

Trusted Network Connect

Vertrauenswürdige Netzwerkverbindungen

Marian Jungbauer
Marian.Jungbauer@internet-sicherheit.de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen



Agenda



- Einleitung
- Aktuelle Problemstellung anhand eines Beispiels
- Trusted Network Connect
 - Einführung
 - Grundlegende Funktionen
 - Komponenten
 - Schutz vor potentiellen Gefahren
 - Beispiel: WLAN
 - Kritische Betrachtung
 - Marktbetrachtung
- Fazit

Agenda

- Einleitung
- Aktuelle Problemstellung anhand eines Beispiels
- Trusted Network Connect
 - Einführung
 - Grundlegende Funktionen
 - Komponenten
 - Schutz vor potentiellen Gefahren
 - Beispiel: WLAN
 - Kritische Betrachtung
 - Marktbetrachtung
- Fazit

Einleitung – Netzwerksicherheit heute

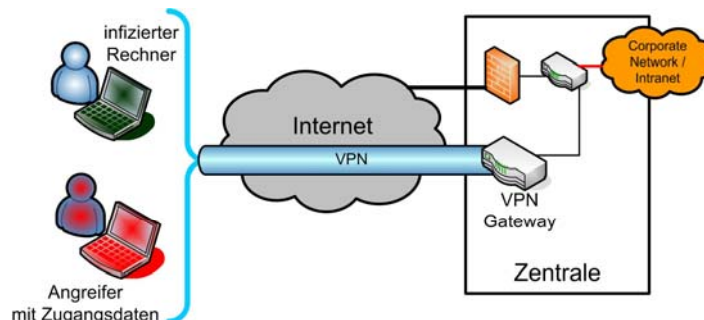
- Zunehmende Vernetzung / Verteilte Systeme
- Zunehmende Gefahr durch Malware (insb. Trojaner und Rootkits)
- Absicherung von Netzwerkzugriffen meist über Nutzerauthentifizierung
- Keine Integritätsprüfung der verwendeten Rechnersysteme
 - =>Keine Unterscheidung zwischen vertrauenswürdigen und nicht vertrauenswürdigen Rechnersysteme
- Folgen
 - **Gefährdung** des Netzwerks **durch Malware und Eindringlinge**
 - Netze sind **nicht vertrauenswürdig**
 - **Kein vertrauenswürdiger Datenaustausch** möglich

Agenda

- Einleitung
- Aktuelle Problemstellung anhand eines Beispiels
- Trusted Network Connect
 - Einführung
 - Grundlegende Funktionen
 - Komponenten
 - Schutz vor potentiellen Gefahren
 - Beispiel: WLAN
 - Kritische Betrachtung
 - Marktbetrachtung
- Fazit

Aktuelle Probleme vorhandener Technologien am Beispiel VPN

- VPN-Verbindung zwischen Außendienstmitarbeiter und Zentrale
- Kein Schutz vor Angriffen von einem mit Malware infizierten Rechner
 - Grund: Keine Integritätsprüfung der Geräte möglich
- Kein Schutz vor gestohlenen Zugangsdaten des VPN-Clients
 - Grund: Keine Überprüfung der Geräteidentität möglich



Agenda

- Einleitung
- Aktuelle Problemstellung anhand eines Beispiels
- Trusted Network Connect
 - Einführung
 - Grundlegende Funktionen
 - Komponenten
 - Schutz vor potentiellen Gefahren
 - Beispiel: WLAN
 - Kritische Betrachtung
 - Marktbetrachtung
- Fazit

TNC – Einführung (1/2)

- Trusted Network Connect von der Trusted Computing Group
- Entwickelt von der TNC Subgroup der TCG mit 75+ Mitgliedern
- Ziele:
 - Überprüfung der Endpunkt-Integrität
 - Zugriffskontrolle
- Eigenschaften:
 - Agenten-basiert
 - Aktuell: Version 1.1 (1. Mai 2006)
 - Noch nicht alle Schnittstellen spezifiziert
 - Offene Spezifikation
 - Optional mit TPM-Unterstützung



