Endpunkt Sicherheit

TNC-basiertes Identitäts- und Access-Management für mobile Anwendungen

Evren Eren

Immer mehr Unternehmen setzen zunehmend mobile Lösungen und Systeme für ihre Geschäftsprozesse ein. Jedoch fehlen ausgereifte und plattformunabhängige Mechanismen zur zentralisierten Authentifizierung bzw. Autorisierung von Benutzer und Endgerät. Insbesondere für mittelständisch geprägte Unternehmen sind Konfiguration und Administration mobiler Systemkomponenten zu komplex. Plattformübergreifende Mechanismen zur zentralen und anwendertransparenten Administration im Sinne von Identitäts- und Zugangssteuerung sind hier essenziell.

NET-Abonnenten steht ergänzend zum Beitrag das Literaturverzeichnis im Heftarchiv 10/09 unter www.NET-im-web.de zur Verfügung.

Prof. Dr. Evren Eren ist am Lehrstuhl für Medieninformatik und IT-Sicherheit an der Fachhochschule Dortmund tätig

Das Wachstum des Internet bringt ständig neue Techniken mit sich und stellt demzufolge neue Herausforderungen an die IT-Sicherheit. Dies betrifft insbesondere die Identifikation von Benutzer und Endgerät. Mitarbeiter in Unternehmen setzen eine Vielzahl von diversen mobilen Endgeräten wie Laptops, PDAs usw. im Mischbetrieb (privat als auch am Arbeitsplatz) ein, was aufgrund der unterschiedlichen Nutzungsprofile sowohl ein Kontext- als auch ein profilbasiertes Sicherheitsmanagement erfordert. Dies ist u.a. auch durch die steigende Zahl von Angriffen auf höheren ISO-OSI-Ebenen (Malware wie Viren und Trojanische Pferde) vonnöten, da die Vertrauenswürdigkeit und Zuverlässigkeit der kommunizierenden Endpunkte hinsichtlich ihrer Integritätsbedingungen und Identitäten beeinträchtigt wird [1]. Unter Integrität ist die relative Reinheit von Endpunkten bez. der installierten Software und der Gerätehardware zu verstehen. Eine Integritätsprüfung erfordert eine Zustandsprüfung (Health Check) des Endgeräts bzw. Clients. Ein solcher besteht üblicherweise aus der Abfrage bestimmter Informationen wie z.B.:

- Version des Virenscanners;
- Einstellungen der Personal Firewall (falls vorhanden);
- Konfiguration installierter Softwareanwendungen;
- Patch-Status des Endgeräts (Firmware) sowie des Betriebssystems.

Falls der Health Check der Security Policy des Unternehmens nicht genügen sollte, ist eine Isolation (z.B. in ein VLAN) mit anschließender Sanierung möglich [2].

Lösungen und Standards gemäß TNC

Es existieren mittlerweile zahlreiche Lösungen am Markt wie z.B. Ciscos Network Admission Control (NAC) sowie Microsofts Network Access Protection (NAP). Im Open-Source-Bereich dominiert der Trusted-Network-Connect-Standard (TNC) der Trusted Computing Group (www.trustedcomputinggroup.org/). Dieser liegt seit 2008 in der Version 1.2 vor.

Alle genannten Lösungen unterstützen eine Zugangssteuerung nach dem verbreiteten und etablierten Standard IEEE 802.1x, der eine Identifizierung des Endgeräts direkt am Switchport beinhaltet und in Kombination mit Radius und EAP (Extended Application Protocol) flexible Authentifizierungsmechanismen erlaubt. Alternativ ist die MAC-basierte Authentifizierung zu nennen, bei der dieselbe Infrastruktur genutzt wird wie bei 802.1x-Topologien. Jedoch wird auf Zertifikate und/oder Benutzer-Credentials verzichtet; der Switch verwendet die MAC-Adresse als Ersatz für die Credentials und prüft diese am Radius-Server. In 802.1x-fähigen Netzen kann dieses Verfahren verwendet werden, um Endsysteme ohne „Supplicant" (IEEE-802.1x-Client) gegen einen Radius-Server abzugleichen [1].

