Mobile Identity Management auf Basis des SIMOIT-Projekts und der TNC@FHH Entwicklung

Evren Eren, Stephan Uhde
FB Informatik
Fachhochschule Dortmund
Emil-Figge-Straße 42
44227 Dortmund
eren@fh-dortmund.de, stephan.uhde@gmx.de

Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
28359 Bremen
detken@decoit.de

Zusammenfassung

Unternehmen setzen zunehmend mobile Lösungen und Systeme ein. Jedoch fehlen hierzu ausgereifte und plattformunabhängige Mechanismen zur Authentifizierung und Autorisierung von Benutzer und Endgerät. Dies gilt insbesondere für den Einsatz in mittelständisch geprägten Unternehmen (KMU), die im Vergleich zu großen Unternehmen über keine Ressourcen für die IT-Sicherheit verfügen. Darüber hinaus werden Konfiguration und Administration mobiler Systemkomponenten sowie Identitätsmanagement und Zugangssteuerung komplexer und daher auch fehleranfälliger. Aus diesem Grunde sind plattformübergreifende Mechanismen zur zentralen und Anwendertransparenten Administration im Sinne von Identitäts- und Zugangssteuerung essentiell.

Dieser Beitrag diskutiert die wesentlichen Elemente von „Identity and Access Management (IAM)“ vor dem Hintergrund der spezifischen Anforderungen in mobilen Umgebungen und Anwendungsszenarien für KMU. Die Autoren geben einen kurzen State-of-the-Art zu IAM wieder und stellen zwei unterschiedliche, jedoch komplementäre, Entwicklungsansätze vor, die in den Forschungs- und Entwicklungsprojekten SIMOIT und TNC@FHH entstanden. Darüber hinaus beschreiben sie die Prototyp-Implementierungen und diskutieren die Ergebnisse.

1 Lösungen für die Endpunkte-Sicherheit

Das Wachstum des Internet bringt ständig neue Technologien mit sich und stellt demzufolge neue Herausforderungen an die IT-Sicherheit. Eine wesentliche betrifft, zusätzlich zur konventionellen Benutzerauthentifizierung, die zunehmende Notwendigkeit für die Geräte-Identifikation und -Authentifizierung sowie die Netzwerkzugangssteuerungsmechanismen in der IP-Schicht. Für die IT-Sicherheit im Allgemeinen sowie in Autorisierungsvorgängen bei Netzwerkzugangsanfragen in den ISO-OSI-Ebenen 2 und 3 ist die gerätebasierte und Plattformauthentifizierung wesentlich. [TCG08]
Heutzutage haben viele Mitarbeiter mobile Endgeräte wie Laptops, PDAs, etc. im Mischbetrieb, d.h., sowohl im privaten Bereich als auch am Arbeitsplatz, im Einsatz. Angriffe auf höheren OSI-Ebenen (Malware wie Viren und Trojanische Pferde) nehmen zu, was die Vertrauenswürdigkeit/Zuverlässigkeit der kommunizierenden Endpunkte (z.B. Client und Server) hinsichtlich der Integritätsbedingungen und ihrer Identitäten anbetrifft. [NISP08]

Integrität von Endpunkten
Unter Integrität verstehen wir die relative „Reinheit“ von Endpunkten bezüglich der eingesetzten (installierten) Software und Hardware. Endpunkte-Sicherheitslösungen nutzen Router, Switches, WLAN-Access-Points, Software und Security Appliances. Authentifizierungs- und Autorisierungsinformationen über mobile Endgeräte werden beispielsweise an einen Richtlinienserver weitergeleitet, der dann den Zugang regelt. Darüber hinaus ermöglicht der Zugriffsschutz eine Zustandsprüfung (Health Check) am Client. Ein solcher Check besteht üblicherweise aus der Abfrage bestimmter Informationen über

das Client-System. Ermittelt werden unter anderem die Version des Virenscanners, Einstellungen der Personal Firewall und anderer Programme sowie der Patch-Status des Endgerätes (u.a. des Betriebssystems). Falls der Client nicht den IT-Richtlinien entsprechen sollte, kann er in ein Virtual LAN (VLAN) isoliert werden, wo schließlich eine „Sanierung" erfolgen kann. [TCG08]

Lösungen und Standards
Neben den lizenzpflichtigen Softwarelösungen Network Admission Control (NAC) von Cisco und Network Access Protection (NAP) von Microsoft gibt es Open-Source-Lösungen, wie den Trusted Network Connect (TNC) Ansatz der Trusted Computing Group[1] verabschiedet wurde.

