UNIVERSITÄT DUISBURG ESSEN

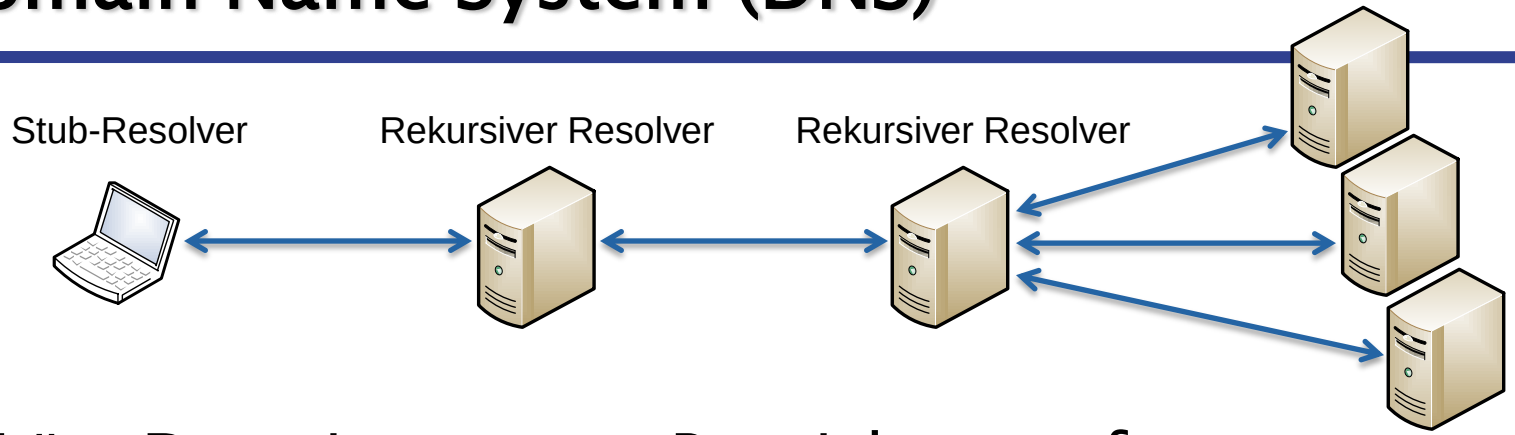
Über die Auswirkungen von DNSSEC auf das Internet

Originaltitel: The Impact of DNSSEC on the Internet Landscape

Matthäus Wander

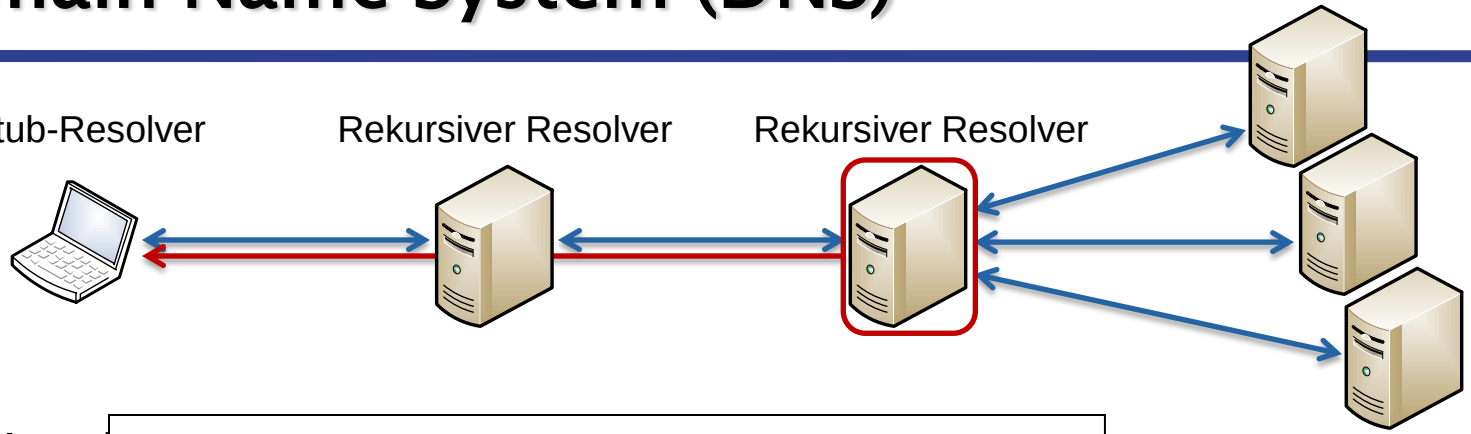
Schloss Dagstuhl, 3. Mai 2016

Domain Name System (DNS)