TNC-Ansatz nach Simoit

Bereits in der NET 6/08 (S. 12) wurde das Projekt Simoit vorgestellt. Es zielte auf die Entwicklung einer auf etablierten Standards basierenden mobilen IT-Sicherheitsplattform nach dem TNC-Standard, die sich in heterogenen mobilen Umgebungen einsetzen lässt. Die in diesem Projekt erarbeiteten Lösungen sollten in unterschiedlichsten, insbesondere in kleinen und mittelständischen Unternehmen (KMU) einsetzbar sein. Fokus war die Entwicklung einer herstellerunabhängigen Lösung als Baukastensystem. SIMOIT entwickelte das sog. Mobile Security Gateway (MSG), das modular

aus den Bausteinen TNC-Server, Firewall und Radius-Server zusammengesetzt ist. *Bild 1* illustriert die Komponenten dieses Ansatzes in einer typischen Unternehmenstopologie [3]. Das MSG kommuniziert mit einer Inventory-Datenbank innerhalb einer Softwaredistributionslösung, die das Management von Softwareversionen und Patchleveln von mobilen Endgeräten erlaubt.

Im Mittelpunkt der Entwicklungen in Simoit lag eine serverseitige Realisierung des TNC-Standards. Dies wurde damit begründet, dass Hersteller mobiler Endgeräte in naher Zukunft eigene Zugangssoftware bereitstellen werden und eine Eigenentwicklung eines TNC-Clients sich nicht lohnen würde. Durch diese serverseitige Realisierung ließe sich jede beliebige TNC-Implementierung anpassen.

Die Simoit-Plattform besteht aus insgesamt vier Servern [4]:

- VPN-Gateway: Dient als Endpunkt des IPsec-Tunnels und nutzt X.509v3-Zertifikate für die Endgeräte.
- Radius-Server/TNC-Modul: Das auf Basis von FreeRadius realisierte Modul dient als Serverkomponente des TNC-Systems. Im Sinne des TNC-Standards stellt dieses den Policy Decision Point (PDP) dar und entscheidet aufgrund der Daten vom Inventory-IMV (Integrity Measurement Validator), in welchen Netzbereich das Endgerät gelangen darf. Der erweiterte Radius-Server übernimmt die Benutzerauthentifizierung und -autorisierung und entscheidet aufgrund der Antwort des TNC-Moduls, ob er Vollzugriff erhält oder nicht bzw. ob das Quarantänenetz isoliert werden soll.
- Windows-2003-Server: Hier liegen die Credentials, die vom Radius-Server abgefragt werden.
- Softwareverteilung: Die auf dem Produkt Matrix42 Empirum (**www.matrix42.de/home/**) realisierte Softwareverteilung hält die Informationen der installierten bzw. fehlenden Pakete vor, die vom Radius-TNC-Modul ausgewertet werden. 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 Systemzustands zum Installieren von Softwarepaketen angehalten werden. Die aktuell zu verteilenden Softwarepakete werden bereitgestellt, so dass mobile Clients diese per HTTP unter den in der Security Policy angegebenen Adressen abrufen können. Dabei können veraltete Updates ersetzt oder fehlende Software neu installiert werden. Updates sind bei Verbindung zum Unternehmensnetz oder bei bestehender Isolation im Quarantänebereich (i.d.R. ein hierfür vorgesehenes VLAN) beziehbar [5].

Die Integritätsprüfung des Clients erfolgt auf Basis der Überprüfung des aktuellen Softwarebestandes gegen die Security Policy des Unternehmens. In dieser ist formuliert, in welchem Zustand sich mobile Endgeräte befinden dürfen (z.B. notwendige Software in verschiedenen Versionen und das aktuelle Pachtlevel des Betriebssystems), um Zugriff auf bestimmte Bereiche des Unternehmensnetzes zu erhalten. Zur Überprüfung des Client-Zustands werden entsprechend den Sicherheitsrichtlinien Softwareversionsstände, installierte Software, laufende Sicherheitsapplikationen und deren Zustände (z.B. Aktualität von Virendefinitionen) analysiert. Auf Anfrage sammelt der TNC-Client Informationen der Integrity Measurement Collectors (IMC), um diese durch die Integrity Measurement Validators prüfen zu lassen und die endgültige Integritätsentscheidung durch den TNC-Server herbeizuführen.