Alle genannten Technologien unterstützen die sichere Authentifizierungsmethode auf Basis des IEEE 802.1x-Authentifizierungsstandards. Diese beinhaltet die Identifizierung des Endsystems direkt am Switch-Port. Sie erfordert entsprechende Funktionen auf Seiten des Switches, des Clients und einer lokalen Authentifizierungsinstanz wie beispielsweise einem RADIUS-Server. Eine weitere Lösung ist die MAC-basierte Authentifizierung, bei der dieselbe Infrastruktur genutzt wird wie bei einer 802.1x-Infrastruktur, jedoch wird auf Zertifikate und/oder Anmeldedaten verzichtet. Der Switch verwendet die MAC-Adresse als Ersatz für die Credentials des Benutzers (Benutzername und Passwort) und prüft diese am RADIUS-Server. In 802.1x-fähigen Netzen kann dieses Verfahren verwendet werden, um Endsysteme ohne „Supplicant" (IEEE 802.1x-Endgeräteschnittstelle) gegen einen RADIUS-Server abzugleichen. [NISP08]

2 Der SIMOIT-Ansatz

Das SIMOIT-Projekt (www.simoit.de) zielte auf die Entwicklung einer auf Standards basierenden mobilen IT-Sicherheitsplattform ab, die sich in heterogenen mobilen Umgebungen einsetzen lässt. Die in diesem Projekt erarbeiteten Lösungen sollten in unterschiedlichsten Unternehmen einsetzbar sein. Ziel war es, technische und auch nicht-technische Lösungen als Baukastensystem zu entwickeln, die herstellerunabhängig entwickelt werden. Die nicht

1 http://www.trustedcomputinggroup.org/

technischen Lösungen zielen darauf ab, die Unternehmensführung von der Notwendigkeit der mobilen IT-Sicherheit zu überzeugen und die Akzeptanz der Mitarbeiter bzw. Benutzer zu erlangen.
Im SIMOIT-Projekt wurde beim Pilotkunden anhand seiner Anforderungen an mobile Endgeräte und Anwendungsfälle eine Entwicklungs- und Testplattform aufgesetzt, die den TNC-Ansatz praktisch evaluieren sollte. Die resultierende Hauptplattform stellt dabei das Mobile Security Gateway (MSG) dar, welches aus diversen Modulen (Firewall, TNC-Server, RADIUS-Server) besteht. Dabei wurden speziell Lösungen und Ansätze im „Open Source"-Bereich untersucht, um eine offene und standardkonforme Umsetzung zu ermöglichen. Gleichzeitig ist man jedoch so flexibel geblieben, dass bestehende Komponenten wie z.B. Firewall-Systeme eingebunden werden können. In diesem Fall würde statt des jeweiligen SIMOIT-Moduls eine Schnittstelle zur Verfügung gestellt. Auch wurde die Anbindung an eine bestehende Inventory-Datenbank im Sinne der Softwaredistribution realisiert, um die erlaubten Software-Versionen und Patch-Level abfragen zu können.
Zur Erreichung einer möglichst hohen Flexibilität wurde die Entwicklung hauptsächlich Server-seitig vorangetrieben, da man davon ausging, dass die Hersteller mobiler Endgeräte in naher Zukunft eigene Zugangssoftware bereitstellen werden. Server-seitig lässt sich somit jede beliebige TNC-Implementierungen anpassen.

