Bin ich schon drin?!
TNC - Network Access meets Trusted Computing

Marian Jungbauer, Markus Linnemann, Norbert Pohlmann

Mit dem Slogan „Bin ich schon drin“ warb ein Provider bereits vor Jahren dafür, wie einfach es ist ins Internet zu kommen. Das Internet als gigantisches Netzwerk ermöglicht heute nicht nur den Zugang zu verschiedenen Webseiten. Das Internet ist die globale Plattform, um Menschen und Firmen zu vernetzten. Ob ich „drin“ bin in einem Netzwerk hängt von der Zugangskontrolle, dem Türsteher des Netzwerkes ab. Dieser erwartet ganz unterschiedliche Vorraussetzungen: Zertifikate, Benutzername und Passwort oder auch einen bestimmten Konfigurationszustand. Eine Auseinandersetzung mit dem Thema „Network Access Control“ ist Pflicht für jedes Netzwerk. Trusted Computing schafft es der Zugangskontrolle den entscheidenden Sicherheitsgewinn zu geben.

Einleitung

Computernetzwerke sind heute in der Wirtschaft, aber auch im privaten Umfeld nicht mehr wegzudenken. Intranets ermöglichen in Firmen eine Verbindung von Arbeitsplätzen und erlauben damit einen direkten Datenaustausch ohne Medienbrüche wie Ausdrucke auf Papier.

Das Internet nimmt immer mehr die Rolle eines universell einsetzbaren Netzwerks ein. Sicherheitskritische Anwendungen über das Internet wie Geschäftsabschlüsse und der Austausch sensibler Informationen zwischen Firmen und ihren Niederlassungen nehmen stark zu. Im Jahr 2005 wurden im Online-Handel Transaktionen im Wert von 321 Milliarden Euro getätigt [Bitk06]. Dies bedeutet einen Anstieg von 58% gegenüber dem Jahr 2004. Der Anteil der Transaktionen zwischen Unternehmen (B2B) betrug hierbei 289 Mrd. Euro (90%). Des Weiteren werden Außendienstmitarbeiter und Heimarbeiter über das Internet mit dem Firmennetzwerk verbunden und ermöglichen so dem Mitarbeiter einen schnellen und aktuellen Zugriff auf Firmendaten.

Auf der anderen Seite sind Netzwerke Quelle und Ziel für zahlreiche Bedrohungen für Unternehmen und Privatpersonen. Das Internet als große „Spielwiese“ für „Angreifer“ stellt eine Plattform für die einfache Verbreitung von Viren, Würmern und Trojanischen Pferden dar. Laut dem „11. Internet Security Threat Report“ von Symantec kamen die von Symantec überwachten Rechnersysteme zwischen Juli und Dezember 2006 mit über 8200 neuen Schädlingen in Kontakt [Syma07]. Es wurden täglich über 5200 sog. Denial of Service-Angriffe gemessen, die einen Dienst lahmlegen können.

Mitarbeiter der Unternehmen sind auch Heimanwender, die immer häufiger ihre Notebooks mit nach Hause nehmen, Familienmitgliedern den Zugriff auf diese Geräte erlauben oder private Rechnersysteme an das Firmennetz anschließen [Mai06]. Zusätzlich nutzen Außendienstmitarbeiter ihre Rechnersysteme in vielfältigen Umgebungen mit unterschiedlichem Sicherheitsbedarf. Gelangen kompromittierte Geräte zurück ins Firmennetzwerk und verbreiten dort Ihre zerstörerische Malware bedeutet dies eine Gefährdung des Unternehmensnetzwerks und der angeschlossenen Rechnersysteme und somit auch eine Gefährdung des Unternehmens selbst. Die Mitarbeiter „tragen“ also die Malware an den etablierten Sicherheitsmechanismen vorbei in die Unternehmen.

Somit wird ein Netzwerk „vertrauensvoll“ genutzt, dessen Flexibilität und kostengünstige Nutzung ein Mangel an Sicherheit entgegensteht. Ein Mangel, welcher eine umfassende Nutzung in sicherheitskritischen Bereichen ohne zusätzlichen Schutz nur eingeschränkt zulässt.

Der Weg zum vertrauensvollen Zugang

Firmen schützen ihr Netzwerk heute zumeist durch „softe“ Mechanismen wie Passwörter oder Zertifikate. Der Zustand der zum Zugriff genutzten Rechnersysteme wurde bisher nicht beachtet. Die eingangs dargestellten Probleme zeigen, dass dieses Vorgehen heute und in Zukunft nicht mehr praktikabel ist.

