Konzeption, Entwicklung und Projektmanagement von ESUKOM

Prof. Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH, Fahrenheitstr. 9, D-28359 Bremen

18.-19.10.2011, Bonn

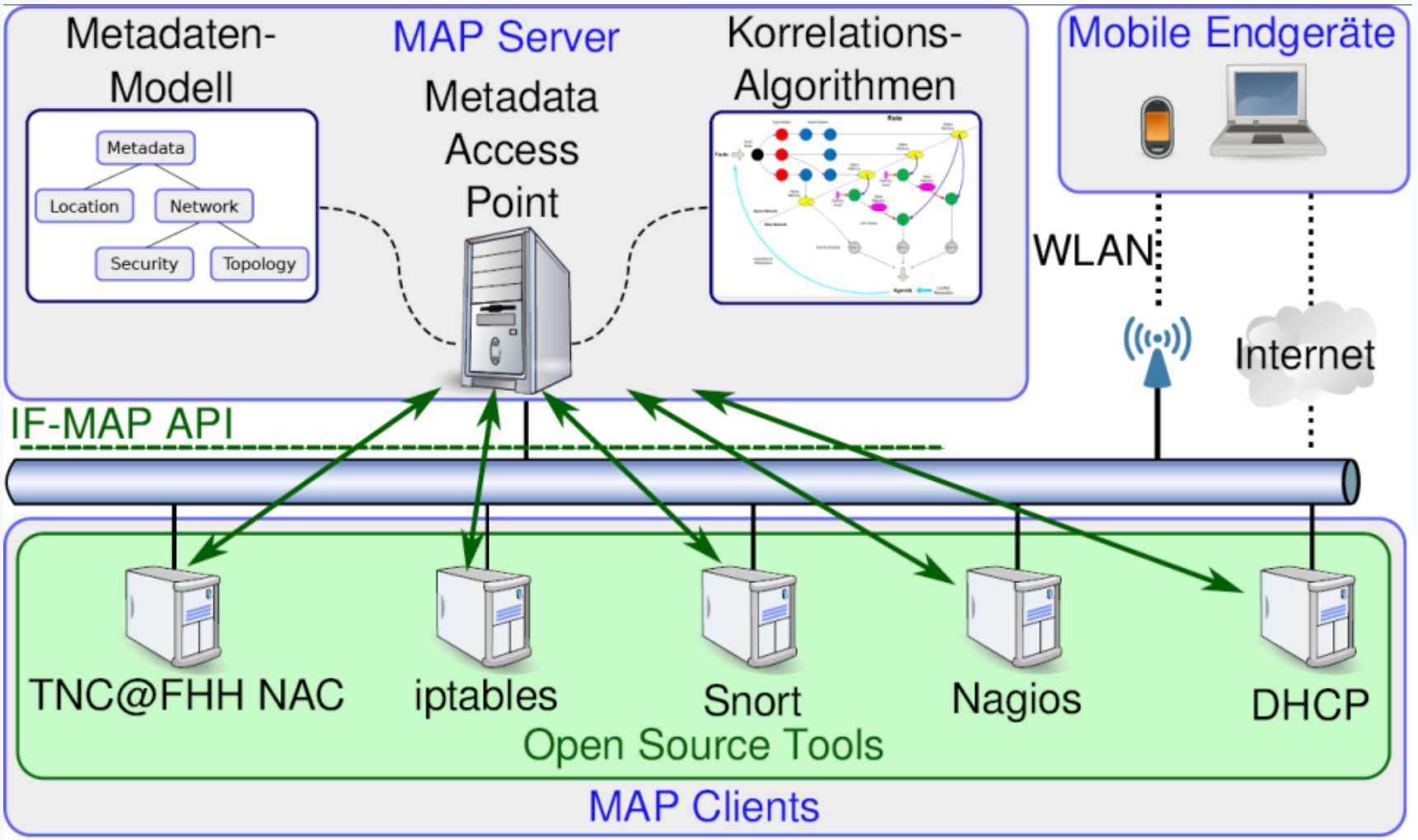
ESUKOM

ESUKOM

Dienstleistungen / Portfolio

- **Technologie- und Markttrends**, um strategische Entscheidungen für und mit dem Kunden vor einer Projektrealisierung treffen zu können
- **Solutions (Lösungen)** zur Identifizierung der Probleme und Angebot einer Lösung für die Umsetzung eines Projekts
- Kundenorientierte **Workshops, Coaching, Schulungen** zur Projektvorbereitung und -begleitung
- **Software-Entwicklung** zur Anpassung von Schnittstellen und Entwicklung von IT-Projekten
- Schaffung innovativer eigener **Produkte**
- Nationale und internationale **Förderprojekte** auf Basis neuer Technologien, um neues Know-how aufzubauen oder Fördermöglichkeiten aufzuzeigen