- Löst Domainname zu Bezeichner auf
- Man-in-the-Middle-Angreifer:
  - Erhält Anfrage, sendet gefälschte Antwort (DNS-Spoofing)
  - Zweck: z. B. Phishing-Angriff, Internetzensur

Domain Name System (DNS)



- Löst

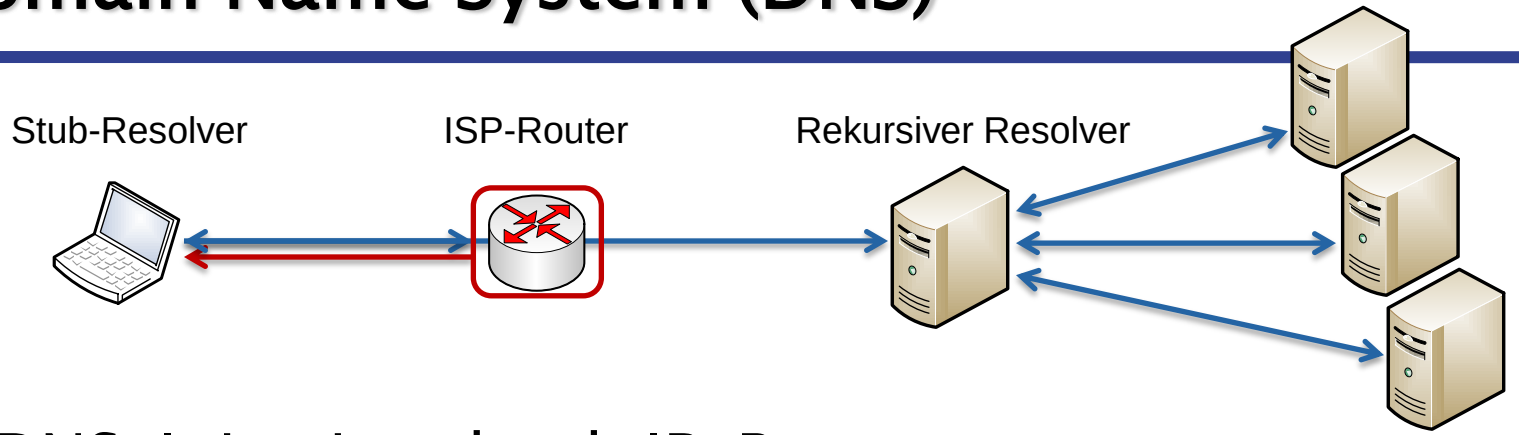
Вие попаднахте на тази страница, защото достъпът до сайта е ограничен във връзка с изпълнение на Разпореждания от 17.06.2013г., 28.06.2013г., 15.07.2013г., 31.07.2013г., 06.08.2013г., 04.09.2013г., 24.09.2013г. и 03.10.2013г. на Софийски районен съд.

- 

Domain Name System (DNS)

- Lös hner auf
- Mar er:
  - E te Antwort (DNS-Spoofing)
  - Z nternetzensur

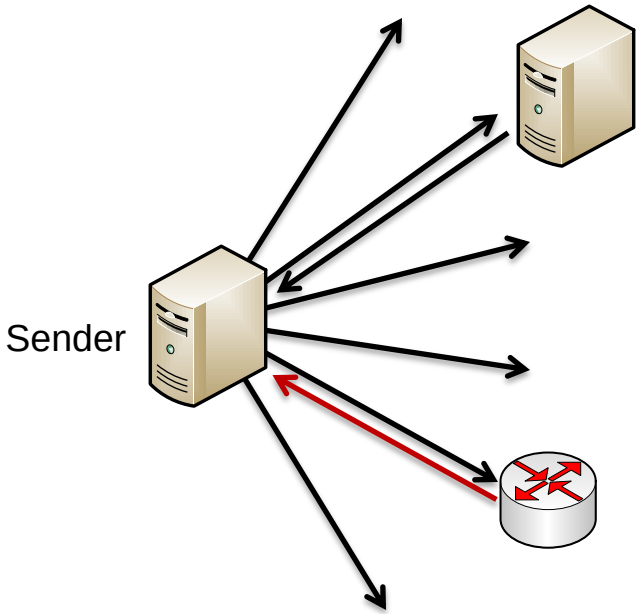
Domain Name System (DNS)



