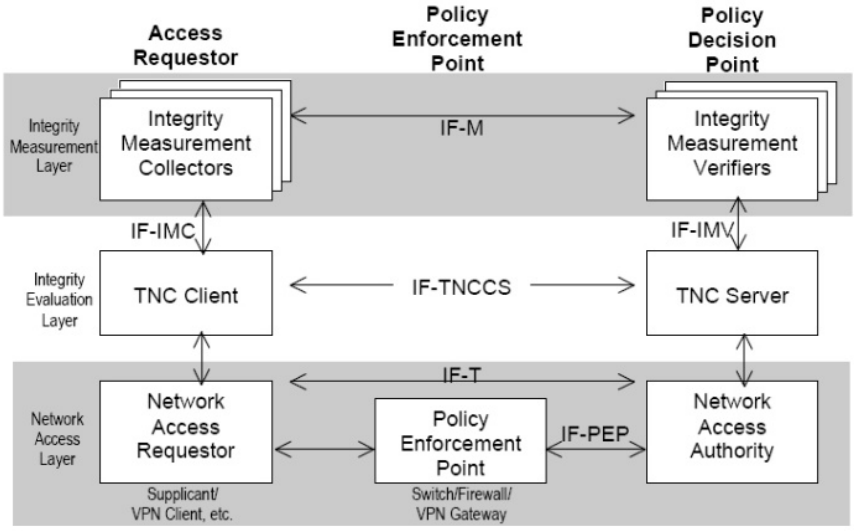

Fig. 1. TNC architecture overview.

The interfaces of TNC are really vendor-independence. Every component in the TNC architecture has been implemented by multiple vendors and these products have been tested to ensure they actually work together. Customers retain full choice and are not tied down to any one vendor. Similar but proprietary approaches are NAP from Microsoft and NAC from Cisco Systems. [2]

3 Related Work

Endpoint security solutions are being implemented in routers, switches, WLAN access points, software and security appliances. Authentication and authorization information of mobile devices are being communicated to a policy server, which decides if the device may have access or not. Furthermore, an access protection enables a state check („health check“) of the client. Such a check typically consists of requests for specific information about the client platform. Some of the gathered data is e.g.: version of the anti-virus software, configuration of the personal firewall, and of other software, and the patch level of the device (also of the operating system). In case that the client does not fulfil the security policy, it can be isolated into a dedicated VLAN with a consecutive „decontamination“. [3]

Beside the licensed software products, “Cisco Network Admission Control (NAC)” and “Microsoft Network Access Protection (NAP)”, an open source solution exists: “Trusted Network Connect (TNC)”. For this solution, some projects implemented their own approach, like SIMOIT (http://www.simoit.de) and TNC@FHH (http://trust.inform.fh-hannover.de).

3.1 Network Access Protection (NAP)

Microsoft‘s Network Access Protection is similar to the TNC functionality. However, the nomenclature of the components varies (NAP client = TNC client, TNC server = Network Policy Server (NPS), Integrity Measurement Collector is comparable to SHA (System Health Agent), and the task of the Integrity Measurement Verifier can be dispatched by the System Health Validator). [6]

Similar to the TNC technology, NAP addresses the following aspects:

a. **Validity check of network policies:** The validation of the mobile devices against policy conformity such as the current patch level of the operating system.
b. **Fulfillment of network policies:** Updating mobile devices, so that they meet the security policies (in an isolated quarantine network segment).
c. **Network access:** After a positive authentication validation and policy validation, access to the network is granted.

Through the so called “Statement of Health”-protocol interoperability between TNC and NAP is given. Furthermore, a licence agreement between Cisco and Microsoft allows NAP clients to communicate with both the “Statement of Health” protocol and the Cisco Trust Agent protocol. [5]

3.2 Network Admission Control (NAC)

Cisco’s Network Admission Control is a further architecture, which can be compared with TNC. It is an “Enforcement and quarantine technology on API level”, which is integrated in the Cisco network infrastructure. Here, the trusted module “Cisco Trusted Agent” is used for user authentication and authorization. It is implemented in the mobile devices and in Cisco routers and switches. [7]

A prerequisite for using the NAC framework architecture are the following Cisco components: [5]

a. **Trusted Network Agent:** Collects information from the clients, which NAC applications are installed. These information are sent to the Network Access Device (NAD) on request.
b. **Cisco Secure ACS:** Acting as policy server, it checks the information coming from the Trust Agent and determines the access privileges of the clients, and sends this information to the Network Access Devices (NAD).
c. **Network Access Devices (NAD):** This is a Cisco device (switch, router, VPN concentrator or access point) supporting Network Admission Control and defining the client access privileges based on the information received from the Cisco Secure ACS.