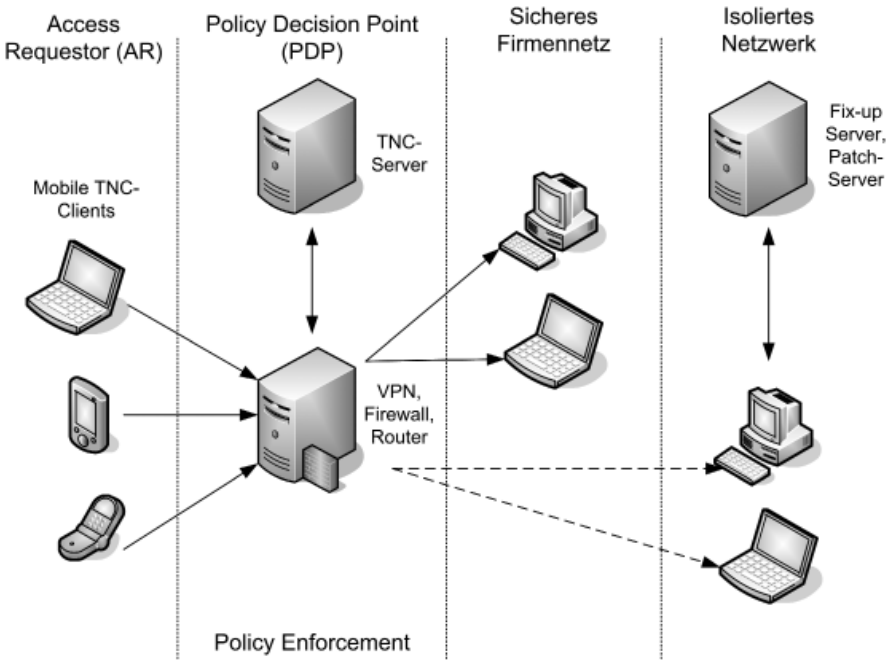

Abbildung 1: SIMOIT Ansatz

2.1 Arbeitsweise der SIMOIT-Lösung

2.1.1 Funktionale Komponenten des Client

In der SIMOIT-Implementierung besteht der Client funktional aus folgenden Komponenten:

- Integrity Measurement Collectors (IMC): Erfassen den aktuellen Zustand des Systems für definierte Teilbereiche, wie z.B. den Stand der Virendefinitionen oder die Version von Sicherheitssoftware.
- TNC-Client: Sammelt auf Anfrage die Informationen der Kollektoren, um diese für Integritätsentscheidungen des TNC-Servers weiterzuleiten.
- Softwareverteiler-Client: Falls der Client die Softwarebestandsanforderungen nicht erfüllt, lässt der TNC-Client anhand der Security Policy die jeweilige Komponente neue Softwarepakete installieren.

- Software-/Datenempfänger: Empfängt Benachrichtigungen über neue Softwareversionen und aktualisierte Security Policies, um automatisiert den Softwarebestand aktuell zu halten. Außerdem ruft diese Komponente nach Anweisung durch den Softwareverteiler-Client die Softwarepakete ab und stellt sie der Softwareinstallation zur Verfügung.
- Softwareinstallation: Nach Abruf von Installationspaketen erfolgt die Installation automatisiert.

2.1.2 Integritätsprüfung des Clients

Die Integritätsprüfung des Clients erfolgt auf Basis der Überprüfung des aktuellen Softwarebestandes gegen die Sicherheitsrichtlinien (Security Policy) des Unternehmens. Diese sollten deswegen im Unternehmensnetz zum Abruf bereitstehen. In diesen muss formuliert und beschrieben sein, in welchem Zustand sich mobile Endgeräte befinden dürfen, um Zugriff auf bestimmte Bereiche des Unternehmensnetzes zu erhalten. Die Sicherheitsrichtlinien beinhalten dabei Informationen, wie z.B. notwendige Software in verschiedenen Versionen und das aktuelle Pachtlevel des Betriebssystems. Zur Überprüfung des Zustands des Client werden entsprechend der Sicherheitsrichtlinien Software-Versionsstände, zusätzlich installierte Software, laufende Sicherheitsapplikationen und deren Zustand (z.B. Aktualität von Virendefinitionen) analysiert. Der TNC Integrity Measurement Collector (IMC) liefert dabei jeweils komponentenspezifische Zustandsinformationen, die vom mobilen Client zusammengetragen werden. Dadurch kann sichergestellt werden, dass diese Zustandsüberprüfung zum selben Ergebnis kommt wie die Überprüfung des RADIUSTNC-Servers.

2.1.3 Softwaredistribution

Die Softwareverteilung kommt zum Einsatz, wenn Clients per Aktualisierung der Sicherheitsrichtlinien oder nach Ablehnung des aktuellen Systemzustandes zum Installieren von Softwarepaketen angehalten werden. Eine Distributionsplattform hält die aktuell zu verteilenden Softwarepakete bereit, so dass mobile Clients diese per HTTP unter den in der Security Policy angegebenen Adressen abrufen können. Veraltete Updates werden ersetzt und fehlender Software initial installiert. Der Zugriff auf Updates ist bei Verbindung zum

Unternehmensnetz oder bei bestehender Quarantäne-VPN-Verbindung möglich. [DETK08]

