IF-MAP

Master-Praktikum „Android“

Michael Eckel

Fachhochschule Gießen-Friedberg

5. November 2010

Gliederung

Problemstellung

Übliches Szenario eines Verbindungsaufbaus

1. Client meldet sich im Netzwerk an
2. Client authentifiziert sich mittels 802.1X
3. Client kann im Netzwerk arbeiten

Problemstellung

Übliches Szenario eines Verbindungsaufbaus

1. Client meldet sich im Netzwerk an
2. Client authentifiziert sich mittels 802.1X
3. Client kann im Netzwerk arbeiten

Reicht diese Art der Authentifizierung aus?
Ist sichergestellt, dass der Client vertrauenswürdig ist?

Problemstellung

Übliches Szenario eines Verbindungsaufbaus

1. Client meldet sich im Netzwerk an
2. Client authentifiziert sich mittels 802.1X
3. Client kann im Netzwerk arbeiten

Reicht diese Art der Authentifizierung aus?
Ist sichergestellt, dass der Client vertrauenswürdig ist?

- NEIN!
- Client könnte kompromittiert sein (Virus, Trojaner, . . .)
- Client könnte ferngesteuert werden

Lösungsansatz – NAC (Network Admission Control)

NAC (Network Admission Control)

- Prüft Client-Authentifizierung
- Prüft, ob der Client bestimmte Richtlinien einhält
- Richtlinien könnten sein:
  - Aktualität des Virenscanners
  - Betriebssystemupdates

TNC (Trusted Network Connect)

TNC ist eine von der TCG spezifizierte NAC Lösung

TNC – Architektur

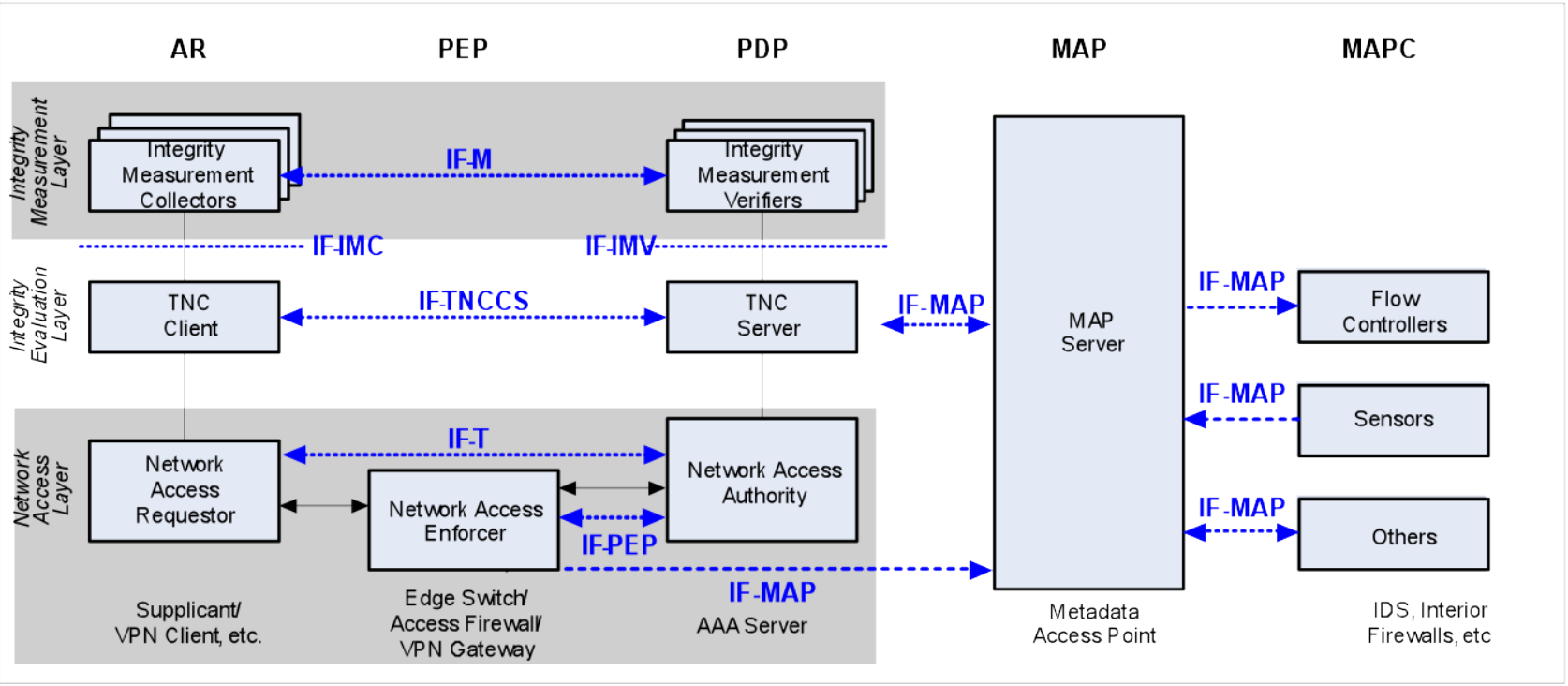

Abbildung: IF-MAP in der TNC-Architektur [Tru12]