3.3 SIMOIT

According to the requirement specifications to mobile devices and the application scenarios of the pilot-user the project SIMOIT (http://www.simoit.de) specified the architecture and implemented a prototype, which evaluated the TNC approach. The core element of the prototype platform is represented by the Mobile Security Gateway (MSG), consisting of different modules (VPN, firewall, TNC, RADIUS, and LDAP). Here, for the sake of an openness and flexibility, mainly open source solutions have been selected. [1]

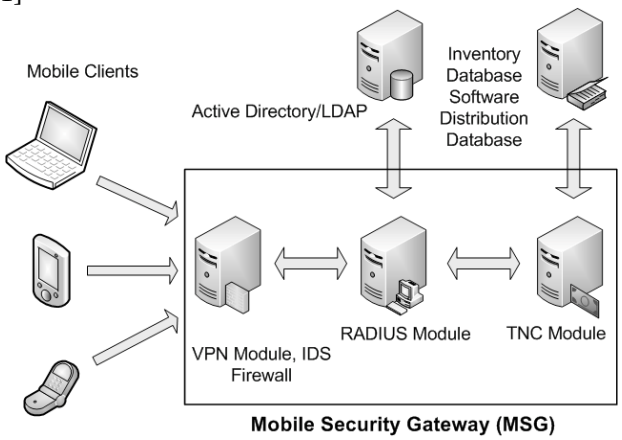

Fig. 2. Overview of the modules of the SIMOIT system.

SIMOIT is able to interact with unmodified clients having a standard configuration, whereas complete TNC-architectures require software-agents and integrity measurement collectors on the client-side. SIMOIT aimed at the development of a mobile IT security platform for heterogeneous environments using standards. The method and solutions developed in this project can be deployed for IT infrastructures in small and medium sized enterprises. The essential aim was to develop a modular and vendor-neutral system.

According to the requirements and the application scenarios of the pilot user SIMOIT realized a development and test platform, which evaluated the TNC methodology. The main platform is represented by the Mobile Security Gateway (MSG) as mentioned before. The project specifically evaluated open source software projects and methods with the aim to realize a standard solution. At the same time, SIMOIT paid high attention to flexibility, so that typical security components such as firewalls can be integrated as well. In this case, instead of using the SIMOIT module an interface was provided. Also, it was stipulated that existing inventory databases can be interconnected in order to retrieve software versions and patch levels. The pilot user required the interconnection of an Active Directory Server (ADS), which made it necessary to develop an interface via LDAP. Through this, all user profiles crucial for authentication can be retrieved, and routed to the Mobile Security Gateway (MSG).

For the sake of high flexibility, SIMOIT mainly focused on a server-side solution. The reason for this is the fact, that in the future mobile device vendors will provide their own access software. Hence, on the server side any TNC implementation can be customized.

3.4 TNC@FHH

The TNC@FHH approach (http://trust.inform.fh-hannover.de) is also an open source implementation of the TNC architecture for integrity check of mobile devices. In order to enable an open and standardized implementation, open source software has been analyzed. As in the SIMOIT project the TNC@FHH approach allows integration of conventional security components such as firewall systems. A further precondition was to develop a framework based on the IEEE 802.1X standard in order to be used in Ethernet-based network environments.