TNC – Einführung (2/2)

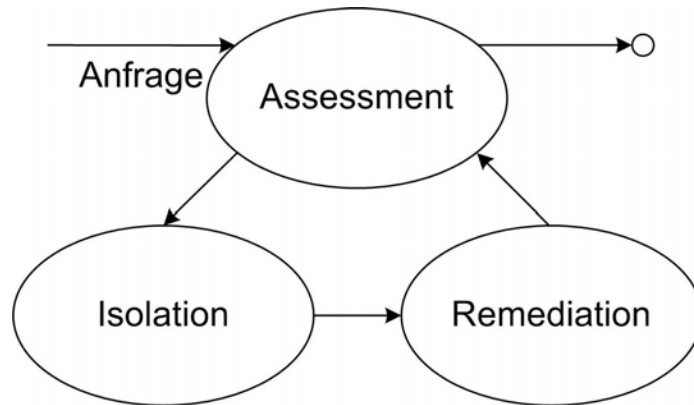
- TNC baut auf vorhandene Technologien auf
Vorteil → Integration in bestehende Infrastrukturen möglich
- Netzwerkzugriff
 - 802.1x
 - VPN
 - PPP
- Nachrichtentransport
 - EAP
 - TLS & HTTPS
- Authentifizierung
 - Radius Server
 - Diameter

TNC – Grundlegende Funktionen

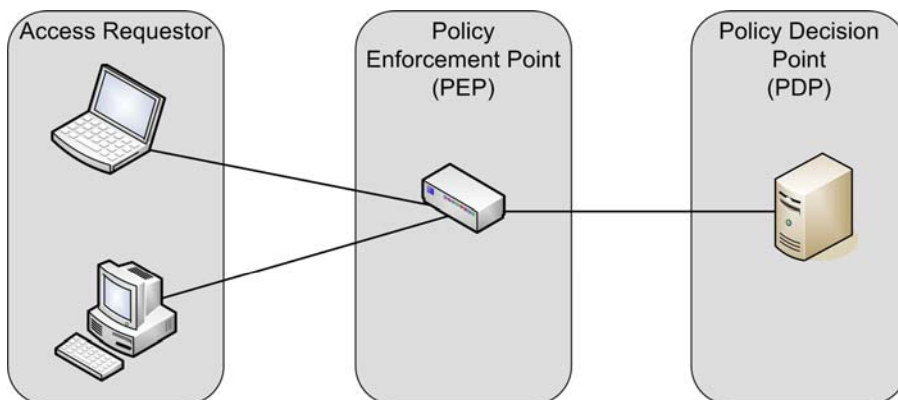
Überprüfung der Vertrauenswürdigkeit:

- Policy-abhängige Zugriffssteuerung für Netzwerke
- Integritätsprüfung - Messen des Systemzustands (Konfiguration der Endgeräte) und Überprüfung dieser Zustände gemäß Policies (Assessment-Phase)
- Isolation von potentiell gefährlichen Rechnersystemen bei Nichterfüllung der Policy (Isolation-Phase)
- Wiedereingliederung nach Wiederherstellung der Integrität (Remediation-Phase)
- Erweiterter Integritätscheck durch TPM-Nutzung
 - z.B. Binden von Zugangsdaten an ein bestimmtes Rechnersystem, Signierung von Messwerten