TNC – Architekturkomponenten (I)

Vertikale Schichten

- **Access Requestor (AR)**
  - Endgerät, welches versucht in ein TNC-geschütztes Netz zu kommen
- **Policy Decision Point (PDP)**
  - entscheidet, ob AR sich mit dem Netzwerk verbinden darf
- **Policy Enforcement Point (PEP)**
  - führt aus, was der PDP entscheiden hat
  - Beispiele von PEPs: Switch, Firewall, VPN-Gateway

TNC – Architekturkomponenten (II)

Horizontale Schichten

- **Integrity Measurement Layer (IML)**
  - AR und PDP tauschen Informationen über die Messung von Clients aus
  - *Integrity Measurement Collectors (IMC)* sind Bestandteile des AR
  - *Integrity Measurement Verifiers (IMV)* sind Bestandteile des PDP
- **Integrity Evaluation Layer (IEL)**
  - prüft Integrität des AR mit Hilfe der Ergebnisse des IML
- **NAL (Network Access Layer)**
  - gewährleistet die gewöhnlichen Sicherheitsstandards wie 802.1X

IF-MAP

- Konzept zum Speichern von Status-Informationen über Endgeräte und Benutzer
- Statusinformationen können sehr verschieden sein:
  - IP-/MAC-Adresse
  - Authentifizierungsstatus
  - Authorisierungsstatus
  - Standort-Informationen
- Informationen werden vom MAP-Server gespeichert (MAP: Metadata Access Point)
- Kurz: Ereignisdatenbank mit Abonnement-, Such und Veröffentlichungsfunktion

Beispielszenario

1. Benutzer A authentifiziert sich mit seinem Endgerät mit der MAC-Adresse `AA:BB:CC:DD:EE:FF` an einem 802.1X-Switch
2. Switch sendet diese Information an den MAP-Server
3. Endgerät bekommt vom DHCP-Server die IP-Adresse `192.168.1.2` zugewiesen
4. DCHP-Server meldet dies dem MAP-Server
5. MAP-Server weiß nun, dass ein Benutzer A sich authentifiziert, die IP-Adresse `192.168.1.2` zugewiesen bekommen hat und die MAC-Adresse `AA:BB:CC:DD:EE:FF` besitzt

Der MAP-Server bildet also einen Informationsgraphen

Anwendungsfälle

- **Veröffentlichen**
  - DHCP-Server verteilt eine neue IP-Adresse
  - Sensor erkennt einen Portscan
  - mobiles Gerät veröffentlicht seinen Standort
- **Suchen**
  - ein Endgerät fragt den Standort eines anderen Endgerätes ab
- **Abonnieren**
  - Firewall abonniert Metadaten über ein Endgerät, um im Falle eines Verstoßes gegen die Netzbestimmungen den Netzverkehr zu blockieren

MAP-Komponenten

- **MAP-Client (MAPC)**
  - eine Netzwerkkomponente, die IF-MAP benutzt, um mit dem MAP-Server zu kommunizieren
- **MAP**
  - der zentrale Punkt in der IF-MAP-Architektur
  - wird vom MAP-Server repräsentiert

Datenmodell von IF-MAP (I)

- **Identifier**
  - Metadaten werden an Identifier gebunden
  - Identifier sind z. B.: IP-Adresse, MAC-Adresse, Benutzername, E-Mail-Adresse
- **Link**
  - beschreibt die Verbindung zwischen zwei Identifiern
  - Beispiel: DHCP-Server stellt Verbindung zwischen IP- und MAC-Adresse her
- **Metadaten**
  - sind frei wählbar
  - TCG hat eine Spezifikation für Security-Metadaten veröffentlicht
  - Hersteller-abhängige Metadaten möglich

Datenmodell von IF-MAP (II)