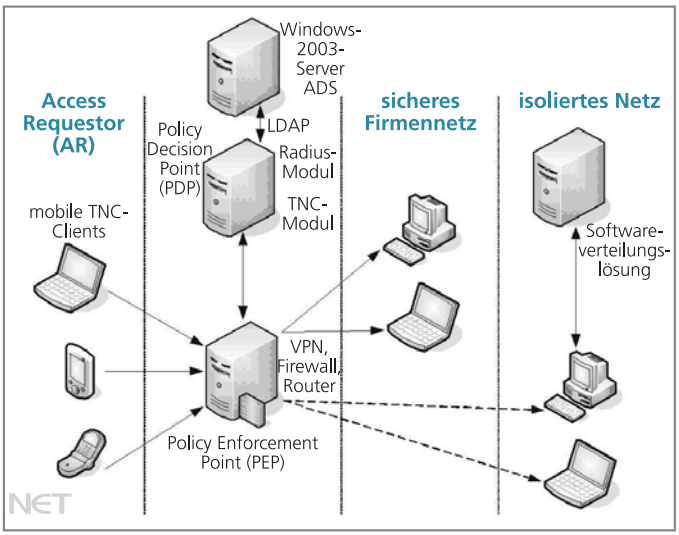

Bild 1: Simoit-Ansatz

Ansatz von TNC@FHH

Eine weitere Open-Source-Implementierung der TNC-Architektur zur Integritätsprüfung von Endgeräten im Rahmen der Netzzugangskontrolle ist der TNC@FHH-Ansatz (**http://trust.inform.fh-hannover.de/joomla/**).

Wie bei Simoit wurde auch hier im Sinne einer offenen und standardkonformen Lösung speziell Open-Source-Software analysiert, um bestehende Komponenten wie z.B. IEEE 802.1x und Firewall-Systeme einbinden zu können (*Bild 2*).

TNC@FHH setzt sich aus zwei getrennt voneinander arbeitenden Softwarepaketen zusammen. Client-seitig sind spezielle IMCs entwickelt worden, die aktuelle Sicherheitsstände des Systems analysieren und an die IMVs auf Serverseite, d.h. an den Radius/TNC-Server, übermitteln und anhand der Security Policy durch diese auswerten lassen. Genügt das mobile Endgerät den in der Security Policy eingetragenen Bestimmungen, wird an den Network Access Server (IEEE-802.1x-fähiger Switch/Router) das

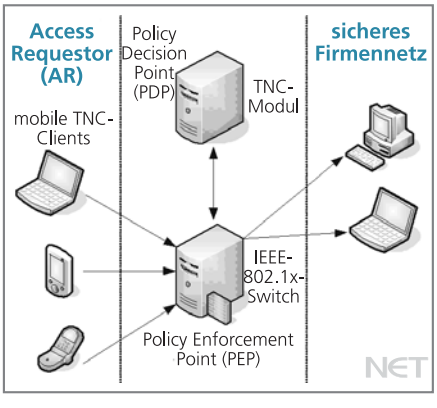

Bild 2: TNC@FHH-Ansatz

Signal (Radius Access-Accept) gesendet, dass dem Client den Netzzugriff erlaubt.

