Lehrstuhl Netzarchitekturen und Netzdienste
Institut für Informatik
TU München

Informationsveranstaltung
für das Seminar

Future Internet

Sommersemester 2009

Prof. Dr.-Ing. Georg Carle
Lehrstuhl für Netzarchitekturen und Netzdienste
TU München

Ablauf

- Organisation und Betreuer
- Hinweise zur Themenbearbeitung
- Bewertung
- Vorstellung der Themen
- Themenvergabe

Organisation und Betreuer – Blockseminar Future Internet

- **Organisation:** Prof. Carle, Corinna Schmitt
- **Ort und Zeit:** 16./17. April 2009, 9-17 Uhr, MI 01.06.011
  genaueres wird noch bekannt gegeben
  Es wird eine Anwesenheitsliste geführt.
- „Nachzügler“ bitte über unser Anmelde-Tool anmelden!
- **Teilnehmer werden auf eine Mailingliste gesetzt, über die wichtige Informationen mitgeteilt wird.**
- Jedes Vortragsthema ist fest mit einem Termin verknüpft
- **Web:**
  http://www.net.in.tum.de/en/teaching/ss09/seminars/

Deadlines – Blockseminar Future Internet

- **Folien: 2 Wochen vor Vortrag**
- **Ausarbeitungen: 29.3.2009 werden dann zum Reviewen verteilt**
- **Reviewrückgabe: elektronische Rückgabe am 17.4.2009**
- **Überarbeitete Ausarbeitungen: elektr. Abgabe bis zum 30.4.2009**

- Das Konzept des Seminars setzt voraus, dass die Teilnehmer die Termine einhalten.

- Auf der Seminarhomepage werden Templates für die Folien, die Ausarbeitung und die Reviews zur Verfügung gestellt.

Hinweise zur Themenbearbeitung - allgemein

- Frühzeitige Kontaktaufnahme mit dem Betreuer

- **Literatur:**
  - Material vom Betreuer
  - Zusätzlich meist **selbständige Recherche** gefordert!

- **Recherchemöglichkeiten:**
  - Katalog der Bibliothek
  - Suche über Google und Citeseer
  - Webseiten von Konferenzen, Workshops, Standardisierungsorganisationen,...

- **Ziel:**
  - nicht einfach nur Informationen anlesen und wiedergeben, sondern
  - **eigenes Verständnis entwickeln** und **Verstandenes mit eigenen Worten erklären**
  - **Neutrale Bewertung des Themas**
    - Die eigene Meinung kann – wenn gewünscht – in einem extra gekennzeichneten Abschnitt vermittelt werden

Hinweise zur Themenbearbeitung - Vortrag

- Dauer: 20 - 30 Minuten
- Stil (Layout) nach Vorlage

- **Die anderen Seminarteilnehmer sollen möglichst viel mitnehmen!**
- verständliche Aufbereitung des Stoffes, z.B. durch (eigene) Abbildungen
- Einbeziehen der Zuhörer, Interaktion
- Quellen von Fremdmaterial (Bilder etc.) angeben!

- Geplant: Videoaufzeichnung zur eigenen Nachbetrachtung!

Hinweise zur Themenbearbeitung - Ausarbeitung

- Längenvorgabe: 5 - 8 Seiten im IEEE-Paper-Format (zweispaltig)
- Ausarbeitung wird korrigiert und ggf. zur Verbesserung zurückgegeben
- Gliederung wissenschaftlicher Artikel einhalten:
  - Kurzfassung
  - Einleitung
  - ...
  - Vergleiche und Bewertungen
  - Zusammenfassung/Fazit/Ausblick
  - Literaturangaben
  - korrekte Literaturangaben

  ➔ mehr Hinweise zur Ausarbeitung werden auf der Webseite bereitgestellt

Reviews

- Betreuer verteilen Reviews, jeder Student bekommt 2 Reviews, der Betreuer ist 3. Reviewer
  - anonym: der Autor kennt die Identität der Reviewer nicht
- Für den Reviewer sind seine geschriebenen Reviews Teil der Note
  → bitte auch kritische Reviews schreiben
- Auf der Seminarseite wird ein Reviewformular zur Verfügung gestellt
- Teile des Review-Formulars:
  - Titel
  - Autor
  - Worum ging es in dem Paper? Hauptpunkte des Themas?
  - Stärken der Ausarbeitung
  - Schwächen der Ausarbeitung
  - Fragen an den Autor (Offene Punkte, Fragen die sich beim Lesen gestellt haben)
  - Sachliche Korrektheit (zb. im Bezug auf die genannten Quellen) (mind. 1 Fehler finden!)
  - Form (Quellen, Bilder, Fußnoten, Rechtschreibung, Zeichensetzung, Grammatik etc.) Referenz ist die Vorlage von der Webseite
  - Überprüfung auf Plagiarismus (ist Text aus anderen Quellen, z.B. Wikipedia kopiert worden, ohne als Zitat gekennzeichnet zu sein)

Bewertung

- **Bewertung:**
  - Vortragsfolien und Vortragsinhalt (nicht der Vortragsstil)
  - Ausarbeitung
  - Geschriebene Reviews
  - regelmäßige Anwesenheit bei den Vortragsterminen (Abzug von 0,3 Notenpunkten oder umfangreichere Ausarbeitung bei unentschuldigtem Fehlen!)