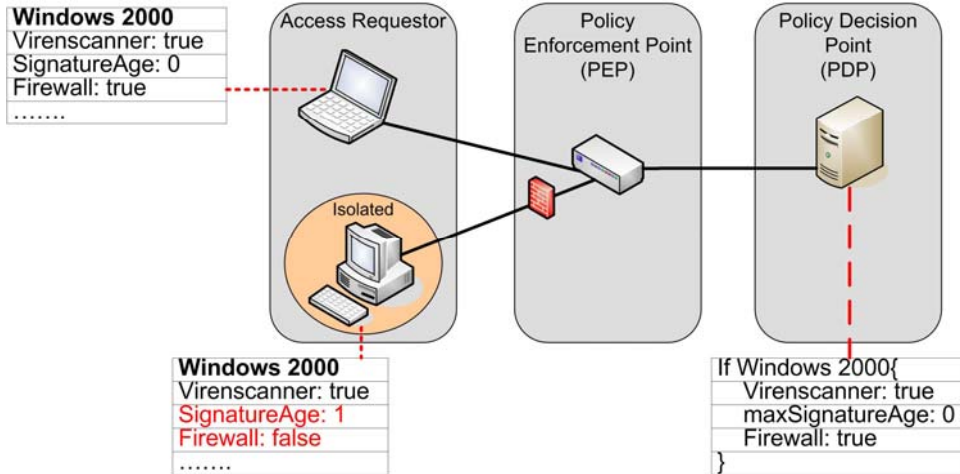
TNC – Zusammenhang der Phasen



TNC - Komponenten

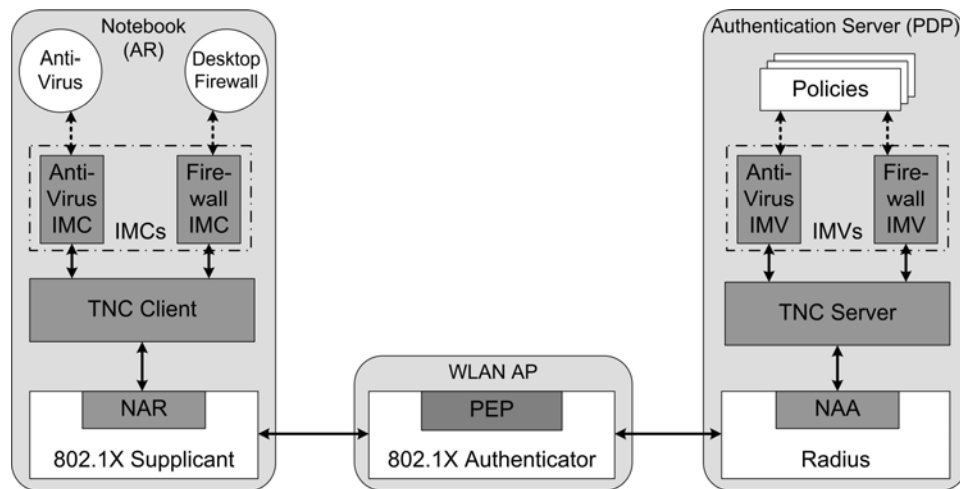


TNC – Schutz vor potentiellen Gefahren



© Marian Jungbauer, Institut für Internet-Sicherheit (ifis)

TNC – Ein Beispiel: WLAN



© Marian Jungbauer, Institut für Internet-Sicherheit (ifis)

Betrachtung des Marktes

- Alternativen?
 - Microsoft NAP (proprietär und Softwareabhängig)
Vorraussichtlich Mitte 2007 verfügbar
 - Cisco NAC (proprietär und Hardware-/Softwareabhängig)
Verfügbar. Benötigt Hardware von Cisco
 - Weitere Ansätze (proprietär)
Teils verfügbar
- Der Markt ist noch nicht „verteilt“

Kritische Betrachtung (1/2)

- Administration
 - Erhöhter Aufwand besonders in heterogenen Netzwerken
 - Jede Konfiguration muss durch Policies abgedeckt werden
 - Gefahr zu restriktiver Policies
 - Mitarbeit der Hardware/Softwarehersteller nötig
- Sicherheit
 - Bei Agenten-basierten Systemen: Gefahr gezielter Angriffe zur Veränderung der Messwerte
 - Anhand von Cisco NAC auf der Black Hat Konferenz 2007 vorgeführt
 - Anmerkung: Sicherheitsplattformen können hier helfen
TNC bietet durch Offenheit eine mögliche Integration in solche Plattformen

Kritische Betrachtung (2/2)