2.1.4 Ablauf

Falls die Installation des mobilen Clients mit der Verbindung zum Unternehmensnetz erfolgt, wird die aktuelle Version der Security Policy direkt vom TNC-RADUIS-Server geladen. Alternativ muss erst eine VPN-Verbindung zum Unternehmensnetz hergestellt werden. Hierbei scheitert die Überprüfung der Zuverlässigkeit des mobilen Systems, da bisher keine Sicherheitsüberprüfung erfolgte und damit wahrscheinlich auch der Softwarebestand nicht ausreichend ist. Jedoch kann der Client die Security Policy im sog. Quarantänebereich erhalten und anwenden, so dass bei der nächsten Verbindung mit dem VPN-Server voller Zugang zum Unternehmensnetz ermöglicht werden kann.

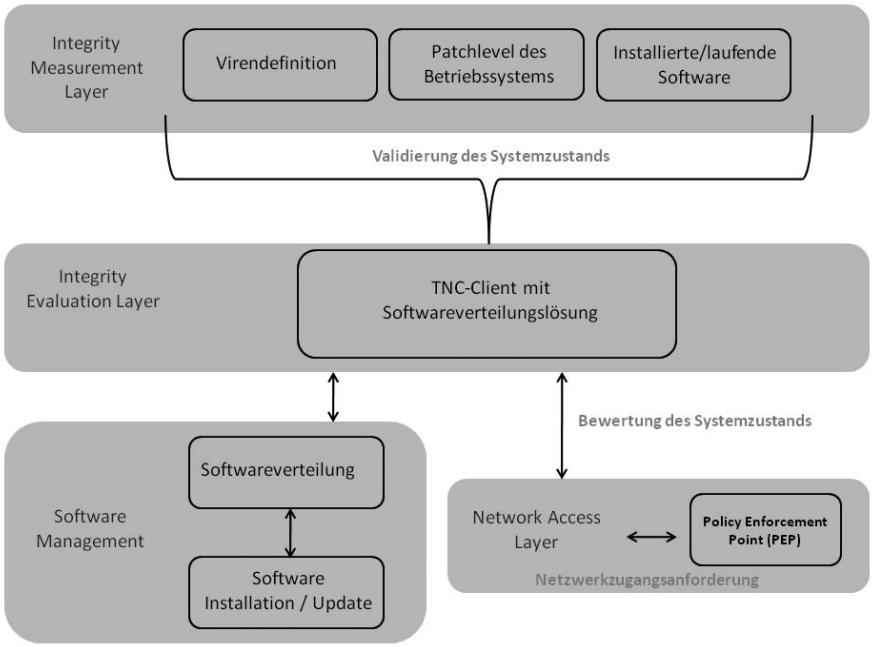

Abbildung 2: SIMOIT-Arbeitsweise

2.2 Implementierung der SIMOIT-Lösung

Die Implementierung der Hardwareplattform wurde mit vier Servern realisiert, wobei zwei Server für die Einwahl zuständig sind und zwei weitere Authentifizierungsdaten (Nutzerdaten und Softwarestand des einzuwählenden Gerätes) vorhalten:

- VPN-Gateway: Dient als Endpunkt des IPsec-Tunnels und nutzt X.509v3-Zertifikate für die Endgeräte. Durch den IPsec-Tunnel wird mittels L2TP die Authentifizierung durchgeführt. Auch die Zertifikats-ID des VPN-Tunnels wird ermittelt und mit den Credentials an den RADIUS-Server weitergeleitet.
- RADIUS-Server: Das auf Basis von FreeRADIUS realisierte Modul dient als Server-Komponente des TNC-Systems. Der TNC-Server basiert auf der Open Source Bibliothek „libtnc". Im Sinne des TNC-Standards stellt dieser den Policy Decision Point dar und entscheidet aufgrund der Daten vom Inventory-IMV, in welchen Netzbereich der TNC-Client gelangen darf. Mit anderen Worten: Der erweiterte RADIUS-Server übernimmt die Autorisierung und Authentifizierung des Benutzers und entscheidet aufgrund der Antwort des TNC-Moduls, ob der eingewählte Client Vollzugriff erhält oder nicht, bzw. in das Quarantänenetz gelangt.
- Windows 2003 Active Directory Server: Hier liegen die Credentials, die vom RADIUS-Server abgefragt werden.
- Softwareverteilung: Hält die Informationen der installierten bzw. fehlenden Pakete vor. Diese werden vom RADIUS-TNC-Modul ausgewertet. Im Rahmen des Pilotprojekts wurde die Softwareverteilung durch Matrix42 Empirum[2] realisiert. Als eine der zentralen Komponenten dient sie der Integritätsverwaltung der mobilen Clients. Sie kommt zum Einsatz, wenn mobile Clients per Aktualisierung der Sicherheitsrichtlinien oder nach der Ablehnung des aktuellen Systemzustandes zum Installieren von Softwarepaketen angehalten werden.