  - Das Seminar wird benotet.

- **Kein Schein bei Plagiarisums!**
  - wörtliche Übernahme von existierenden Texten sind unter Angabe der Quelle als Zitate zu kennzeichnen
  - Nichtbeachtung erfüllt den Tatbestand des Plagiarismus

- **Ausschluß vom Seminar sobald gegen eine der Deadlines verstoßen wird oder Plagiarismus vorliegt.**

Lehrstuhl Netzarchitekturen und Netzdienste
Institut für Informatik
TU München

Themenvorstellung und Themenvergabe für das Blockseminar

Themenübersicht I

- Moderne Botnetze – Marc (vergeben)
- Trusted Platform Module (TPM) – Holger (vergeben)
- IT-Sicherheit – Psychologische Anspekte – Corinna (vergeben HS)
- Datenschutz unter juristischem Blickwinkel – Corinna (vergeben HS)

- Trusted Network Connect - Holger
- Geographic Location/Privacy (GeoPriv) – Holger
- IP Fast Reroute (IPFRR) - Nils
- RSerPool: Standardisierte Server-Replikation – Nils
- Mobilität und Locator-/ID-Split – Nils
- Host Identity Protocol – Andreas
- Datagram Congestion Control Protocol (DCCP) – Andreas
- Zero Configuration Networking – Andreas
- Abhängigkeitsanalyse mit Hilfe von passiven Verkehrsmessungen – Gerhard und Lothar
  - Untersuchung mit Graphen
  - Untersuchung von zeitlichen Korrelationen

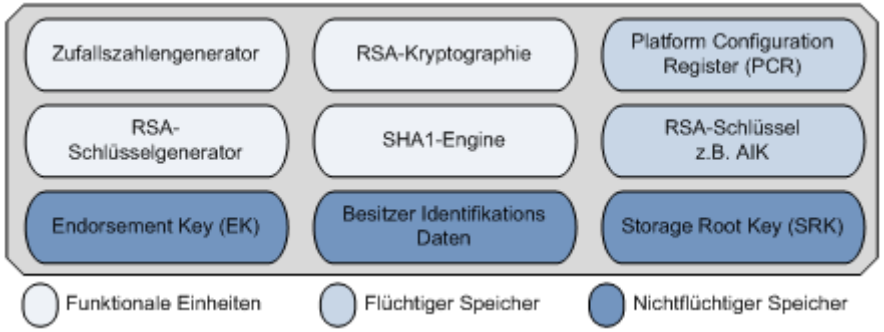
Themenübersicht II

- Simple Network Management Protocol – Marc-Oliver
- DoS-Angriffe - Marc
- Wuala - Marc
- Delay Tolerant Networks – Tobias
- Evolution der Kernnetze im Mobilfunk - Tobias
- Schlauere Navigation durch Mobilfunk? - Tobias

- Weitere Themen der Gruppe Fuhrmann werden ohne Folien vorgetragen

Reminder: Trusted Computing - Holger

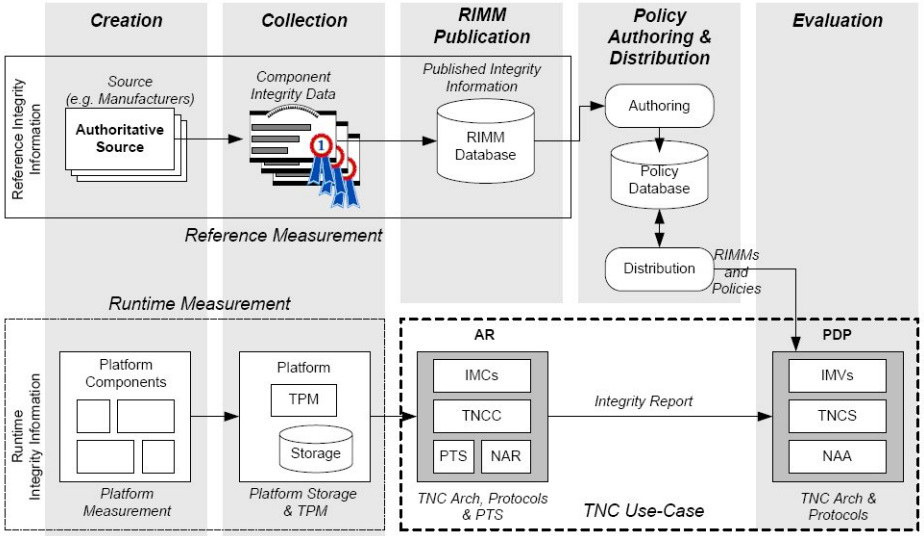
- Das *Trusted Platform Module* (TPM) ist ein fest in einen Gerät eingebauter Cryptochip und dient als „Vertrauensanker“ in ein System
- Eine mit TPM reasisierbare Anwendung ist die *Remote Attestation*. Hierbei wird die Integrität eines Systems einem anderen System bewiesen („Ist das System vertrauenswürdig?“)
- Als Grundlage für die Remote Attestation dient die *Integrity Measurement Architecture* (IMA).
- **Ziel:** Verständnis des Konzepts des „Trusted Computing“, TPM, IMA und die Funktionsweise der Remote Attestation
  - Das Thema ist schon vergeben!