ESUKOM High-Level-Architektur



Teilvorhaben der DECOIT GmbH

- Fokus
  - Projektmanagement und -koordination
  - Konzeption & Weiterentwicklung von Open-Source-Tools (wie Snort, iptables, Android, RADIUS, Nagios)
  - Technologische Basis: IF-MAP Protokoll der TCG
- Aufgabendetails im Überblick
  - Verwertung und Außendarstellung (Webseite, Konferenzen, Veröffentlichungen etc.)
  - Definition von Sicherheitsaspekten von praxiserprobten Szenarien
  - Sicherheitsanalyse von Praxisszenarien
  - Entwicklung von IF-MAP-Clients für Open-Source-basierte Systeme
  - Integration der entwickelten IF-MAP-Clients in den neuen IF-MAP-Server
  - Analyse der vorhandenen IF-MAP-Metadaten
  - Mitarbeit an der Modellierung und Formalisierung des Metadatenmodells
  - Integration des Modells in die eigenen IF-MAP-Clients
  - Definition von Security Policys für definierte Szenarien
  - Mitentwicklung von Algorithmen, basierend auf dem Metadaten-Modell/Vokabular
  - Integration der Algorithmen in die entwickelten IF-MAP-Clients
  - Strukturieren und Verfassen des Best-Practice-Dokumentes

Herausforderungen

- Standardkonforme Erweiterung bestehender Open-Source-Tools mit IF-MAP
  - iptables
  - Android (Smartphone)
  - Snort
  - RADIUS
  - Nagios
- Definition relevanter Metadateninformationen
- Integration der IF-MAP-Clients mit dem IF-MAP-Server
- Beherrschung der Datenmengen(!)

Aktueller Stand (1)

- Verwertung und Außendarstellungen
  - Die Webseite des Projektes ist auf dem neusten Stand
  - An diversen Konferenzen wurden aktiv teilgenommen
  - Verschiedene Veröffentlichungen in Fachzeitschriften sind erfolgt und weitere sind in Arbeit
- Forschungsarbeiten
  - Identifikation relevanter Metadaten wurde angefangen
  - Spezifikation des Metadatenmodells und der Vokabularien steht noch aus
  - Konsolidierung der Metadaten steht noch aus

Aktueller Stand (2)

- Prototypenentwicklung
  - IF-MAP Clients
    - Nagios: liegt in der ersten Version vor
      - Erkennung, Aufbereitung und Veröffentlichung von Nagios-Events: Host-State und Service-State („Publish“)
    - Snort: liegt in der ersten Version vor
      - Aufbereitung und Veröffentlichung von Snort-Meldungen: verdächtiger Datenverkehr, Portscan-Erkennung etc. („Publish“)
    - iptables: liegt in der ersten Version vor
      - Aufbereitung und Veröffentlichung von erkannten Datenströmen („Publish“)
      - Registrierung für die Benachrichtigung bei Änderungen an den Metadaten durch den MAP-Server („Subscribe“)
      - Periodische Abfrage von Änderungen an den Metadaten der registrierten Clients („Poll“)
      - Evtl. darauf folgendes Enforcement eines Clients, wenn bestimmte, vorher festgelegte Kriterien eintreffen (z.B. bei Vorhandensein bestimmter Metadaten)

Aktueller Stand (3)

- Prototypenentwicklung
  - IF-MAP Clients
    - Android: liegt in der ersten Version vor
      - Auslesen unterschiedlicher Geräteeigenschaften des Endgerätes : IP-Adresse, MAC, IMEI, IMSI, OS-Version, installierte Anwendungen inkl. Berechtigungen, Position des Endgerätes (GPS/Cell-Based) etc.
      - Veröffentlichung dieser Eigenschaften an den MAP-Server („Publish“)
    - RADIUS: ist noch in Arbeit, Veröffentlichung in Kürze
      - Auslesen und Veröffentlichung von RADIUS-Informationen: An/Abmeldung eines Clients („Publish“)
  - Vollständige Unterstützung von IF-MAP 2.0

Weitere Arbeiten

- Metadaten-Vokabular
  - Abbildung der identifizierten Merkmale auf IF-MAP
    - Nagios
    - Snort
    - iptables
    - Android
    - RADIUS
  - Integration des Fraunhofer-Modells in IF-MAP
- Korrelation
  - Einfache (statische) Auswertung relevanter IF-MAP-Client-Daten
- Prototypenentwicklung
  - IF-MAP-Client: Zertifizierung(?)
  - Remote-Teilnahme am kommenden TNC Plug-Fest in San Jose (USA)
  - Teilnahme am ersten TNC Plug-Fest in Deutschland (Darmstadt) in 2012
- Best-Practice-Report
  - Definition von Best-Practice-Richtlinien zur Konsolidierung von Metadaten in IF-MAP-Infrastrukturen

Vielen Dank

Fragen?

ESUKOM

ESUKOM

Copyright 2010-2012

Das dem Projekt zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen „01BY1050“ gefördert. Die Verantwortung für den Inhalt liegt bei den Autoren.