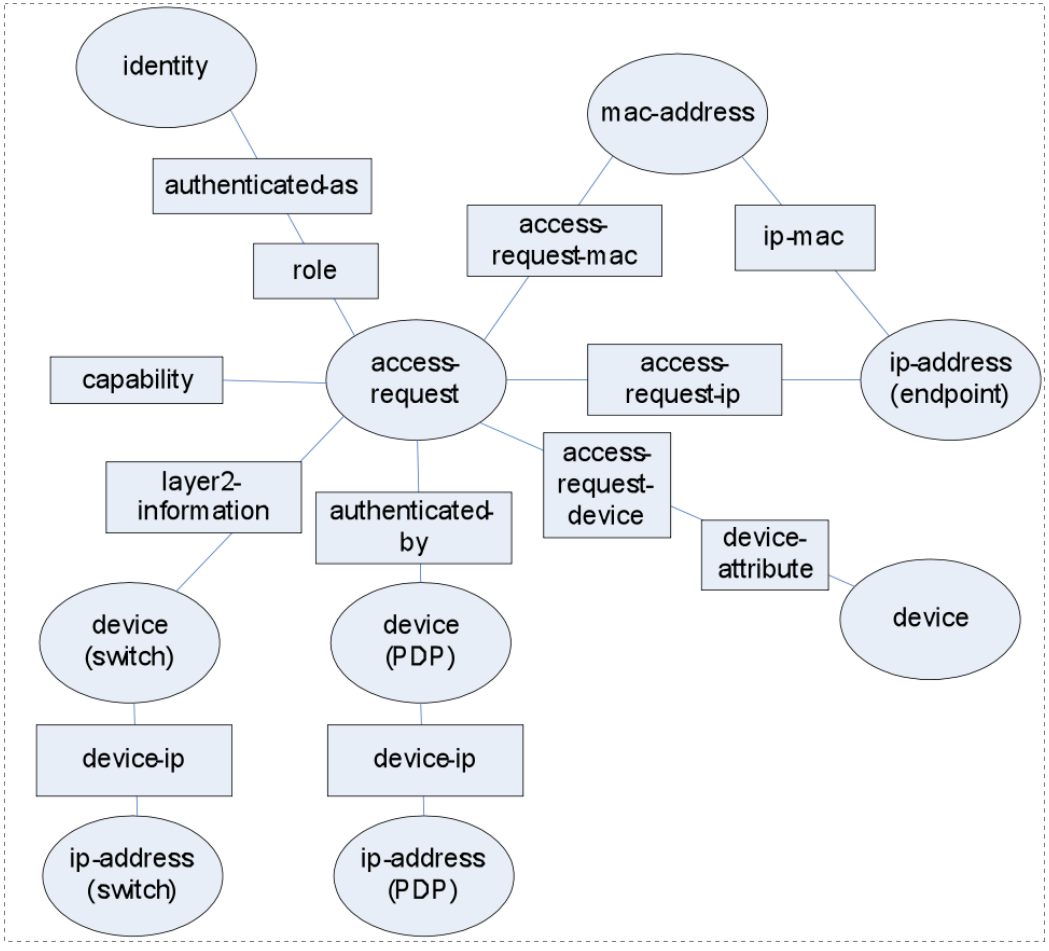

Abbildung: Datenmodell von IF-MAP [Tru12]

Kommunikationsmodell

- MAP-Client kann bis zu zwei Kanäle zum MAP-Server aufbauen
- Kanalarten:
  - **Synchron:** SSRC (Synchronous Send-Receive Channel)
    - Veröffentlichen
    - Suchen
  - **Asynchron:** ARC (Asynchronous Receive Channel)
    - Abonnieren

Operationen zum Verbindungsaufbau

Verbindungen werden immer vom Client zum Server aufgebaut!

- **newSession**
  - Aufbau einer Verbindung
  - Option zur Aufrechterhaltung oder Abbau nach 180 sec
  - keinerlei Authentifizierung
- **renewSession**
  - gleiche Funktionalität wie „keepalive pinging“
- **poll**
  - eigentlich keine Operation zum Verbindungsaufbau
  - dennoch beeinflusst sie das Verbindungsmanagement
  - poll muss immer über einen ARC geschickt werden
  - Verbindung bleibt bestehen, bis der Server antwortet
- **endSession**
  - beendet die Verbindung zum Server

Operationen zum Datenaustausch (I)

Verbindungen werden immer vom Client zum Server aufgebaut!

- **publish**
  - veröffentlichen und löschen von Metadaten
  - drei verschiedene Arten:
    - *Publish-Update:* Veröffentlichen und Speichern
    - *Publish-Notify:* Nur Veröffentlichen
    - *Publish-Delete:* Löschen
- **subscribe**
  - abonnieren eines Identifiers
  - standardmäßig werden alle Daten abonniert
  - filtern möglich

Operationen zum Datenaustausch (II)

- **poll**
  - *asynchrones* Abfragen von Metadaten für abonnierte Identfier
  - zur Not abwarten, bis Metadaten verfügbar
- **search**
  - *synchrones* Abfragen von Metadaten
  - sofortige Antwort
  - es werden keine Identifier abonniert
- **purgePublish**
  - Anfrage zur Löschung der Daten eines Publishers
  - je nach Konfiguration kann der Server dies jedoch verweigern

Quellen I

[Ben10] Bender, Waldemar:

Entwicklung eines IF-MAP Clients für die Android Plattform, Fachhochschule Hannover, Diplomarbeit, August 2010.

http://sit.sit.fraunhofer.de/smv/publications/download/20100817_Thesis_Bender_final.pdf

[Tru12] Trusted Computing Group:

TCG Trusted Network Connect TNC IF-MAP Binding for SOAP.

Mai 2012

Fragen?

Danke für die Aufmerksamkeit!