Bilder: Trusted Computing Group, TUM

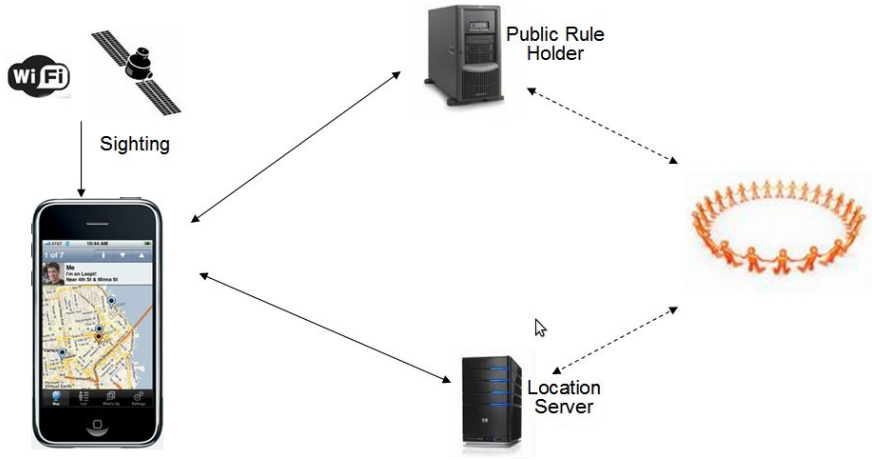
Trusted Network Connect - Holger

- Problem: Mobile Geräte unter User-Kontrolle sind ein mögliches Einfallstor für Schadsoftware in (Firmen) Netzwerke.
- Abhilfe: Nicht nur der Benutzer des Geräts wird beim Netzwerkzugang authentisiert, sondern auch die Konfiguration / der Zustand des Geräts wird überprüft
  - Ist der Virenscanner aktiv und die Virensignaturen aktuell?
  - Sind alle Patches installiert?
  - Auch Remote Attestation des Systems ist denkbar.
- Ziel: Verständnis der TNC Architektur
  - Aufbau / Architektur,
    - v.a. Network Access
  - Assessment
  - Isolation
  - Remediation



Geographic Location/Privacy (GeoPriv) - Holger

- *Location-based Services* benötigen geographische Informationen (Koordinaten, Adresse, …) über ein *Target*
  - Bsp.: Personen können sich gegenseitig per Handy lokalisieren
- GeoPriv sieht Regeln vor, mit denen ein Target bestimmen kann, was mit seinen Geoinformationen geschehen darf
  - Wer kann zugreifen? (Meine Freunde und Kollegen)
  - Wie genau? (Freunde auf 50 Meter genau, für den Chef reicht die Stadt)
- Zusätzlich: die Übermittlung solch sensitiver Daten erfordert Sicherheit.
- Ziel: Verständnis der GeoPriv Architektur und Arbeitsweise



IP Fast Reroute (IPFRR) - Nils

- Bewährte Routingprotokolle reagieren zwar auf Ausfälle …
  - OSPF, IS-IS usw.: ≈100ms
  - BGP sogar 1–10s
  - Protokolle gut und bewährt – ***aber zu langsam!***
- Gewünscht: Schnelle, instantane Reaktion auf Ausfälle
  - "Notfallreaktion", bis Routingprotokoll Ordnung wiederhergestellt hat
  - MPLS: Existiert bereits+funktioniert, **aber:** kompliziert → teuer zu managen (zusätzlicher Layer zwischen IP-Layer und Link Layer)
  - Warum denn nicht auf IP-Ebene? …
- **… ja: IP Fast Reroute (IPFRR)**
  - IETF-Standard: RFC 5286
  - Verschiedene Methoden für IPFRR, z.B. Not-Via-Adressen
- Literatur z.B.:
  - *An evaluation of IP-based Fast Reroute Techniques* (Francois, Bonaventure)
  - *Evaluation of IP Fast Reroute Proposals* (Yang, Gjoka, Ram)
  - RFC 5286