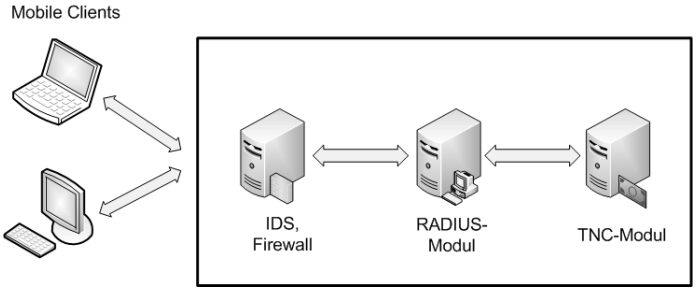

Fig. 3. TNC@FHH implementation.

The realization of the project bases on two essential and separated software packages. On the client-side specific IMCs have been developed, which analyze and communicate the current security status of the systems. This critical information is communicated to the IMV residing on the RADIUS/TNC server and validated against the security policy. After the evaluation has been accomplished and the mobile device meets the requirements, the RADIUS server sends an access-accept notification to the Network Access Server (IEEE 802.1X compatible switch or router), which then grants the client the respective network access.

4 The VOGUE approach

Until now transferring the TNC approach to mobile phones has not been the subject of R&D projects. It is a favourable point in time to realise such a project, because modern mobile platforms such as Android and iPhone OS, now permits application development on mobile devices, thus enabling the security components for TNC and the integration of a root-of-trust on smartphones. Such a root-of-trust is capable of vouching for the integrity of the platform, collecting and reporting the device platform configuration to a challenger in a trustworthy manner. This aspect is one of the core themes of VOGUE project. Such a root-of-trust for mobile systems, named Mobile Trusted Module (MTM) 0, which is a modified version of the TPM, has been specified by the The TCG Mobile Phone Work Group and will soon be introduced into the market. A software emulator 0 also used in VOGUE has being developed to allow the development of products for this emerging security technology.

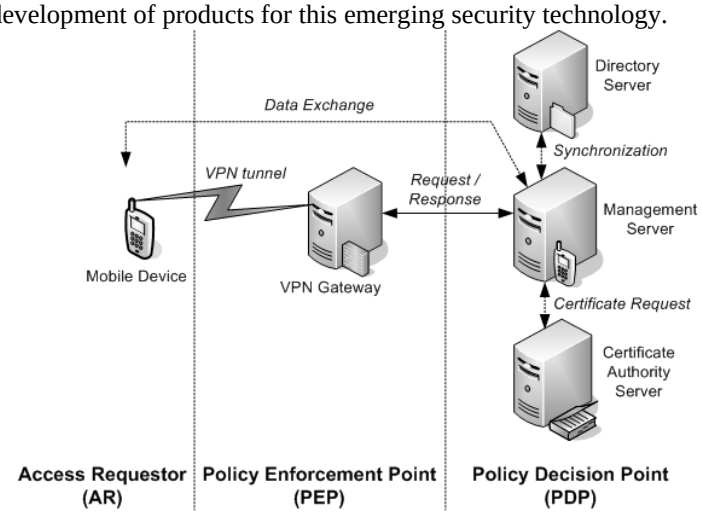

Fig. 4. VOGUE platform overview.

According to the scenario and requirements discussed above, the project VOGUE specified the following platform assumption for the first prototype. The core element of the platform is represented by the VPN gateway. Additionally, a management server (e.g. RADIUS), a directory server (e.g. LDAP), and a certification authority server is necessary. In the first step, the user has to be identified for the correct access with the VPN gateway. All criteria are available on the directory server and assign the user to different profiles and user groups.

Each user group has different security policies for different access rights. The management system synchronizes continuously in intervals the user information with the directory server. That includes that user from the directory server with VPN access rights, if they are not yet available on the management server, will synchronize with all user group membership automatically after one interval. As an option a public certification authority (CA) can be adapted. If a new user is created on the management server, a certificate will apply. The management server platform is then a registration authority. The VPN gateway has to be configured that all requested

clients will be authenticate via the management server. Therefore, the gateway site does not need adaptations for new user. That will be done automatically by the communication with the management server.