Seit wenigen Jahren existieren nun sog. Network Access Control (NAC) - Systeme.

Definition

Unter Network Access Control (NAC) versteht man eine Technologie, mit der der Zugang zu einem Rechnernetzwerk abhängig vom Benutzer und der Vertrauenswürdigkeit des zum Zugriff eingesetzten Rechnersystems gesteuert wird.

NAC-Systeme regeln also, wie ein Türsteher, wer in ein Netzwerk eintreten darf und wer nicht und machen ihre Entscheidung nicht nur von den Login-Daten des Benutzers, sondern auch vom Zustand der zum Zugriff genutzten Rechnersysteme abhängig.

Wird bei NAC-Systemen durch ein Rechnersystem eine Verbindung zu einem Netzwerk aufgebaut, findet neben einer Nutzerauthentifizierung eine Überprüfung der Vertrauenswürdigkeit des eingesetzten Rechnersystems statt. Diese Überprüfung basiert auf Messungen der Konfiguration des Rechnersystems und einem Vergleich dieser Messung mit Sicherheitsrichtlinien (Policies) des Netzwerkbetreibers. Rechnersysteme mit einer aus Sicht des Netzbetreibers fehlerhaften, also nicht vertrauenswürdigen Konfiguration können entdeckt und präventiv vom Netzwerk mit seinen angeschlossenen Rechnersystemen und angebotenen Diensten fern gehalten werden.

Die Anwendungsfelder von NAC-Systemen sind dabei vielfältig. NAC kann den Schutz des Intranets vor Angriffen von außen erhöhen. Eine Erweiterung des VPN-Zugriffs mit NAC-Funktionen ermöglicht die Messung der Konfiguration entfernter Rechnersysteme. Damit wird es möglich Heimarbeiter und insbesondere Außendienstmitarbeiter sicher und vertrauenswürdig in das Firmennetzwerk zu integrieren. Im Intranet können beispielsweise 802.1x-basierte Netzwerke mit NAC-Funktionen ausgestattet und so Angriffe von innen präventiv abgewendet werden. Zusätzlich besteht die Möglichkeit, Gefahren durch firmenfremde Rechnersysteme, z.B. von Gästen, zu minimieren.

Mobile Endgeräte werden immer leistungsfähiger und deshalb auch vermehrt in Geschäftsprozesse und vorhandene Netzwerkstrukturen integriert. Durch den verstärkten Einsatz mobiler Endgeräte auch für sicherheitskritische Aufgaben rücken diese Geräte immer weiter in den Fokus der Angreifer und erfordern somit eine Ausweitung der vorhandenen Sicherheitstechnologien auf mobile Netzwerke [HJP07].

Schon heute existieren NAC-Ansätze verschiedenster Hersteller. Die prominentesten Vertreter sind die Microsoft Network Access Protection (NAP) und Cisco Network Admission Control (NAC). Diese Lösungen sind proprietär und vom Grundsatz her nicht interoperabel. Eben diese fehlende Interoperabilität stellt ein großes Hemmnis in der Verbreitung von NAC dar. Aktuell existieren zwei Standardisierungs-Ansätze die diesen Umstand beheben wollen. Die „Trusted Network Connect“ (TNC) Spezifikation der Trusted Computing Group und der von der IETF unter dem Namen „Network Endpoint Assessment “ (NEA) entwickelte Standard, der sich noch in einem sehr frühen Stadium befindet [Ietf07].

Trusted Network Connect

Trusted Network Connect wird durch die TNC-Subgroup der Trusted Computing Group entwickelt. Das Ziel ist die Schaffung eines offenen NAC-Standards. Die Spezifikation liegt zurzeit (Januar 2008) in Version 1.2 vor [TnSg07].

TNC baut wiederum auf vielen vorhandenen und etablierten Standards auf. Darunter aktuelle Sicherheitstechnologien für den Netzwerkzugriff („802.1x“ und „VPN“), für den Nachrichtentransport („EAP“, „TLS“ und „HTTPS“) und für die Authentifizierung („Radius“ und „Diameter“).

TNC Architektur

Grundsätzlich wird in der TNC-Spezifikation zwischen drei Elementen unterschieden.