2 http://www.matrix42.de/home/

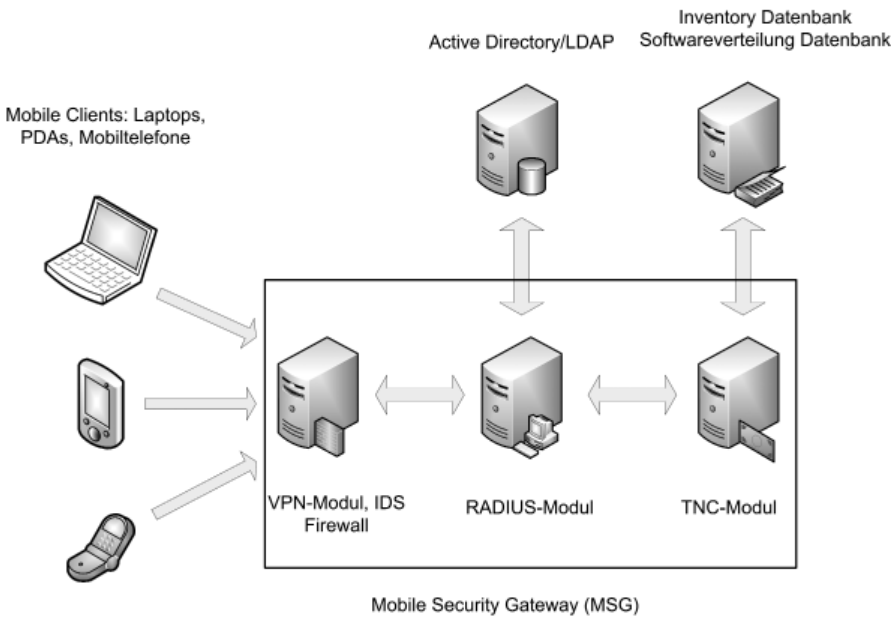

Abbildung 3: SIMOIT-Implementierung

2.3 Stand bei Projektende

Der TNC-Ansatz liegt seit 2008 in der Version 1.2 vor. Im SIMOIT-Projekt wurde aufgrund der fehlenden TNC-Client-Implementierungen eine reine Server-Lösung umgesetzt, die modular aufgebaut ist und mit anderen Sicherheitskomponenten genutzt werden kann. Durch den Einsatz einer Softwareverteilung wird das Fehlen des TNC-Clients kompensiert. Mit der Weiterentwicklung und Standardisierung sowie Marktdurchdringung von Lösungen, insbesondere durch Betriebssystemhersteller, kann der SIMOIT-Ansatz entsprechend erweitert werden. Bis dahin muss eine geeignete Softwareverteilungslösung Funktionen eines TNC-Clients kompensieren.

3 TNC@FHH

Der TNC@FHH-Ansatz[3] ist auch eine „Open Source"-Implementierung der TNC-Architektur zur Integritätsprüfung von Endgeräten im Rahmen der Netzwerkzugangskontrolle. Damit eine offene und standardkonforme Umsetzung ermöglicht werden konnte, wurde wie bei SIMOIT speziell Open Source Software untersucht und analysiert. Auch hier können bestehende Komponenten wie z.B. spezielle Firewall-Systeme eingebunden werden. Eine weitere Rahmenbedingung bestand darin, dass die TNC-Architektur auf Basis von IEEE 802.1x entwickelt werden sollte und in Ethernet-basierten Netzwerkumgebungen Verwendung findet.

Die Realisierung dieses Projektes besteht aus zwei wichtigen und getrennt voneinander arbeitenden Softwarepaketen. Client-seitig sind spezielle IMCs entwickelt worden, die aktuelle Sicherheitsstände des Systems analysieren und übermitteln. Diese sicherheitskritischen Informationen werden Server-seitig an den IMV, d.h. an den RADIUS/TNC-Server, übermittelt und anhand der Security Policy ausgewertet. Sobald die Evaluierung der gesammelten Information abgeschlossen ist und das mobile Endgerät den in der Security Policy eingetragenen Bestimmungen genügt, wird an den Network Access Server (IEEE 802.1x-fähiger Switch/Router) das Signal (Access-Accept) gesendet, welches dem Client den Netzwerkzugriff erlaubt.