RSerPool: Standardisierte Server-Replikation - Nils

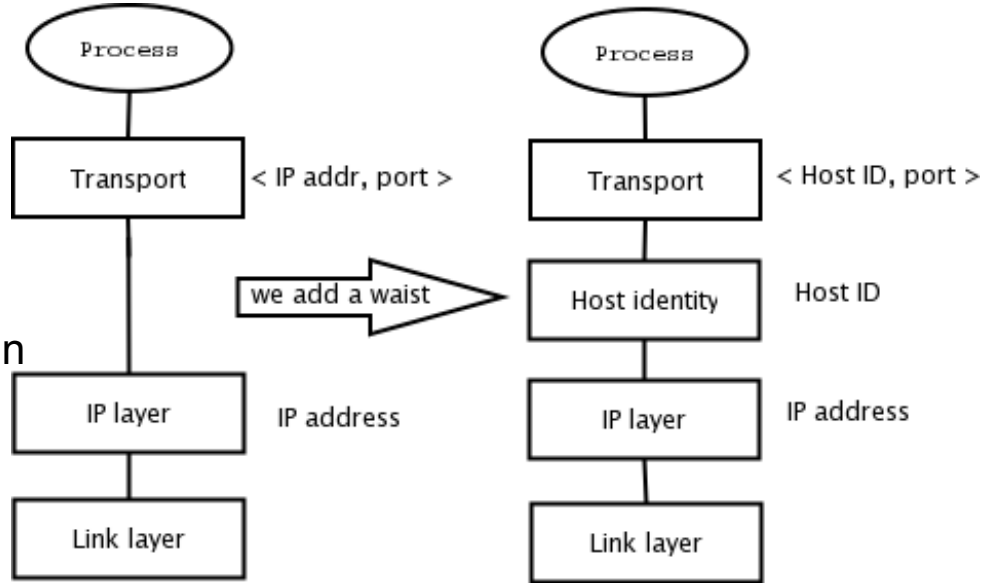
- Häufig: Server poolen (z.B. Webserver, Datenbankserver)
  - weil: Serverausfall = teuer → Redundanz erhöhen
  - oder: Mehrere Server parallel in Betrieb → bessere Leistung
- Pooling → Replikation von Daten zwischen Servern nötig
  - Bislang: Jede Implementierung "kocht ihr eigenes Süppchen"
  - Warum das Rad *n*-mal neu erfinden?
- **→ IETF-Standard: RSerPool-Protokollsuite**
  - Gedacht für zukünftiges Internet
  - Verwendet SCTP (≈Nachfolger-Protokoll von TCP)
    … und diverse darauf aufbauende Protokolle
  - RFC 5351 bis RFC 5356
- Literatur: Diverse, z.B.:
  - *Implementing the Reliable Server Pooling Framework* (Dreibholz, Rathgeb)
  - *The Performance of Reliable Server Pooling Systems in Different Server Capacity Scenarios* (Dreibholz, Rathgeb)
  - *An Application Demonstration of the Reliable Server Pooling Framework*
  - RFCs …?

Mobilität und Locator-/ID-Split - Nils

- Zunehmende Mobilität von Endgeräten: PDAs, Mobiltelefone, Laptops,...
  - → Routing/Switching muss ständig an neue Position angepasst werden
- Mobilität auf Link-Layer? (z.B. GSM/UMTS)
  - IP-Adresse bleibt innerhalb des Netzwerks konstant
  - Aber: kein Roaming zwischen Netzen! (z.B. UMTS→WLAN oder O2→D1)
- Mobilität auf höheren Layern? (z.B. Dynamic DNS; Peer-to-Peer-Netze)
- **Mobilität auf IP-Layer**
  - Roaming zwischen verschiedenen Netzwerken
  - z.B. Mobile IP (Mobile IPv4 Triangular Routing, Mobile-IPv6-Tunnels)
  - Grundsatzproblem: IP-Adresse ist *Locator* und *Identifier* in einem
- **Pläne für Future Internet**
  - ***"Locator-ID-Split":*** häufiges Buzzword
  - *Evolutionary* vs. *Revolutionary*
- Literatur: Diverse (längere Liste gibt's bei mir)
  - z.B. *Evaluating the Benefits of the Locator/Identifier Separation*
  - Selbständige Recherche/Selektion der interessantesten Quellen
  - Bei Bedarf evtl. zwei Vorträge zum Thema