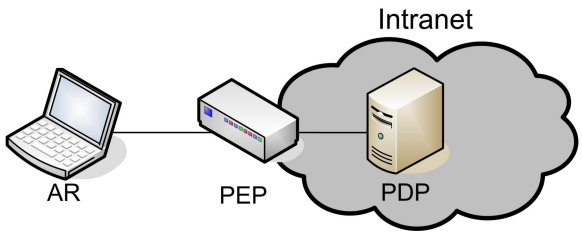

Abbildung 1: Architektur von TNC

Das Rechnersystem, über das eine Netzwerkverbindung zu einem TNC-Netzwerk aufgebaut werden soll, wird **Access Requestor (AR)** genannt. Der **Policy Decision Point (PDP)** stellt die Gegenseite zum AR dar. Der **Policy Enforcement Point (PEP)** ist das TNC-Element am Eintrittspunkt des Netzwerkes.

Abbildung 2: TNC Phasen

Alle durch TNC bereitgestellten Funktionen werden in drei Phasen eingeordnet.

Die **Assessment Phase** umfasst alle Aktionen vom Versuch eines Verbindungsaufbaus zu einem TNC-geschützten Netzwerk bis zur Entscheidung über dessen Vertrauenswürdigkeit. In dieser Phase werden Messwerte vom Rechnersystem an einen Server im Netzwerk gesendet und dort anhand von Policies verglichen. Durch diesen Vergleich ist eine Entscheidung über die Vertrauenswürdigkeit möglich. Wird das Rechnersystem, bei Nichterfüllung der Policies, als nicht-vertrauenswürdig eingestuft, gelangt es in die **Isolation Phase** in der das Rechnersystem in einem geschützten Netzwerkbereich isoliert wird. Eventuell mit Malware kompromittierte Rechnersysteme oder Angreifer erhalten so keinen Zugriff auf das Netzwerk und die dort angebotenen Dienste. In der **Remediation Phase** können isolierte Rechnersysteme ihre Konfiguration, zum Beispiel über die Installation fehlender Patches, gemäß den Policies anpassen und nach einer erneuten Überprüfung, Zugriff auf das Netzwerk mit seinen angebotenen Dienste zu erhalten.

So funktioniert TNC

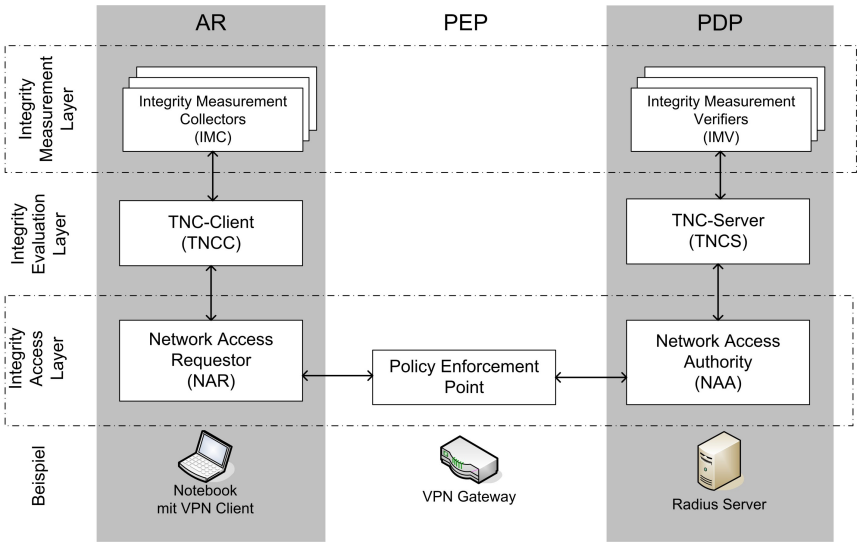

Abbildung 3: TNC im Detail

Der **Access Requestor (AR)** besteht aus drei Komponenten, den „Integrity Measurement Collectors“ (IMC), dem „TNC-Client“ und dem „Network Access Requestor“. Ein IMC übernimmt die Messung einer einzelnen, speziellen Komponente des Rechnersystems. Das heißt, dass auf einem Rechnersystem mehrere IMCs, für jede Komponente existieren. Beispiele sind IMCs für Virenscanner und für die Personal-Firewall. Der „Network Access Requestor“ (NAR) kümmert sich um den Aufbau der Kommunikationsverbindung zum TNC-Netzwerk, beispielsweise über 802.1x.

Der **Policy Decision Point (PDP)** besteht ebenfalls aus drei Komponenten. Die „Integrity Measurement Verifier” (IMV) stellen das Gegenstück zu den IMCs des AR dar. Für jeden IMC des AR existiert auf dem PDP ein passender IMV. Die IMVs vergleichen die übermittelten Messwerte anhand

der in den Policies festgelegten Regeln und teilen ihr Ergebnis dem TNC-Server mit. Dieser erstellt aus allen Teilergebnissen eine Handlungsempfehlung und teilt diese Entscheidung der Network Access Authority (NAA) mit. Die NAA trifft dann eine endgültige Zugriffs-Entscheidung.