3 http://trust.inform.fh-hannover.de/joomla/

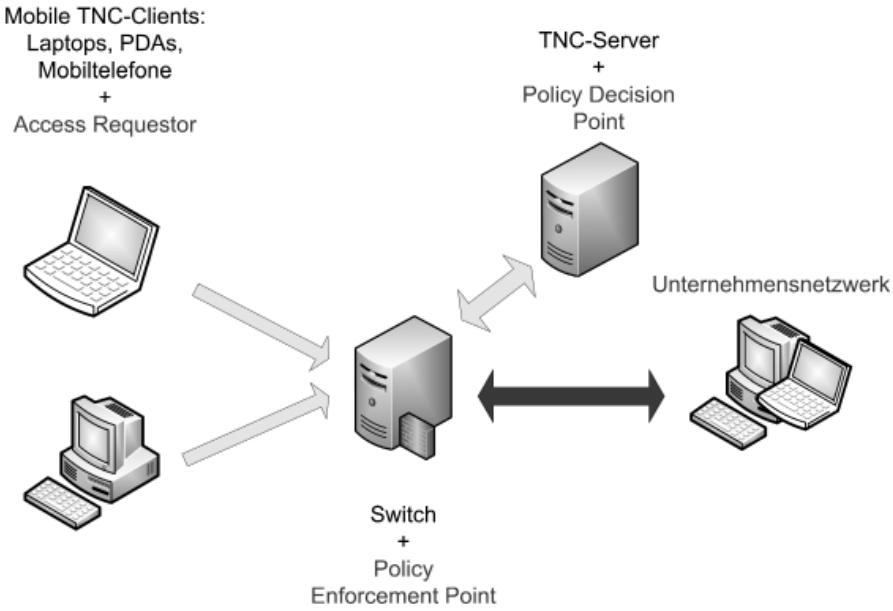

Abbildung 4: TNC@FHH-Ansatz

3.1 Arbeitsweise der TNC@FHH-Lösung

3.1.1 Integritätsprüfung des Clients

Die Integritätsprüfung erfolgt hier durch Erfassen der aktuell laufenden Dienste wie z.B. Telnet (Port 23) und SSH (Port 22) – weitere Server-Dienste sind möglich.
Auch hier wirken drei wesentliche TNC-Elemente. Die IMCs erfassen den aktuellen Zustand des Clients für definierte Teilbereiche, die sich zum derzeitigen Zeitpunkt auf spezielle Ports und deren Dienste beschränken. Der TNC-Clients sammelt auf Anfrage die Informationen der Kollektoren (IMC), um diese für Integritätsentscheidungen an den TNC-Server weiterzuleiten, welcher die Benachrichtigungen über die ausgelesenen Messdaten des Client empfängt und diese gegen die aktuell gültige Security Policy überprüft.

3.1.2 Ablauf

Die Überprüfung des Client-Zustands werden entsprechend der Sicherheitsrichtlinien sämtliche anwendungsbezogene Ports gecheckt. Der IMC liefert dabei exakte Zustandsinformationen, die dann zusammengetragen und an den RADIUS-TNC-Server übermittelt werden.
Wenn die Integrität nicht gewährleistet werden kann, ist eine erfolgreiche Authentifizierung nicht möglich. Die Security Policies des Unternehmens auf Seiten des Servers ist für die Einhaltung der Sicherheitsrichtlinien des Netzwerkes zuständig. Hier muss formuliert und beschrieben sein, in welchem Zustand das mobile Endgerät sich befinden darf, um Zugriff auf Netzwerkressourcen zu erhalten. Die Sicherheitsrichtlinie ist nicht nur auf Anwendungen und deren Ports beschränkt, sondern kann auch Informationen, wie z.B. notwendige Software in verschiedenen Versionen und zu startende Sicherheitsapplikationen beinhalten.