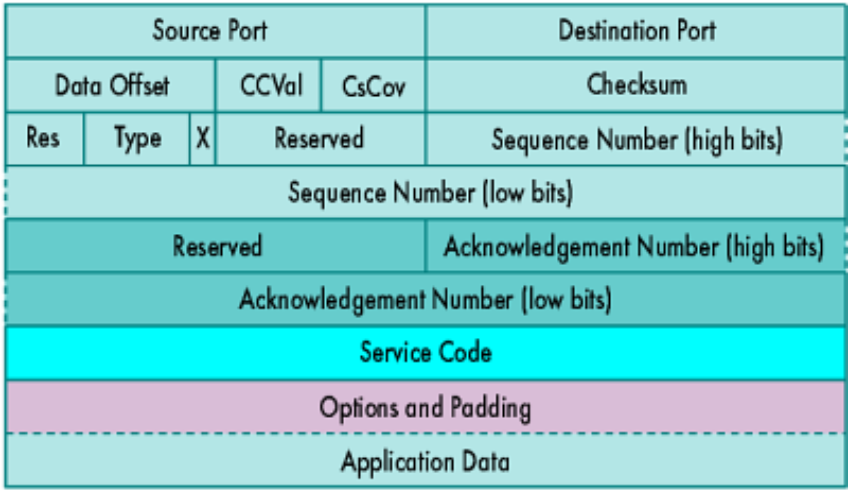
Host Identity Protocol - Andreas

- Im heutigen Internet gibt es zwei Namespaces
  - Domain Names
  - IP Adressen
- Durch doppelte Belegung von IP Mobilität eingeschränkt
  - Transport Protokolle werden an IP-Adressen gebunden
- Das Host Identity Protocol (HIP) führt einen neuen Namespace ein
  - Lokator/Identifikator Split
  - Cryptographic IDs
  - IP-Adressen für Routing
- Fragen in der Seminararbeit
  - Wie funktioniert HIP
  - Welche Probleme löst es
  - Welche Einschränkungen bestehen
- Literatur
  - http://infrahip.hiit.fi
  - RFCs: 4423, 5201, 5205



Datagram Congestion Control Protocol (DCCP) – Andreas

- TCP und UDP als wohlbekannte Transportprotokolle im heutigen Internet
  - Verbindungsorientiert vs. verbindungslos
- Neue Szenarien könnten die Standards in Bedrängnis bringen
  - Streaming Audio und Video
  - Eigentlich unzuverlässig erwünscht, aber UDP würde Internet lahmlegen (RFC 3714)
- DCCP: UDP + Staukontrolle?
  - Zuverlässiger Verbindungsaufbau
  - Zuverlässige Aushandlung der Paketoptionen
  - Stauvermeidung mit unzuverlässigen Datagrammen
- Fragen in der Seminararbeit
  - Wie funktioniert DCCP
  - Für welche Einsatzgebiete eignet es sich
  - Aktueller Stand



- Literatur
  - RFCs: 4336, 4340
  - http://www.heise.de/netze/Ausweichmanoever--/artikel/77542/0
  - http://www.read.cs.ucla.edu/dccp/

Zero Configuration Networking - Andreas

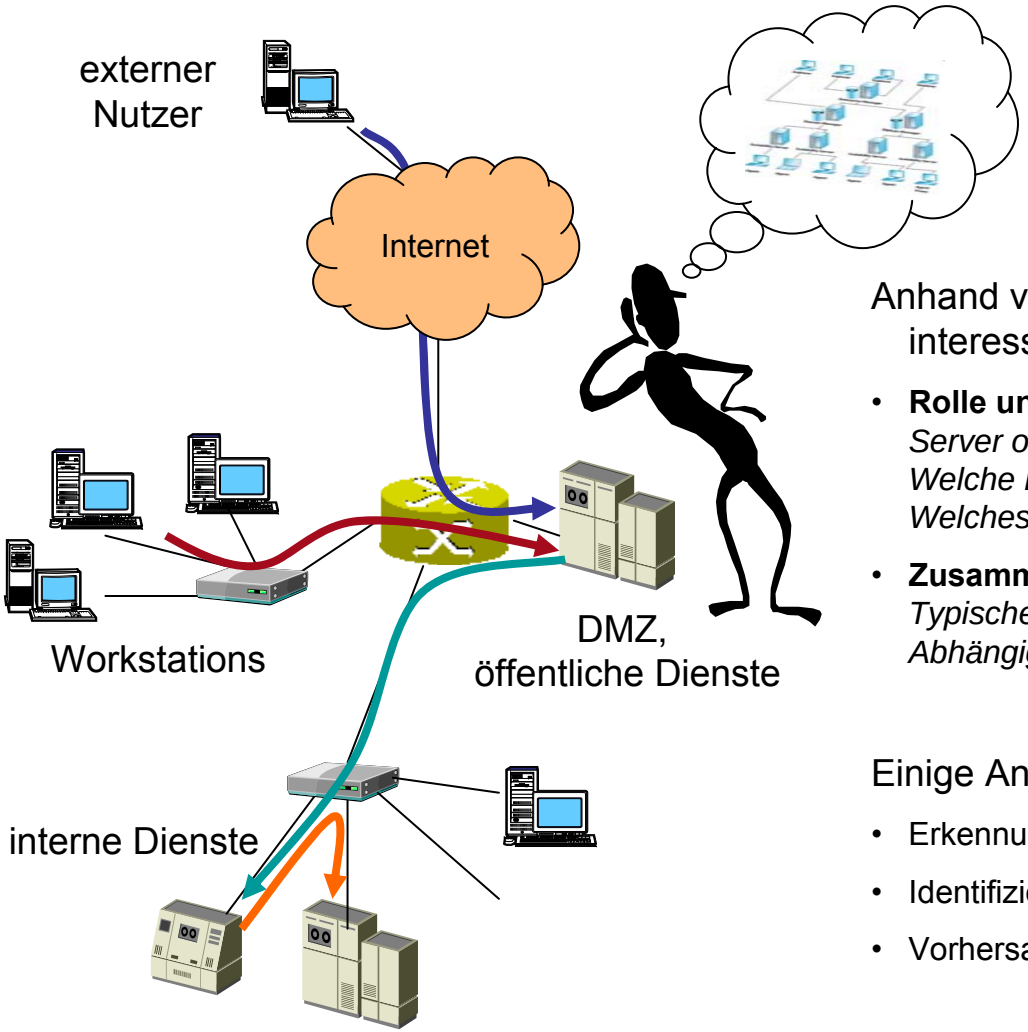
- Ad Hoc Szenarien immer interessanter
  - Wie konfiguriere ich „auf die Schnelle“ ein IP Netzwerk?