- DNS-Injection durch IP-Router:
  - Deep Packet Inspection aller DNS-Anfragen
  - Router sieht Anfrage, sendet gefälschte Antwort
- Effektive Filterung aller DNS-Anfragen im Netzwerk

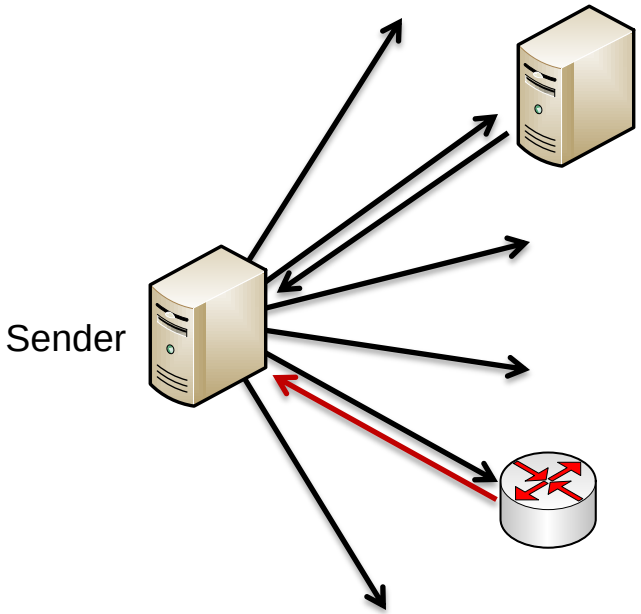