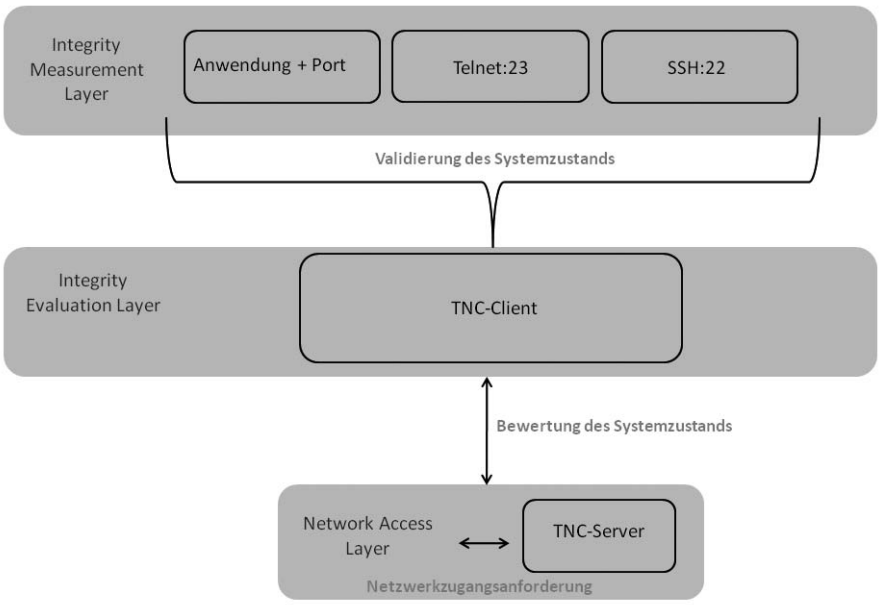

Abbildung 5: Arbeitsweise TNC@FHH

3.2 Implementierung

Die von der TNC@FHH implementierte Plattform besteht aus den Komponenten: mobiles Endgerät, 802.1x-Switch (Policy Decision Point) sowie dem RADIUS/TNC-Server. Der TNC-Client wird durch den das „Open Source"-Einwahl-Programm wpa_supplicant[4] ausgestattet, um die TNC-spezifischen Daten an den Server zu übermitteln und vorab die Authentifizierungsverbindung zum RADIUS-Server aufzubauen. Der RADIUS/TNC-Server übernimmt die Authentifizierung/Autorisierung von Benutzer und Endgerät und entscheidet aufgrund der Antwort des TNC-Moduls, ob der eingewählte Client Zugriff auf das Netzwerk erhält.
Wie bei SIMOIT ist die Basis des TNC-Ansatzes ein FreeRadius-Modul. Als weitere Komponenten sind, neben dem FreeRadius-Server und dem Inventory-IMV/IMC, die Softwarepakete TNCUtil sowie NAA-tncs im Einsatz. [Wutt06], [SCHMI06]

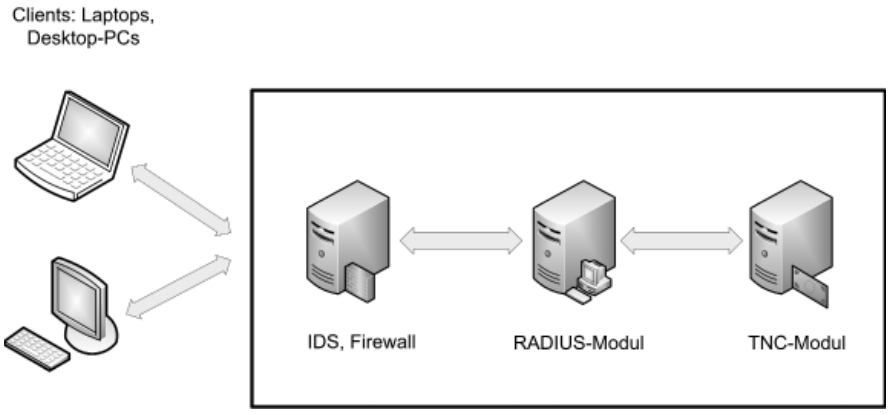

Abbildung 6: TNC@FHH-Implementierung

3.3 Stand bei Projektende

Das Projekt ist nun mit einem eigenen IANA[5]-Schlüssel registriert. Die Arbeit mit den Projektverantwortlichen des TNC@FHH-Ansatzes und denen der Trusted Computing Group[6] (TCG) sind seit der IANA-Registrierung intensiviert

4 http://open1x.sourceforge.net/
5 http://www.iana.org/
6 http://wwww.trustedcomputinggroup.org/

worden. Des Weiteren ist die Teilnahme an einem TCG-PlugFest[7] geplant. Hier wird versucht, den TNC@FHH-Ansatz mit einer anderen „Open Source"-TNC-Lösung zu kombinieren.