- Zero Configuration Networking
  - Einfaches Einrichten und Betreiben eines Netzes auf Basis von IP
  - Automatische Zuweisung von IP-Adressen ohne DHCP-Server
  - Übersetzen von Hostnamen ohne DNS-Server
  - Finden von Diensten ohne Directory Server

- Fragen in der Seminararbeit
  - Welche Techniken bzw. Standards gibt es
  - Wie funktionieren diese
  - Wo werden diese bereits eingesetzt

- Literatur
  - IETF Zeroconf Working Group
  - RFC 3927
  - Apple Bonjour (http://developer.apple.com/networking/bonjour/index.html)

Abhängigkeitsanalyse mit Hilfe von passiven Verkehrsmessungen – Gerhard und Lothar



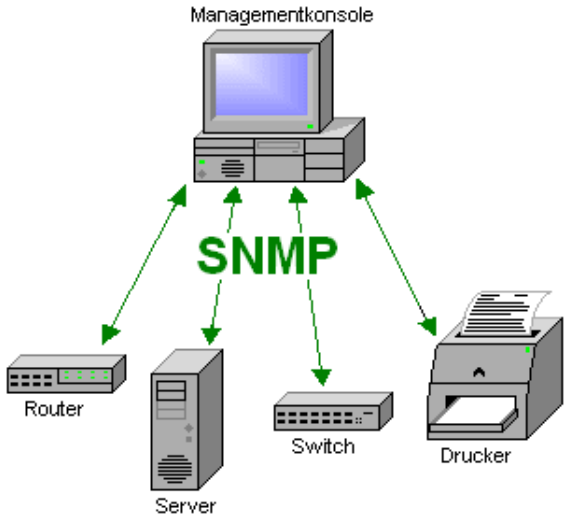
Anhand von beobachteten Verkehrsströmen sind interessante Rückschlüsse möglich, z.B.:

- **Rolle und Verhalten einzelner Rechner:**
  Server oder Client?
  Welche Dienste und Anwendungen?
  Welches Verhaltensmuster?
- **Zusammenhang zwischen Verkehrsströmen:**
  Typische Muster?
  Abhängigkeiten zwischen verschiedenen Diensten?

Einige Anwendungsmöglichkeiten:

- Erkennung von Störungen und Angriffen
- Identifizierung von Schwachstellen und Flaschenhälsen
- Vorhersage des Verkehrs nach Topologieänderungen

Thema 1: Untersuchung mit Graphen
Thema 2: Untersuchung von zeitlichen Korrelationen
Betreuer: Gerhard Münz, Lothar Braun



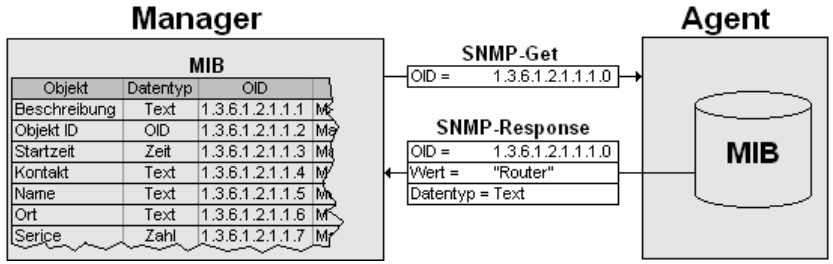
Simple Network Management Protocol (SNMP) is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

[en.wikipedia.org]

In this talk **SNMP** should be presented.

A **structure** could be:

- Historical overvies
- Shift of Design goals
- Spread of application today
- Future?



