IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
21-23 September 2009, Rende (Cosenza), Italy

User Centric Identity Management in Mobile Scenarios: The SIMOIT Project

Prof. Dr.-Ing. Evren Eren[1], Stephan Uhde[2], Prof. Dr.-Ing. Kai-Oliver Detken[3]
[1] FH Dortmund, FB Informatik, Emil-Figge-Straße 42, D-44227 Dortmund,
eren@fh-dortmund.de, http://www.fh-dortmund.de
[2]FH Dortmund, FB Informatik, Emil-Figge-Straße 42, D-44227 Dortmund,
uhdes@stud.fh-dortmund.de
[3] DECOIT GmbH, Fahrenheitstraße 9, D-28359 Bremen,
detken@decoit.de, http://www.decoit.de

Abstract **- This paper considers some of the identity and access management mechanisms, and adds to this the new requirements posed by identity management in mobile ubiquitous environments. The authors present the state-of-the-art in identity management standards and initiatives in the context of the SIMOIT project. Furthermore, the paper discusses the results achieved by the SIMOIT-prototype implementation with respect to the generic requirements in different scenarios.**

Keywords **- Identity and Access Management, TCG, TNC, TPM, SIMOIT project.**

I. INTRODUCTION

Transparent and centrally controlled identity and access management (IAM) gains significance in future networks and services, particularly in mobile scenarios. As 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 number of services (but also fraudulent service usage), mobile devices (and the users as such) 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 R&D project SIMOIT (www.simoit.de) has identified this problem and implemented the TNC approach partly in the form of a vendor-neutral prototype. [1]

II. IT-SECURITY FACTORS

IT-Security is a basic need in enterprise infrastructures and a significant issue. Increasing vulnerability implying economic damage defines the needs 'active management of IT security'. Besides confidentiality and availability, a comprehensive security approach essentially bases on the following factors:

1. **Access control:** This mechanism involves the spectrum of tools that are used to manage digital identity with respect to accessing networks and resources such as computers, servers, printers, and software services. In general, access control is coupled with authentication methods, verifying the authenticity of users and their privileges, e.g. by means of EAP (Extensible Authentication Protocol). A successful authentication is followed by the authorization which determines to which

resources and services a user may have access to.

2. **Integrity:** This comprises measures ensuring that protected data cannot be altered during processing or transmission. The main objective is to ensure correctness and completeness of data. Both data itself and hardware/software must be protected from unauthorized access. The use of cryptographic hash functions ensures the integrity of sensitive data. It cannot prevent an alteration of data, but it can detect such an alteration.
3. **Originality (authenticity):** Important factors that describe this term in the field of IT security are originality/authenticity of sensitive data, correct identification of the sender as well as the proof that the information has not been manipulated on its way to the addressee or that no copies have been made without the sender's knowledge. Authentication is used to determine the identity of a user or a device for the sake of access control.
4. **Authorization:** This is a privilege owned by a user, device, or application/service defining who is allowed to effect certain actions within a network or which system resources may be used.

III. ENDPOINT SECURITY

The growth of the Internet IP infrastructure in the last few years has introduced new technologies and new security challenges. One of these security challenges concerns the increasing need for machine-to-machine identification and authentication, and network access authorization at the IP layer, in addition to the usual user authentication. 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 the increased attacks at the higher layers (e.g. viruses and Trojan horses) a major problem that needs to be addressed is that of achieving endpoint integrity.

The problem of endpoint integrity concerns the trustworthiness of two communicating endpoints (e.g. client and server) with regard to the integrity conditions of the two endpoints, including their identities. By the term integrity we understand relative purity of the endpoints of software (and hardware) which is considered harmful to the endpoint itself and others with whom it interacts. This problem of harmful software is best exemplified by the growing number of viruses and Trojan horse attacks on corporate networks. Many employees today connect their mobile devices (e.g. laptops, PDAs) at home to the open Internet, often resulting in malware being inadvertently downloaded onto the device. When connected to the corporate network, the device becomes a distributor of the malware to other devices on the Enterprise network. [2]

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 fulfill the security policy, it can be isolated into a dedicated VLAN with a consecutive „decontamination“. [3]

Beside the licenced software products, “Cisco Network Admission Control (NAC)” and “Microsoft Network Access Protection (NAP)”, an open source solution exists: “Trusted Network Connect (TNC)”.