4 Vergleich SIMOIT und TNC@FHH

Beide TNC-Ansätze arbeiten Server-seitig mit ähnlichen Softwarepaketen. SIMOIT nutzt die Software libtnc[8] in Verbindung mit einem RADIUS-Server. Auf den mobilen Endgeräten wird, nach erfolgreicher IEEE 802.1x-Authentifizierung, mit Hilfe einer Softwareverteilungslösung dafür gesorgt, dass die aktuellen Sicherheitsrichtlinien eingehalten werden. Erst im Anschluss wird der sichere Netzwerkzugriff erlaubt. Die TNC@FFH Technologie dagegen setzt eine spezielle, selbst entwickelte TNC-Client- und Server-Software ein, die ebenfalls in Verbindung mit einem Open Source RADIUS-Server[9] dafür sorgt, dass nur die mobilen Endgeräte Zugang zum Netzwerk erhalten, die den Sicherheitsrichtlinien genügen.

4.1 Fazit

Die vorgestellten TNC-Ansätze der Projekte SIMOIT und TNC@FHH sind unterschiedliche „Trusted Computing"-Implementierungen für mobile Szenarien. Sie erlauben ein relativ hohes Sicherheitsniveau für mobiles Identity und Access Management. Die Ansätze sind modular aufgebaut, so dass auch andere Herstellerlösungen (z.B. VPN-Gateways oder Firewalls) integriert werden können. Beide sind modular aufgebaut, erweiterbar und mit konventionellen Sicherheitsmechanismen wie VPN und Firewalling kombinierbar. Beide Ansätze wurden im Laboratory for IT-Security Architectures – LISA (www.lisa.fh-dortmund.de) in einer typischen Unternehmensreferenzinfrastruktur implementiert und validiert.
Obgleich die Kernspezifikationen des TNC-Standards bereits abgeschlossen sind und dieser von Produkten wie Switches, Routern, VPN-Gateways unter-

7 http://trust.inform.fh-hannover.de/joomla/index.php/component/content/article/80-tncfhh-participates-in-tcg-plugfest-2009/
8 http://sourceforge.net/projects/libtnc/
9 http://freeradius.org/

stützt wird, sind noch Lücken bzgl. Veränderungen der Agenten auf Endgeräten vorhanden. Auch gehen Herstelleransätze noch weit auseinander.
In Zukunft ist geplant, TNC-Clients für unterschiedliche mobile Betriebssysteme (Windows Mobile 6.1, Android und Symbian) zu entwickeln, so dass sich der Einsatzbereich nicht nur auf Laptops beschränkt, sondern auch Smartphones sicher in ein Unternehmensnetz im Sinne des Trusted Computing eingebunden werden können. Im LISA-Labor des Fachbereichs Informatik der Fachhochschule Dortmund wurde vor Kurzem parallel die Entwicklung eines TNC-Clients für iPhone3G begonnen.

Literaturverzeichnis

[SUBA09] Stephan Uhde: Evaluation und Realisierung von Trusted Network Connect Ansätzen. Bachelorthesis. Dortmund, August 2009

[DACH09] Eren und Detken: User-Centric Identity Management in mobilen Szenarien im SIMOIT-Projekt. P. Horster (Hrsg.) · D.A.CH Security 2009 · syssec (2009) pp.

[TCG05] Trusted Computing Group, https://www.trustedcomputinggroup.org/home/

[DGBS08] 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

[TCG08] TCG Trusted Network Connect TNC Architecture for Interoperability; Specification 1.3; Revision 6; April 2008

[NISP08] Markus Nispel; Enterasys Secure Networks: Was Sie über NAC wissen sollten. http://www.computerwoche.de/knowledge_center/security/1871427/index.html

[DETK08] K.-O. Detken: Trusted Network Connect - die sichere Einwahl mobiler Mitarbeiter ins Unternehmen; Handbuch der Telekommunikation; Deutscher Wirtschaftsdienst; 129. Ergänzungslieferung von April; Köln 2008[Wutt06] Master-Thesis, Daniel Wuttke, 2006, Fachhochschule Hannover, Master_Thesis_Daniel_Wukkte.pdf

[Schmi069] Master-Thesis, Martin Schmiedel, 2006, Fachhochschule Hannover, tnc_masterarbeit-martin_schmiedel-de.pdf