Next to the authentication of the user, the smartphone platform (hardware and software configuration) is checked according to the enterprise TNC's requirements. After the establishment of a VPN connection, the network access of the mobile device is limited to the quarantine zone. Within this area, it is only possible to update software components of the mobile device like anti-virus-software or operating system patches. The access to other network areas of an enterprise network is forbidden. Information about the status of the mobile device is available by the access requestor (AR) on the client-site. The AR includes the network requestor (as a component of the VPN client), the TNC client (as an interface between the network access requestor and plug-in software), and the integrity measurement collector (describes the plug-ins which allows different software products like antivirus software to communicate with TNC).

In detail, the following points will initiate for a mobile device communication (also depicted in figure 5):

1) A VPN connection is established.
2) The management server (TNC server) initializes an integrity check.
3) The mobile device (TNC client) collects integrity measurements (IM) information using the local Integrity Measurement Clients (IMC) on the mobile device.
4) The management server (TNC server) forwards the IM information for a check to the integrity measurement verifier (IMV).
5) The Integrity Measurement Verifier (IMV) checks the IMs and sends the results with a recommendation to the management server (TNC server).
6) The management server (TNC server) takes access decision und forward this information to the VPN gateway (PEP) and the mobile device (AR).
7) The VPN gateway (PEP) allows or does not allow the access to the network for the mobile device (AR).

Summarized, the integration of the MTM allows a further check of the software components on the mobile device. This simplifies the detection of rootkits. Furthermore it is possible to sign and encrypt messages with key material of the MTM. That means a strong security check of the origin of the information.

5 Conclusions

The TNC approach within VOGUE presented in this paper is a viable solution to raise the security level in mobile networks. Though the core specifications are already accomplished and various network components are available on the market, there are still shortcomings and manufacturers differ in their approaches. With Microsoft‘s “Statement-of-Health Protocol” future interoperability can be reached, but Cisco Systems will go its own way and will not be interoperable with the standard.

The projects SIMOIT and TNC@FHH are based on TNC too, but include only the server-side implementation of the standards. The TNC approaches of both projects

presented in this paper are different, but are similar trusted computing implementations for mobile scenarios. They allow a relatively high security level for mobile and scalable identity and access management. Both platforms are modular, extensible, and can be combined with conventional security components such as VPN and firewalls.

The VOGUE project will improve existing TNC approaches with own developed TNC clients for mobile operating systems (e.g. Android) in order to extend the applicability beyond laptops or notebooks, since smartphones are widely used in corporate networks. With this work, it is hoped, that the integration of smartphones for "Trusted Computing" will bring the TCG initiative one step further in the development and standardization process.

6. Acknowledgements

The project VOGUE (http://www.vogue-project.de) is fund by the Federal Ministry of Education and Research (BMBF) of Germany. The project started in October 2009 and will end at September 2011. The authors would like to thank the BMBF for their support. We also wish to express our gratitude and appreciation to all VOGUE partners for their strong support and valuable contribution during the various activities presented in this paper.

References

1. Detken, Gitz, Bartsch, Sethmann: Trusted Network Connect - sicherer Zugang ins Unternehmensnetz; D.A.CH Security 2008: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven; Herausgeber: Patrick Horster; syssec Verlag; ISBN 978-3-00-024632-6; Berlin (2008)
2. TCG, Trusted Network Connect Architecture for Interoperability; Specification 1.3; Revision 6; April (2008)
3. Nispel, M.; Enterasys Secure Networks: Was Sie über NAC wissen sollten; http://www.computerwoche.de/knowledge_center/security/1871427/index.html
4. Eren, E., Detken, K.-O.: Mobile Security - Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit. Carl Hanser Verlag. ISBN 3-446-40458-9; München Wien (2006)
5. Eren, E., Detken, K.-O.: Identity and Access Management according to the implementation of the SIMOIT project and TNC@FHH. International Journal of Computing, ISSN 1727-6209, Ukraine (2010)
6. http://www.infowan.de/index.html?windows_2008_profvogl2.html
7. Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)
8. TCG, TCG Specication Architecture Overview v1.2, page 11-12. Technical report, Trusted Computing Group (April 2004)
9. TCG Mobile Phone Work Group, Mobile Trusted Module Overview Document, 2006
10. Strasser, M., Stamer, H., Molina, J.: Software-based TPM Emulator, http://tpm-emulator.berlios.de