Above mentioned technologies support secure authentication based on IEEE 802.1X. This comprised device identification at the switch port. Such an authentication requires respective functions on switch side, of the clients, and of a local authentication unit (e.g. a RADIUS server). A further solution is MAC-based authentication. Here, the same infrastructure is being used like in 802.1X. However, certificates and/or credentials are obsolete. The switch uses the MAC addresses as substitute for the user name (credential) and compares this against the RADIUS server. In 802.1X-supported networks this method can be used for architectures without “802.1X supplicants”. The web-based authentication rolls the device registration to a web portal, on which the user can log in. Hence, device and system registration can be accomplished without any specific conditions. [4]

IV. USER CENTRIC IDENTITY MANAGEMENT

User-centric security requires new ways of role- and context-based authentication and authorization, which is also denoted as Identity Management – a central topic in the security industry. Definition of Identity Management varies. Novell defines it as something that “allows you to integrate, manage and control your distributed identity information, so you can securely deliver the right resources to the right people – anytime and anywhere”. Microsoft defines it as combining “processes, technologies and policies to manage digital identities, and specify how they are used to access resources”.

Identity Management comprises the spectrum of tools, which allow the representation and administration of digital identities. Access management represents the centralized authentication and authorization for network resources provided. This functionality is also denoted as Extranet Access Management (EAM). Main idea of IAM is the improvement of provisioned services, and thus a consistent access of resources. The user authentication is realized based on 802.1X. Here, user identities and privileges are validated. Normally, an authentication server (e.g. RADIUS server) is responsible the authentication process.

In order to realize a standardized authentication

method, the 802.1X standard has been created. It aimed at providing a secure platform for user authentication. Essentially, it is based on the Extensible Authentication Protocol (EAP). 802.1X offers a mechanism for access authorization for users at their endpoints. It is a access control protocol operating at port level using numerous authentication methods. It does not provide user authentication. However, it translates authentication messages of the chosen method into other message formats. 802.1X is also a port-based access control method, which offers authentication at higher levels between a client and authentication server.

A. Trusted Network Connect (TNC)

With the Trusted Network Connect (TNC) specification the Trusted Computing Group (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. TNC offers hardware support by means of the Trusted Platform Module (TPM), so that e.g. only certified (digitally signed) software is allowed on a system.

The TCG standard is based on the Trusted Platform Module (TPM). 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. This work will be done by the TNC server.

The following diagram illustrates the TNC architecture.

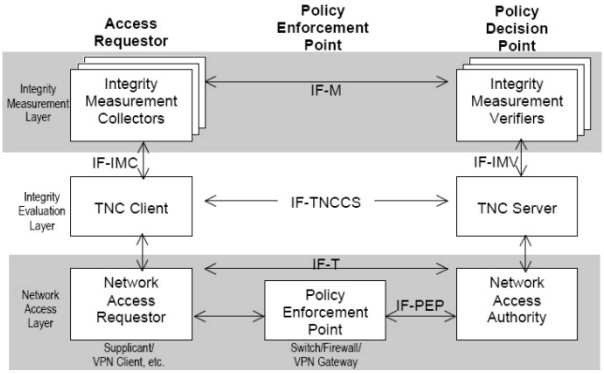

Fig. 1. TNC architecture overview.

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]

B. 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 im May 2007, 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]

C. 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.

V. THE SIMOIT APPROACH

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]

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.

A. Technical Platform

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) comprising different modules such as VPN, firewall, TNC, RADIUS, and LDAP. 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 justification 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.

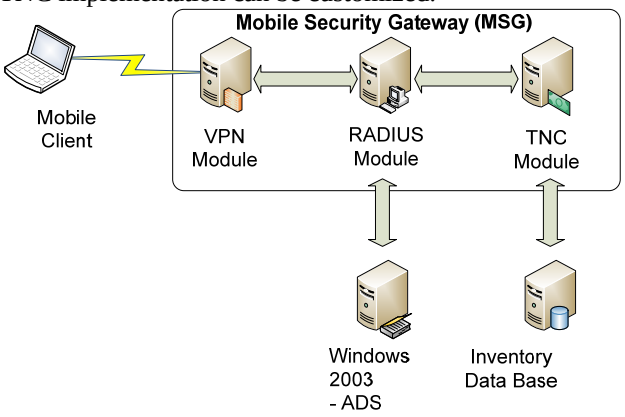

Fig. 2. Overview of the SIMOIT system modules.