Der **Policy Enforcement Point (PEP)** sitzt am Eintrittspunkt zum Netzwerk, beispielsweise integriert in ein VPN-Gateway. Er leitet ankommende Verbindungsanfragen eines AR direkt an den PDP weiter. Hat der PDP eine Zugriffs-Entscheidung getroffen, teilt er diese dem PEP mit, der die Entscheidung ausführen muss.

Warum ist TNC alleine nicht ausreichend für hohe Sicherheit?

Der durch heutige NAC-Lösungen, aber auch durch TNC, geschaffene Vertrauenslevel ist hauptsächlich von der Vertrauenswürdigkeit des Clients und der dortigen Ermittlung der Messwerte abhängig. Die Messwerte müssen korrekt gemessen und unverfälscht, d.h. nicht kompromittiert, an das NAC-Netzwerk übermittelt werden. Hierbei bestehen zwei Einschränkungen:

Zum Einen ist es bei heutigen Betriebssystemstrukturen nur sehr eingeschränkt möglich, eine Kompromittierung durch unbekannte Malware festzustellen. Das heißt, dass selbst mit einem aktuellen Patch-Level, einer aktuellen Firewall und einem Virenscanner mit neuester Virensignatur die Gefahr einer unentdeckten Kompromittierung besteht.

Zum Anderen kann die Vertrauenswürdigkeit der gesendeten Messwerte generell als nicht sicher angesehen werden. Es fehlt die Garantie, dass die Messung des Systemzustands tatsächlich den Zustand des Rechnersystems abbildet. Durch diese Eigenschaft entsteht zwangsläufig ein Paradoxon, das die Glaubwürdigkeit der Messwerte stark herabsetzt:

Wurde ein Rechnersystem auf Hardware- oder Softwareebene kompromittiert, dürfen die durch das System ermittelten Messwerte als nicht mehr vertrauenswürdig angesehen werden. Da die Messwerte aber zur Entdeckung von fehlender Integrität genutzt werden sollen, entsteht durch die ständige Gefahr der unbemerkten Fälschung ein dauerhaftes Misstrauen gegenüber den Messwerten. Das dieses Problem kein theoretisches ist, wurde unlängst auf der Black Hat Konferenz 2007 anhand von Cisco NAC vorgeführt. Mittels eines modifizierten Cisco Trust Agent (CTA) war es jederzeit möglich, unabhängig vom Rechnerzustand Zugriff auf ein NAC-geschütztes Netzwerk zu erlangen [Ruet07].

Hierbei handelt es sich aber um kein TNC-spezifisches Problem, sondern ein Gesamtproblem heutiger Rechnersysteme. Aktuelle monolithische Betriebssystemstrukturen ermöglichen keine klare Trennung von Komponenten, so dass das Betriebssystem nach der Kompromittierung nur einer Komponente automatisch als komplett kompromittiert zu werten ist.

TNC bietet durch die Nutzung eines Trusted Platform Moduls(TPM), ein fest mit dem Mainboard verbundener passiver Cryptochip, die Möglichkeit, die Messwerte und die TNC-Komponenten auf Seiten des Clients zu überprüfen. Dies stellt aber bei heutigen Betriebssystemen keine zusätzliche Sicherheit dar. Die Schwelle für Malware wird zwar etwas höher gesetzt, sie ist aber immer noch zu niedrig, um das Vertrauenslevel zu erhöhen, da ein kompromittiertes Betriebssystem einen beliebigen Wert an das TNC-Netzwerk übergeben könnte, das auf Vertrauenswürdigkeit schließen lassen würde, aber nicht der Realität entspricht.

TNC braucht eine Sicherheitsarchitektur

Erst eine Kombination mit neuen Sicherheitsarchitekturen, kann die grundlegende Einschränkung der Vertrauenswürdigkeit verhindern. Genau hier liegt auch die Stärke der TNC-Spezifikation. Durch die Einbindung in das Trusted Computing Konzept und die offene Spezifikation ist es möglich, einen Industriestandard zu schaffen, der auch mit zukünftigen Technologien, wie beispielsweise Sicherheitsplattformen, kompatibel ist.