- Standardisierung
 - Alle bisherigen Lösungen inkompatibel zueinander
=> Standardisierungsbedarf
 - Erste Bestrebungen der Standardisierung durch die IETF
 - Network Endpoint Assessment (NEA) Working Group
 - Bis jetzt nur ein Draft "Overview and Requirements" in Version 2 (1. Mai 2007) veröffentlicht
 - Mitglieder unter anderem Cisco und Intel
 - Eine (offene) Standardisierung ermöglicht auch eine einfachere Portierung auf neue Plattformen (z.B. Sicherheitsplattformen)

Fazit

- Zunehmende Vernetzung und zunehmende Anzahl an Gefahren
- Vorhandene Lösungen (VPN) sind nicht ausreichend für vertrauenswürdige Netzwerkverbindungen
- Mit einer Integritätsprüfung werden vertrauenswürdige Netzwerkverbindungen möglich
 - TNC ist ein offener Lösungsansatz mit TPM-Unterstützung
- Vorhandene Lösungen sind nicht kompatibel zueinander
 - ⇒ Standardisierungsbedarf

Trusted Network Connect

Vielen Dank für Ihre Aufmerksamkeit

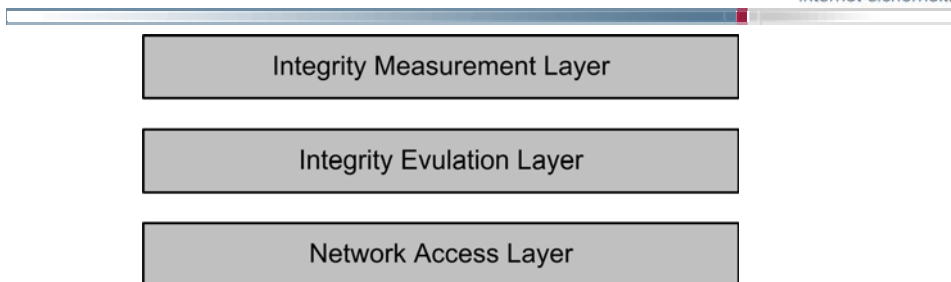
Fragen ?

Marian Jungbauer
Marian.Jungbauer@internet-sicherheit.de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen

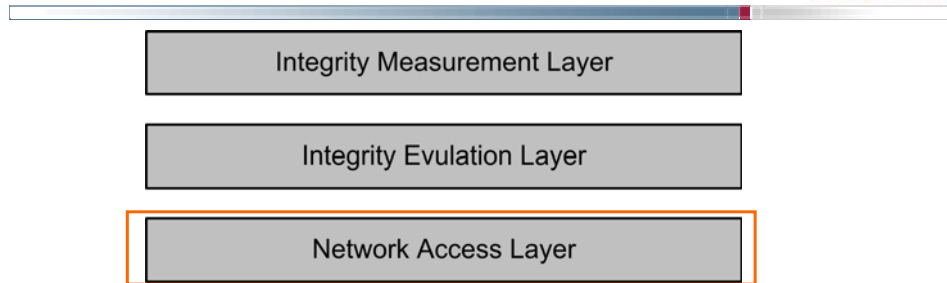


TNC – Detail – Schichtenmodell (1/4)



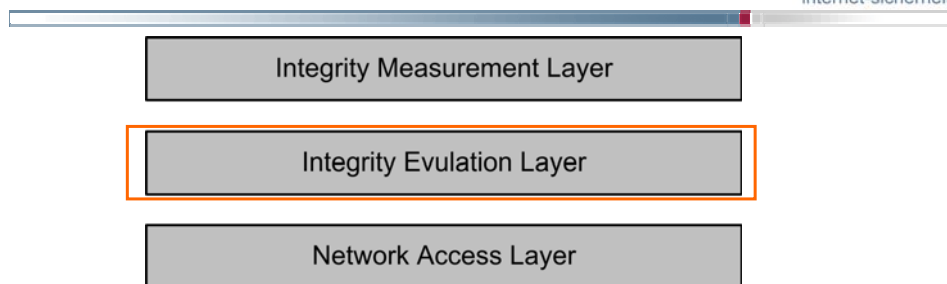
- 3-Schichtmodell
- Setzt auf vorhandene Modelle auf

TNC – Detail – Schichtenmodell (2/4)