Sources will be the RFCs as well as some publications.

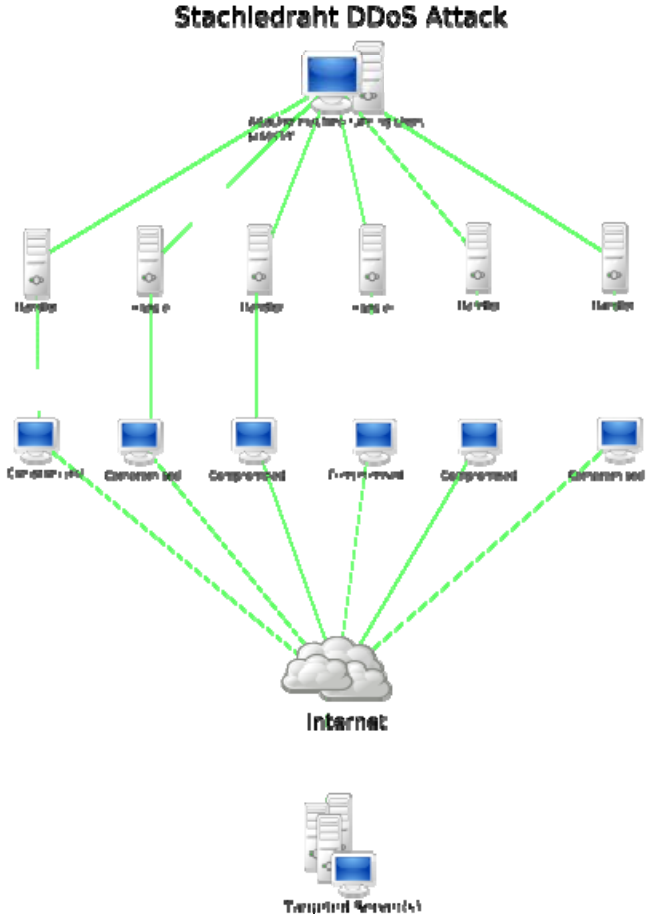
graphics: [de.wikipedia.org]

DoS-Angriffe (Marc)

- Als **Denial of Service** (**DoS**, zu Deutsch etwa: *Dienstverweigerung*) bezeichnet man einen Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. (wikipedia)

- Auf Nachrichtenseiten liest man öfters von DoS-Angriffen. Technische Details gibt es dabei so gut wie nie.

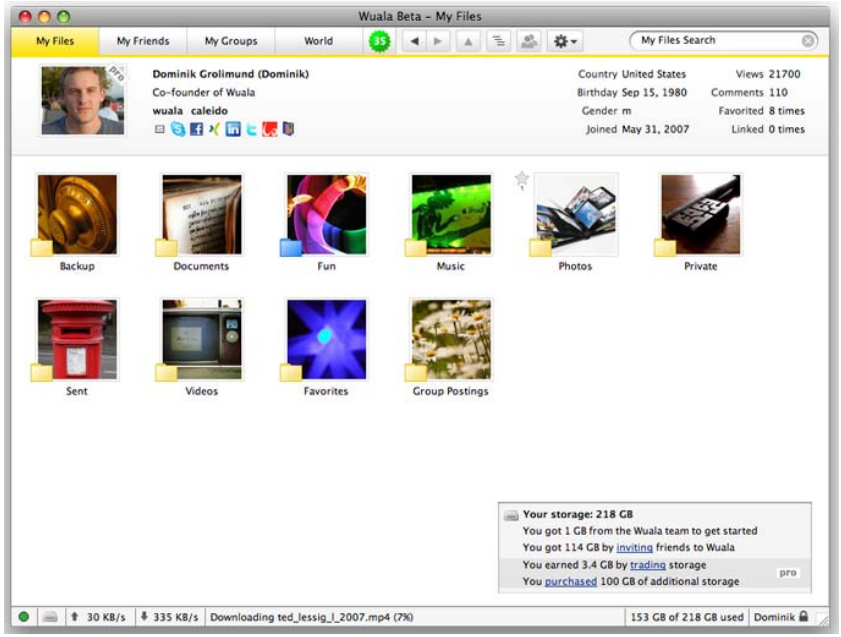
- Im Vortrag sollen reale DoS-Angriffe näher beleuchtet werden:
  - Was für Pakete werden geschickt?
  - Wie viele? (Bandbreite)
  - Von wo? (gespoofte Quell-IP? Botnetz?)
  - Wie häufig finden DoS-Angriffe statt?
  - Was ist die Motivation der Angreifer?



Wuala (Marc)

- Wuala ist eine Software, die einen P2P Online-Speicher realisiert.
- Im Gegensatz zu normalen P2P Filesharing Netzen speichert man seine eigenen Dateien verschlüsselt im P2P Netz.
  - als Backup
  - um von überall aus auf die Dateien zugreifen zu können
  - die Dateien werden verschlüsselt gespeichert
- Es ist allerdings möglich, Dateien für andere Benutzer freizugeben.

