

# Domain Name Service

Albert Weichselbraun

# Domain Name Service

- Das Domain Name Service (DNS) erlaubt die Lokalisierung von Diensten im Internet.
- DNS hilft beim Auffinden verschiedener Dienste  
=> Unterschiedliche Typen von DNS-Einträgen

Typ	Bezeichnung	Verwendung
A	Hosteintrag	IP-Adresse eines Rechners
CNAME	Canonical name	Alias Name
MX	Mailexchanger	Name des zuständigen Mailservers
NS	Nameserver	Name des zuständigen Nameservers
TXT	Text	Zusätzliche Informationen zur Domäne

# Inhalt

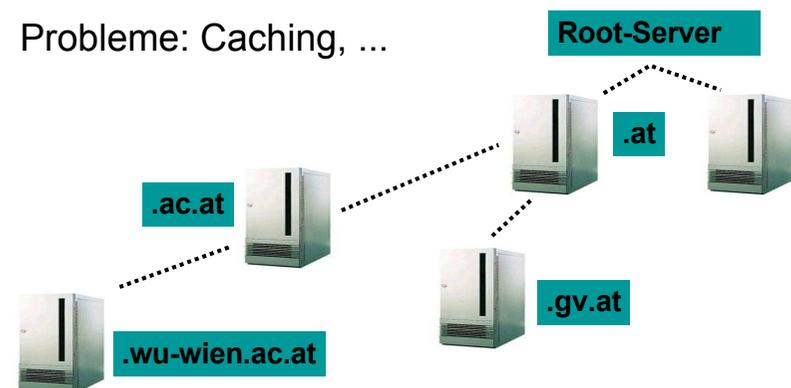
- Domain Name Service
- WHOIS
- Spoofing

## Ziele dieser Einheit:

- Awareness!
- Grundlagen für die Nachverfolgung von E-Mails, unerlaubten Zugriffen, ...

# DNS - Funktionsweise

- Hierarchischer Aufbau
- 13 Root-Server (a-m.root-servers.net)
- Probleme: Caching, ...



## DNS Abfragen mit dig

- “dig” ist **das** Standardtool zum Abfragen von DNS Informationen

- Syntax:

```
dig [@nameserver] [Typ] dnsname
```

- zum Beispiel

```
dig @ns1.univie.ac.at ns wu-wien.ac.at
```

```
;; AUTHORITY SECTION
```

```
wu-wien.ac.at. 10800 IN NS ns2.wu-wien.ac.at.
```

```
wu-wien.ac.at. 10800 IN NS ns5.wu-wien.ac.at.
```

```
wu-wien.ac.at. 10800 IN NS ns1.wu-wien.ac.at.
```

## DNS Abfragen mit dig

- Namen zu IP-Adressen:

```
dig -x IP-Adresse
```

- Achtung diese Information ist nicht immer eingetragen und/oder zuverlässig

## Übungsbeispiel

- Ermitteln Sie die IP-Adresse des Nameservers für die Domäne chello.at.
- Wie lauten die Nameserver für die Domäne atnet.at?
- Wie lauten die IP-Adresse(n) der Server, auf welchen sich die ORF-Homepage befindet?
- Welche Information enthält das Textfeld von .atnet.at?

## Übungsbeispiel

- Ermitteln Sie den Namen für die IP-Adresse 128.130.57.131
- Wie lautet der Name für die IP-Adresse 194.153.160.139

## WHOIS

- WHOIS erlaubt die Abfrage von Informationen zu Internet-Domänen, IP-Adressen und deren Eigentümer

- Entsprechender Befehl:

```
whois [domainname|IP-Adresse]
```

## Übungsbeispiel

- Ermitteln Sie die für die Domäne heise.de zuständigen Personen
- Wer ist für die IP-Adresse 194.154.160.139 zuständig?
- Wer versteckt sich hinter den NIC-Handle TH766710-NICAT ?

## DNS-Spoofing

- Idee: Die Antwort eines DNS-Servers wird verfälscht  
=> das Opfer wird zu einem anderen „Dienst“ umgeleitet (Beispiel: Microsoft „hack“, ...) .
- Gegenmaßnahmen:
  - a) DNS-SEC
  - b) Verwendung von Zertifikaten