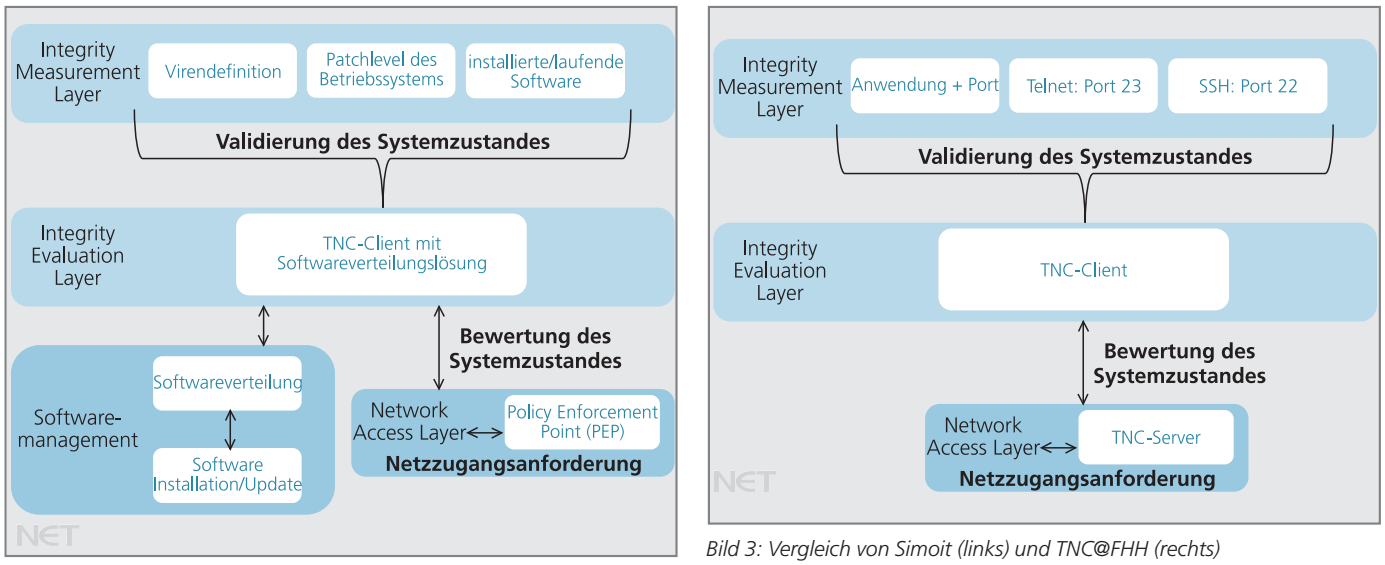

Bild 3: Vergleich von Simoit (links) und TNC@FHH (rechts)

Die Integritätsprüfung des Clients erfolgt hier durch Erfassen von aktuell laufenden Diensten wie z.B. Telnet (Port 23) und SSH (Port 22); weitere Serverdienste 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-Client sammelt die Informationen der Kollektoren (IMC), um diese für Integritätsentscheidungen an den TNC-Server weiterzuleiten, der die Benachrichtigungen über die ausgelesenen Messdaten empfängt und diese gegen die aktuell gültige Security Policy überprüft.

Die von der TNC@FHH implementierte Plattform besteht aus den Komponenten: mobiles Endgerät, 802.1x-Switch sowie Radius/TNC-Server. Der TNC-Client wird durch das Open Source-Einwahlprogramm wpa_supplicant (http://open1x.sourceforge.net/) realisiert. Es baut die Authentifizierungsverbindung zum Radius-Server auf und übermittelt die TNC-spezifischen Daten an den Server. Der Radius/TNC-Server übernimmt die Authentifizierung bzw. Autorisierung von Benutzer sowie Endgerät und entscheidet aufgrund der Antwort des TNC-Moduls, ob der eingewählte Client Zugriff auf das Netz erhalten darf. Wie bei Simoit ist die Basis des TNC-Ansatzes ein FreeRadius-Modul. Als weitere Komponenten wirken, neben diesem und den Inventory-IMV/IMC-Paaren, die Softwarepakete TNCUtil sowie NAA-tncs [6], [7].

Vergleich von Simoit und TNC@FHH

Beide TNC-Ansätze arbeiten serverseitig mit ähnlichen Softwarepaketen. In Simoit wurde aufgrund der fehlenden TNC-Client-Implementierung eine rein modulare Serverlösung umgesetzt, die mit anderen Sicherheitskomponenten wie Firewalls und VPN-Servern kombinierbar ist. Durch 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. Der TNC-Server basiert auf der Open-Source-Bibliothek libtnc (http://sourceforge.net/projects/libtnc/) in Verbindung mit einem Open-Source-Radius-Server (http://freeradius.org/).

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 Netzzugriff erlaubt.

Die TNC@FFH-Technik dagegen setzt eine spezielle, selbst entwickelte TNC-Client- und Serversoftware ein, die ebenfalls in Verbindung mit FreeRadius dafür sorgt, dass nur die mobilen Endgeräte Zugang zum Netz erhalten, die den Sicherheitsrichtlinien genügen. *Bild 3* vergleicht die beiden TNC-Ansätze hinsichtlich der Integritätsprüfung des Clients.

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, gut skalierbares Identitäts- und Access-Management. Beide sind modular aufgebaut, erweiterbar und mit konventionellen Sicherheitsmechanismen wie VPN und Firewalls kombinierbar. Beide Ansätze wurden im Laboratory for IT-Security Architectures – LISA (www.lisa.fh-dortmund.de) in einer typischen Unternehmensreferenzinfrastruktur implementiert und validiert.

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 beispielsweise auch Smartphones sicher in ein Unternehmensnetz im Sinne des Trusted Computing eingebunden werden können. *(bk)*