The communication workflow in SIMOIT is as follows:

a. **Model 1** (a user tries to connect to the corporate network via remote access): At first, a user authentication is carried out. Based on the data from the software distribution system the mobile device of the user is placed to the quarantine zone. The user has only access to software updates. If he requests access to an internal server, a VPN connection is established automatically, and the VPN module sends a „RADIUS Access Request" tot he RADIUS module. Then, the RADIUS module carries out an authorization request by means of a „LDAP Request" to the Windows 2003 Server. Now, the TNC module sends a query to the inventory database if any critical software packages do exist. Authentication via RADIUS relies on classical user credentials (username and password). The RADIUS module sends back all necessary firewall settings to the VPN module and applies the firewall rules.
b. **Model 2** (a user tries to connect the corporate network via remote access after updating of his system): The software distribution system informs, that the device is up-to-date and the user is granted full Access to the corporate network.
c. **Model 3** (a hacker or the legitimate user

compromises the mobile device): The mobile device obtains full access to the corporate network, and an attack it. Now, the Intrusion Detection System (IDS), which is integrated in the VPN module, is being applied. The IDS detects the attack and prohibits all further access requests.

B. Mechanisms of the quarantine zone

The status of the client is crucial for integrity. The following components on the client are integral parts of the SIMOIT system:

- **Integrity Measurement Collectors:** Capture the current status of the system for specific parts such as the antivirus software level.
- **TNC client:** Collects information for the TNC server.
- **Network Access Requestor:** Connects the client with the corporate network for the VPN. In the authentication phase it provides the channel for transmission of state information to the TNC server, and the security policy to the TNC client.
- **Software Distribution Client:** In case that the client does not fulfill the requirements, the TNC client allows to install new software packages according to the security policy.
- **Software and Data Receiver:** Receives notifications about new software versions and up-to-date security policies in order to automize the software asset management. Furthermore, this component retrieves software packages and provides them for installation, when instructed by the Software Distribution Client.
- **Software Installation:** After the call of installation packages automated installation processes provide a load as low as possible of the end-user.

The current security policy is ready for receiving from the enterprise network. If the installation of the mobile secure client is carried out with the connection to the enterprise network, the current version of the security policy is loaded directly. Alternatively, a first VPN connection to the enterprise network must be established. If no security policy was used till now, the check of the reliability of the mobile system fails and so the software version also probably is not sufficient. However, the secure client can get and use the security policy in the quarantine area so that at the next connection with the VPN server a full access to the enterprise network can be made possible.

For the check of the client condition regular secure applications and their condition (e.g. actuality of virus definitions) will be analysed according to the security policy software versions and installed software. TNC Integrity Measurement Collectors delivers component-specific status information which are collected by the mobile secure client. It can be made sure that this condition check comes like the check of the authorization server to an identical conclusion.

The conditions of the clients are checked during the authentication on server side. If these is not sufficient, corresponding software packages are provided, which lead to achieving the required conditions. The mobile secure client is responsible for the compliance with the secure guidelines of the enterprise. These are formulated in the security policy and describe in which condition the mobile device must be to get access to the enterprise network. The security policy contains information, such as necessary software with its versions and safety applications to be started. The software distribution is used if mobile clients are stopped by the security policy update or after the rejection of the current system state for installing software packages. A distribution platform has the software packages to be distributed currently ready, so that mobile clients can call these by HTTP under the addresses indicated in the security policy. The access is possible at connectivity to the enterprise network or at an existing quarantine VPN connection.

As conclusion, SIMOIT is able to work with the TNC approach on server-site without software installation on client-site. Therefore, SIMOIT is open and flexible for further standard extensions and interworking with other 3rd party software.

C. Implementation

The implementation of the hardware platform has been realized with four servers. Two of them are responsible for the dial-in procedure and the other for authentication (user data and software status of the mobile device):

a. **VPN gateway:** is the end-point of IPsec and use X.509 certificates for the mobile devices. The IPsec tunnel will be established by the combination of L2TP and PPTP authentication. Additionally the certification ID of the VPN tunnel will be determined and with the authentication data forwarded to the RADIUS server.
b. **RADIUS server:** is responsible for the authorization and authentication of the user and the mobile devices. The server decides by the answer of the TNC module, if the dial-in client will get a full-access or will be forwarded to the quarantine zone.
c. **Windows 2003 active directory server:** The user data can be hold into an active directory or LDAP directory. This user data will be queried from the RADIUS server.
d. **Software distribution server:** the software distribution server knows which software packets are available for the mobile devices and which patches are necessary to reach the internal network. This information will be checked by the RADIUS TNC module of SIMOIT.