Durch die Integration in eine Sicherheitsplattform lassen sich die TNC-Komponenten effektiv vor Manipulation schützen und die Konfiguration des Rechnersystems zuverlässig ermitteln. Eine Kompromittierung eines auf der Plattform laufenden herkömmlichen Betriebssystems kann durch strenge Isolation von Speicherbereichen nicht auf die TNC-Komponenten übergreifen.

TNC in der Anwendung und Forschung

Die TNC-Spezifikation ist noch nicht vollständig, doch schon heute ist TNC Gegenstand von Forschung und Entwicklung und zunehmend auch in der Wirtschaft.

In der Forschung existieren unterschiedliche Projekte zu TNC. Aus Deutschland kommt das TNC@FHH-Projekt der Fachhochschule Hannover [Tfhh07]. Ziel ist die Entwicklung einer Open Source Implementierung von TNC.

Zunehmend entdecken auch die Hersteller heutiger NAC-Lösungen die Vorteile von TNC. Microsoft hat ein zentrales NAP-Protokoll der TNC-Subgroup zur Verfügung gestellt und ermöglicht so eine gewisse Interoperabilität zwischen NAP und TNC-Lösungen. Andere Hersteller gestalten ihre NAC-Lösungen direkt kompatibel zu TNC. So beispielsweise Juniper Networks mit ihrer Unified Access. Control (UAC).

Fazit

Der zunehmende Einsatz von Netzwerken für sicherheitskritische Aufgaben erzeugt einen immer stärkeren Bedarf an den vorgestellten Technologien, der aktuell nicht ausreichend befriedigt werden kann. Der noch vor ein paar Jahren aktuelle Werbeslogan „Bin ich schon drin“ zeigt indirekt die größte Einschränkung vorhandener Netzwerke, die Vernachlässigung der Sicherheit. Für die aktuelle und zukünftige Nutzung muss dieser Slogan angepasst werden. Anwender müssen sich nun fragen: „Bin ich schon sicher drin?“.

TNC als virtueller Türsteher ist für diese Aufgabe ein denkbares und sinnvolles Szenario. Es erlaubt die Überprüfung der Konfiguration entfernter Rechnersysteme und stellt somit die Basis zur Bewertung der Integrität und Vertrauenswürdigkeit dieser Rechnersysteme zur Verfügung.

Insbesondere durch die einfache Unterstützung neuer Sicherheitsarchitekturen ist tatsächlich ein vertrauenswürdiger Zugang für Netzwerke möglich, der mit schon heute existierenden NAC-Lösungen aufgrund fehlender Vertrauenswürdigkeit der Messwerte nicht erreicht werden kann.

Standards können sich nur durchsetzen, wenn sie durch genügend Unternehmen unterstützt werden. Durch die große Mitgliederzahl in der TNC-Subgroup, mittlerweile sind dort über 80 Firmen vertreten, hat TNC das Potential sich als „der“ NAC-Standard zu entwickeln.

Literatur

[Bitk06] European Information Technology Observatory (EITO); Nicht mehr laufen, online kaufen!; BITKOM e.V. - http://www.bitkom.org; 2006; http://www.bitkom.org/de/presse/43408_39401.aspx

[Ietf07] http://tools.ietf.org/wg/nea/

[HJP07] Malte Hesse; Marian Jungbauer; Norbert Pohlmann; Trusted Computing; Aus: <kes>; Sonderausgabe Juli07; SecuMedia; ISSN: 1611-440X

[Mai06] McAfee Inc.; Gefahren von innen: Die eigenen Mitarbeiter als Sicherheitsrisiko; all-about-security.de - http://www.mcafee.com; 2006; http://www.all-about-security.de/artikel+M5575b662171.html

[Ruet07] Christian Ruetten; Ciscos Netzwerkzugangskontrolle NAC ausgetrickst; Heise Verlag - http://www.heise.de; 2007; http://www.heise.de/newsticker/meldung/87663

[Syma07] Symantec Corporation; Zusammenfassung des 11. Interent Security Threat Reports; Symantec Deutschland GmbH - http://www.symantec.de; 2007; http://www.symantec.com/content/de/de/about/downloads/PressCenter/DatenFakten_ISTR_XI_final.pdf

[Tfhh07] http://tnc.inform.fh-hannover.de/wiki/index.php/Main_Page

[TnSg07] https://www.trustedcomputinggroup.org/specs/TNC

Autoren

Markus Linnemann und Marian Jungbauer sind Mitarbeiter am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen.

Prof. Dr. Norbert Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de, https://norbert-pohlmann.com/)