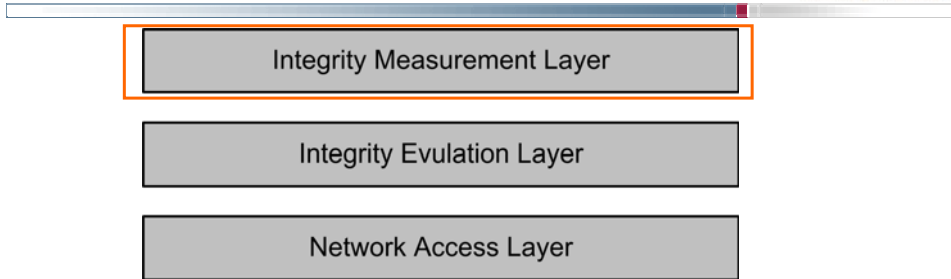
- Erstellung, Durchführung und Abbau der Netzkommunikation
- Entgegennahme bzw. Ausstellung von Anfragen
- Ausführung von Handlungsempfehlungen der Integrity Evaluation Schicht.
- Verhandene Technologien (wie VPN und 802.1X) werden unterstützt
- Beinhaltet VPN-Clients und Gateways sind dieser Schicht zuzuordnen

TNC – Detail – Schichtenmodell (3/4)



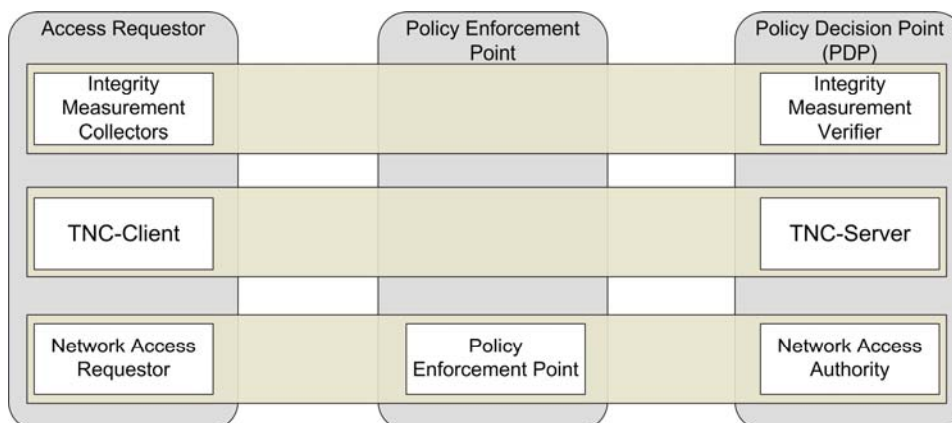
- Funktionen zur Integritäts-Prüfung des Client
- Sammlung von einzelnen Handlungsempfehlungen der Integrity Measurement Schicht
- Erstellung einer Gesamt-Handlungsempfehlung (für den NAL)

TNC – Detail – Schichtenmodell (4/4)