The TNC module of the SIMOIT project is a FreeRADIUS (www.freeradius.org) module. It is used as server component of the TNC system and decided as PDP by the incoming data of the Inventory Integrity

Measurement Validator (Inventory-IMV) in which network the mobile device will be forwarded (internal network or quarantine zone). FreeRADIUS and the Inventory-IMV are extended with the TNC server, including the open source library "libtnc".

The TNC implementation in SIMOIT focused only the server-site. The RADIUS server gets on demand status information from the TNC module. The module can use different validators with dynamical configuration for the status inquiry. The implementation includes the validator Inventory-IMV, which sends a request to the inventory database regarding the software status of the mobile devices. After that the server compares both information to find a decision if software updates are necessary or not.

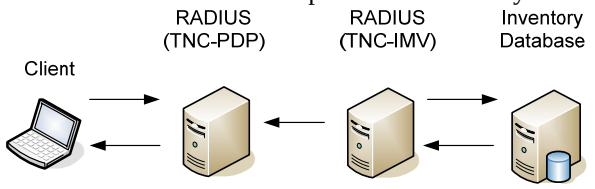

Fig. 3. TNC communication within the prototype of SIMOIT.

The Inventory-IMV was implemented with help of the HTTP(s)GET/XML method. The following requests are supported:

a. **Software packets:** The used HTTP-URI is described as "inventory/packages". As response the servers sends a XML data structure, which includes different software packets.
b. **Software status on the mobile device:** The used HTTP-URI is described as "/inventory/device/[device-id]/packages". As response a XML data structure will be sent too.

By the status code the following can be recognize: successful transmission (code 200), failure (code 404), and non-reachability of the inventory server (code 503). This request will ever send if a mobile device wants to dial-in into the infrastructure.

The database SQLite has been used for the packet management regarding the current software status. All end-devices are available within this database, with the parameters MAC address, serial number, device ID). Furthermore the installed software basis (software ID and status ID) is available. SIMOIT can use different software distribution solutions. But there is an adaptation necessary, because every software distribution works different.

As directory service it can be used LDAP or Active Directory (AD) from Microsoft. If AD will be used the schema must be adapt regarding the assignment of the network access, because the AD attributes offer no network choice. If the software patch status will checked positively, the TNC module changes the attribute and forwards this information to the AAA module and VPN module. The VPN module changes the firewall rules for the requested client and makes the access to the internal network possible.

VI. CONCLUSIONS

The TNC approach within SIMOIT 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. However, only few users and companies have the necessary know-how in the TNC area.

SIMOIT is based on TNC and the server-side implementation of the standards. Device integrity relies on existing infrastructure assets. Its modular approach allows integration of vendor-neutral solutions such as VPN gateways or firewalls with TNC support. In the future, it is planned to implement TNC clients on the devices, so that any operating system can be used. At the moment, we are still in the development phase after the founded duration of the project, which requires proprietary systems.

ACKNOWLEDGMENT

The project SIMOIT (www.simoit.de) has been funded by the city of Bremen during the time of the years 2007-2008. The authors wish to acknowledge the city of Bremen for their support. We also wish to acknowledge our gratitude and appreciation to all SIMOIT 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 TNC Architecture for Interoperability; Specification 1.3; Revision 6; April 2008
[3] Markus Nispel; Enterasys Secure Networks: Was Sie über NAC wissen sollten; http://www.computerwoche.de/knowledge_center/security/1871427/index.html
[4] Evren Eren, Kai-Oliver Detken: Mobile Security - Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit. Carl Hanser Verlag. ISBN 3-446-40458-9; München Wien 2006
[5] K.-O. Detken: Trusted Network Connect - die sichere Einwahl mobiler Mitarbeiter ins Unternehmen; Handbuch der Telekommunikation; Deutscher Wirtschaftsdienst; 129. Ergänzungslieferung von April; Köln 2008
[6] http://www.infowan.de/index.html?windows_2008_profvogl2.html
[7] http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/412/cam/m_intro.html
[8] Trusted Computing Group, TCG: https://www.trustedcomputinggroup.org/home/