- Im Vortrag sollen 2 Punkte untersucht werden:
  - Wie brauchbar / benutzbar ist Wuala in der Praxis (durch ausprobieren).
  - Wie ist die Datensicherheit im Wuala-Netz? Dazu sollen öffentlich verfügbare Quellen (z.B. über das Schlüsselmanagement von Wuala) herangezogen werden.



Delay Tolerant Networks - Tobias

- Problematische Kommunikation
  - Kommunikation zwischen weit entfernten Kommunikationspartnern
  - Kommunikation mit Gegenstellen die nur bedingt erreichbar sind
  - Kommunikation mit Gegenstellen die nur ein eingeschränktes Zeitfenster für Kommunikation haben
  - z.b. Raumsonden, U-Boote, ...

- Beispiel: Erde-Mars Kommunikation
  - Abstand ~ 240 Millionen Kilometer => ~ 800 Sekunden Signallaufzeit
  - TCP Handshake: 2400 Sekunden (40 Minuten) => Timeouts
  - Befinden sich Sender und Empfänger auf der Planetenoberfläche so ist der Zeitraum in dem Kommunikation möglich ist stark eingeschränkt
  -

- Thema: Überblick über die Thematik und die Forschungsergebnisse zu Delay Tolerant Networks

Evolution der Kernnetze im Mobilfunk - Tobias

- GSM, UMTS, SAE
- Jede neue Mobilfunkgeneration bringt Veränderungen im Kernnetz
  - BTS, NodeB, eNodeB
  - BSC, RNC, ???
- Thema: Darstellung der Evolution der Kernnetze
  - Herausarbeiten der Neuerungen und Besonderheiten jedes Evolutionsschritts
  - Aufzeigen der Unterschiede

Schlauere Navigation durch Mobilfunk? - Tobias

- Heutige Navigationssysteme arbeiten meist mit:
  - Statischen Karten
  - Informationen über Verkehrsstörungen
  - Statistischen Informationen über Auslastung verschiedener Strecken
- Neue Ansätze beziehen weitere Informationsquellen mit ein
  - Auslastung bestimmter Mobilfunkzellen
  - Bewegungen einzelner TIMSI durch die einzelnen Zellen
  - Informationen von direkt über das Mobilfunknetz erreichbaren Navigationsgeräten
- Thema:
  - Aufzeigen der Methoden verschiedener Ansätze (TomTom IQRoutes, Nokia,...)
  - Darstellen der Funktionsweise

Weitere Themen der Gruppe Fuhrmann

Benedikt Elser (elser@net.in.tum.de)

- BitTorrent
- X-Layer Design

Bernhard Amann (ba@net.in.tum.de)

- Spiele in P2P Netz
- Churn in P2P Systemen
- Verteilte datenbanken in P2P

Yaser Houri (houri@ibds.uka.de)

- P2P Video on Demand
- P2P Traffic in Providerenetzen halten
- Network Coding

Themenvergabe Future Internet I

- Moderne Botnetze – Marc, Hattendorf
- Trusted Platform Module (TPM) – Holger, Rupprecht
- IT-Sicherheit – Psychologische Anspekte – Corinna (Stauber im HS)
- Datenschutz unter juristischem Blickwinkel – Corinna (Bothmann im HS)

- Trusted Network Connect - Holger
- Geographic Location/Privacy (GeoPriv) – Holger, Alexandra Simon, Amin Hammami
- IP Fast Reroute (IPFRR) - Nils
- RSerPool: Standardisierte Server-Replikation – Nils, Konrad Windszus
- Mobilität und Locator-/ID-Split – Nils
- Host Identity Protocol – Andreas, Alexander Hummel
- Datagram Congestion Control Protocol (DCCP) – Andreas
- Zero Configuration Networking – Andreas, Daniel Siegel
- Abhängigkeitsanalyse mit Hilfe von passiven Verkehrsmessungen – Gerhard und Lothar
  - Untersuchung mit Graphen
  - Untersuchung von zeitlichen Korrelationen

Themenvergabe Future Internet II

- Simple Network Management Protocol – Marc-Oliver, Rene Brogatzki
- DoS-Angriffe – Marc, Carl Denis
- Wuala – Marc, Florian Wohlfart
- Delay Tolerant Networks – Tobias
- Evolution der Kernnetze im Mobilfunk - Tobias
- Schlauere Navigation durch Mobilfunk? – Tobias, Matthias Kienzler

- BitTorrent - Simon Mittelberger
- X-Layer Design
- Spiele in P2P Netz
- Churn in P2P Systemen
- Verteilte datenbanken in P2P
- P2P Video on Demand
- P2P Traffic in Providerenetzen halten
- Network Coding

Lehrstuhl Netzarchitekturen und Netzdienste
Institut für Informatik
TU München