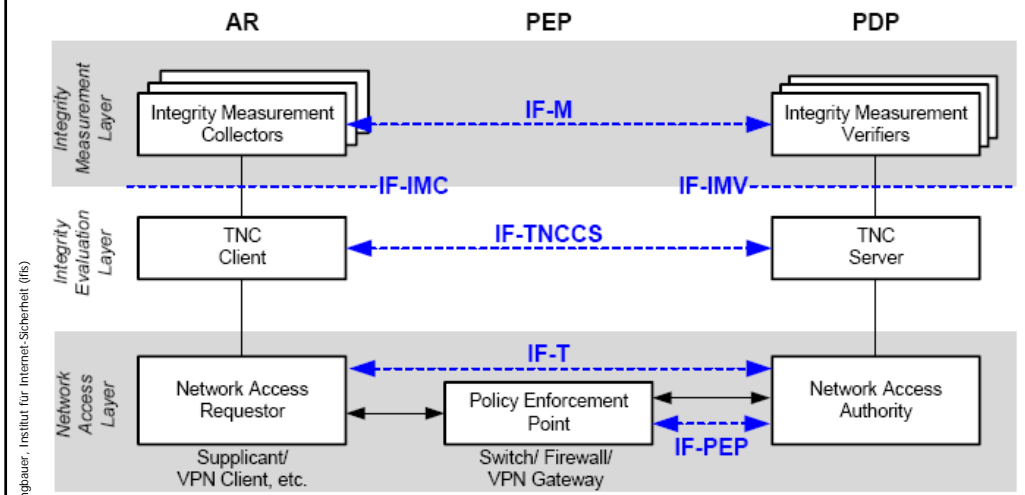


- Sammlung von Messdaten und Erfassung des aktuellen Integritätsstatus des Client.
- Anfrage entsprechender Messdaten zur Erfüllung von Policies
- Ausstellungen einzelner Handlungsempfehlungen (für den IEL)

TNC – Detail – Komponenten



TNC – Detail –Schnittstellen

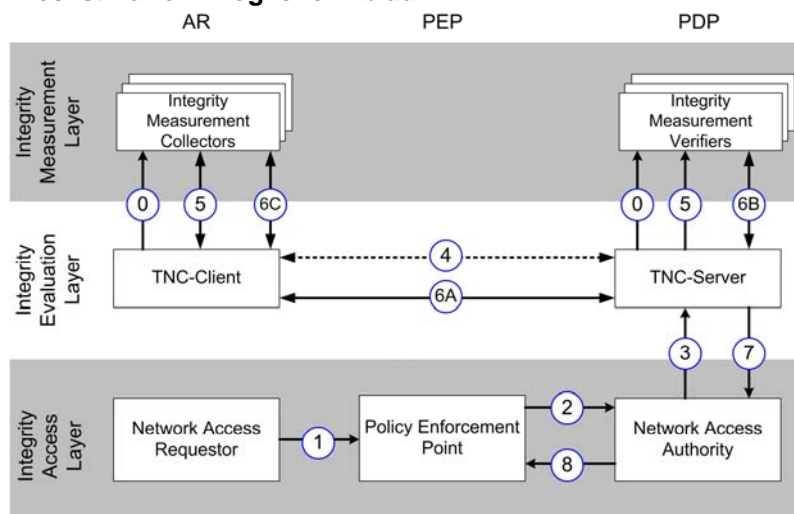


© Marian Jungbauer, Institut für Internet-Sicherheit (IfIS)

Quelle: https://www.trustedcomputinggroup.org/specs/TNC/TNC_Architecture_v1_1_r2.pdf

TNC – Detail Ablauf eines Netzwerkzugriffs

Dies ist nur ein möglicher Ablauf

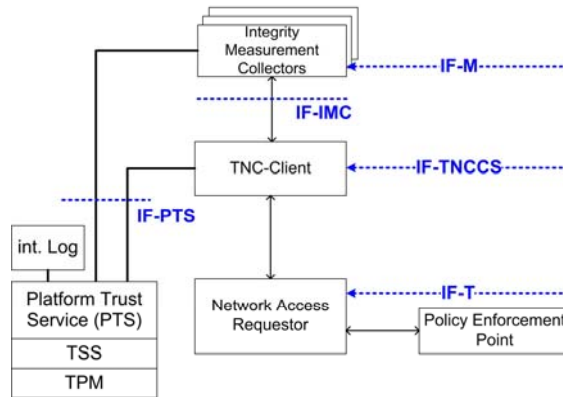


© Marian Jungbauer, Institut für Internet-Sicherheit (IfIS)

Quelle: https://www.trustedcomputinggroup.org/specs/TNC/TNC_Architecture_v1_1_r2.pdf

TNC – Detail – Mehrwert durch TPM

- Nutzung der TPM-Funktionen zur Erhöhung der Vertrauenswürdigkeit
 - z.B. Aussage über Plattform-Integrität durch Secure Boot



© Marian Jungbauer, Institut für Internet-Sicherheit (IfIS)

Quelle: https://www.trustedcomputinggroup.org/specs/TNC/TNC_Architecture_v1_1_r2.pdf 27