DNS-Injection lokalisieren

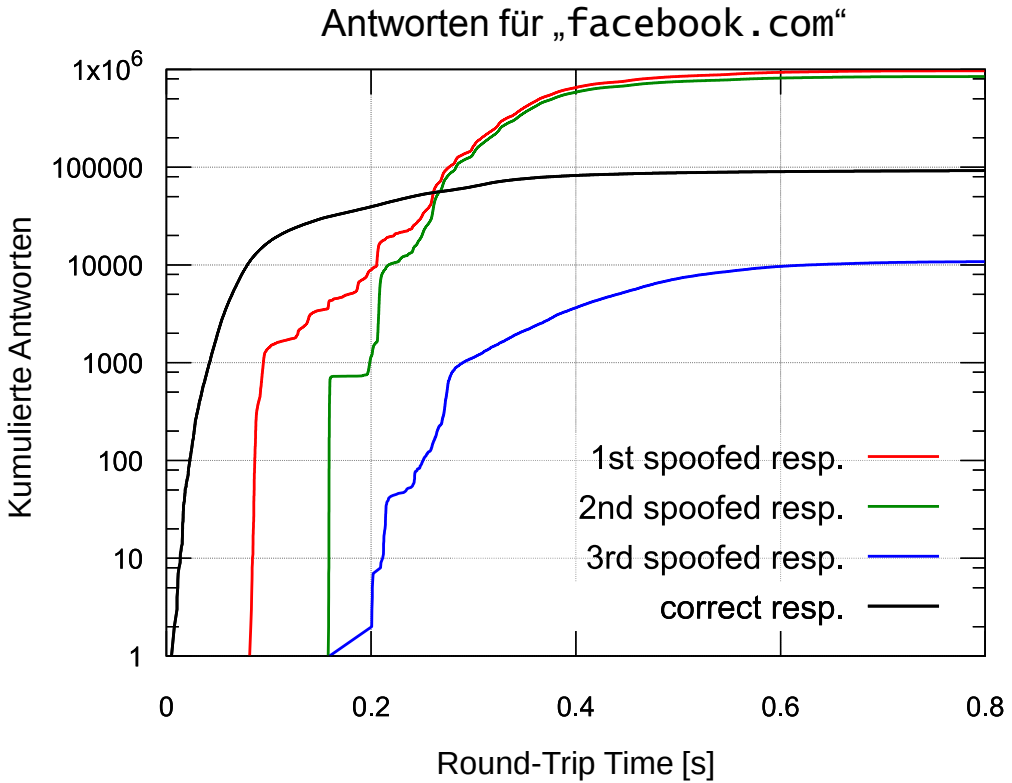
Veröffentlicht in:
IEEE Access, 2014



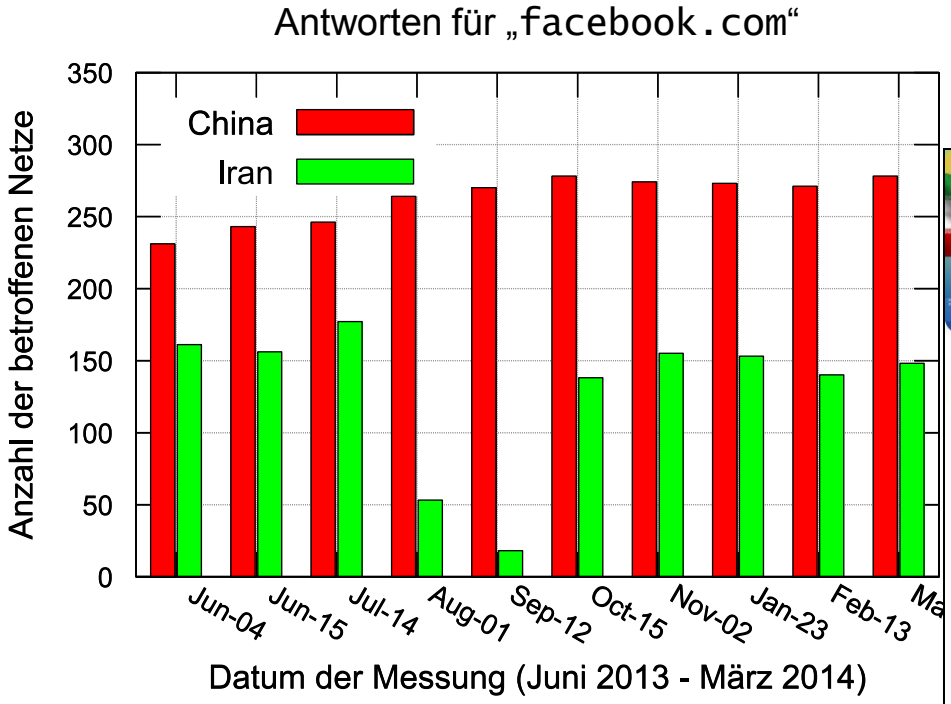
DNS-Injection lokalisieren

Veröffentlicht in:
IEEE Access, 2014



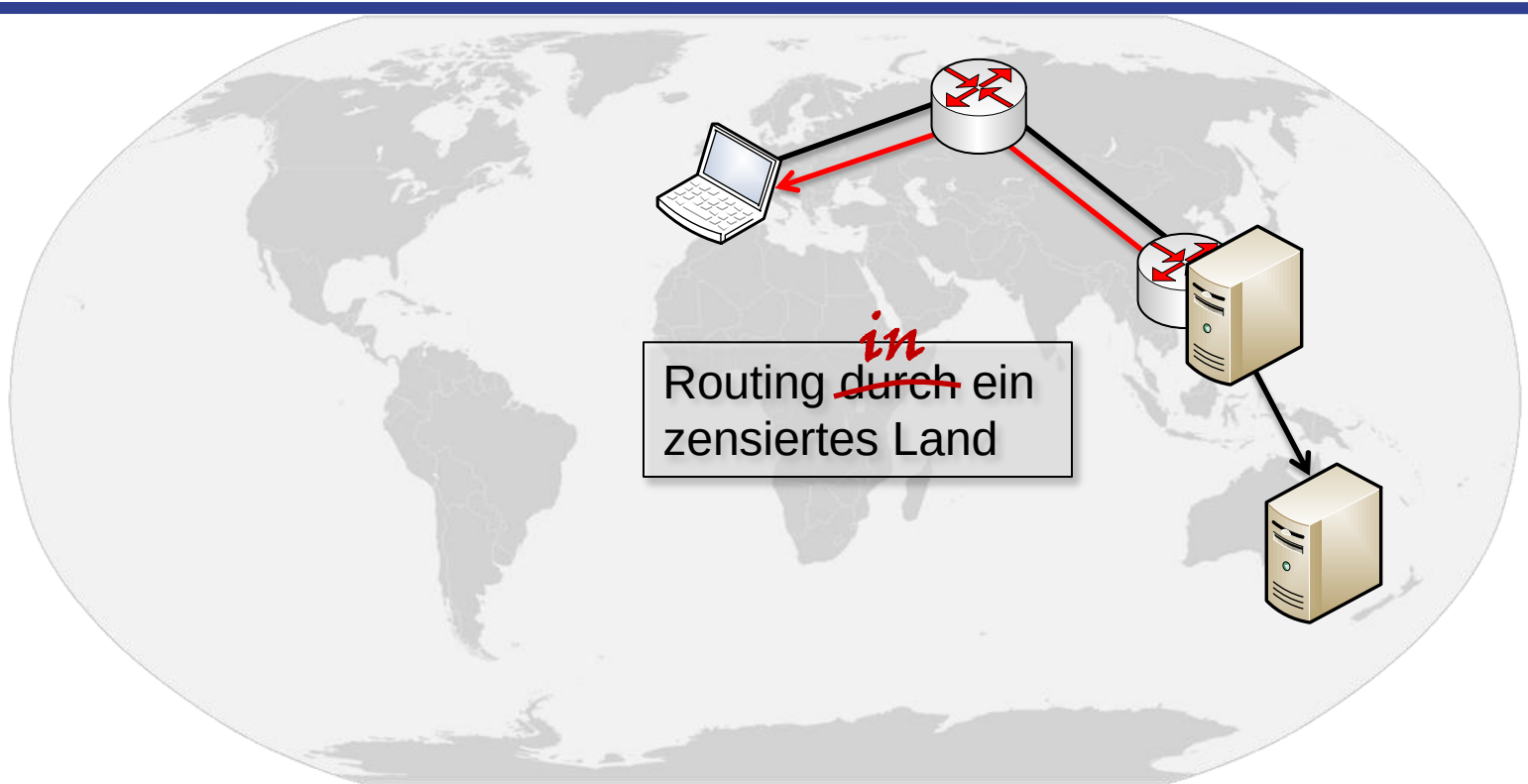


DNS-Injection im Zeitverlauf



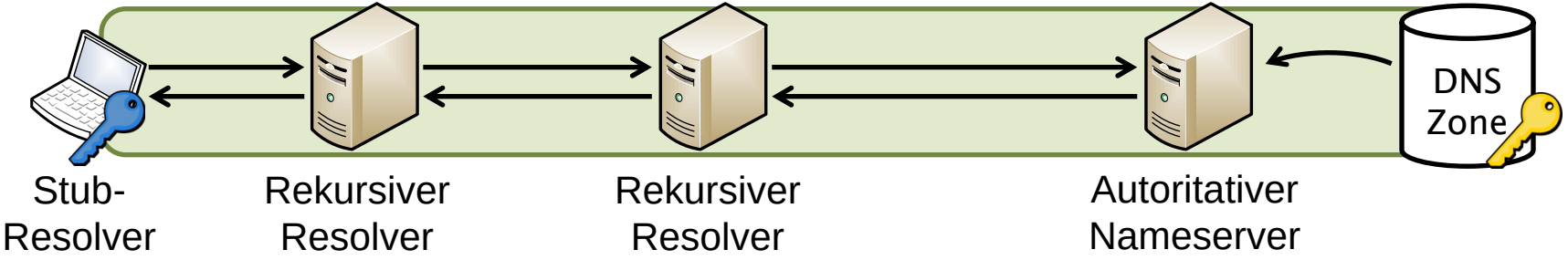
Auswirkungen auf Dritte

Veröffentlicht in:
IEEE Access, 2014



DNSSEC

Konzept

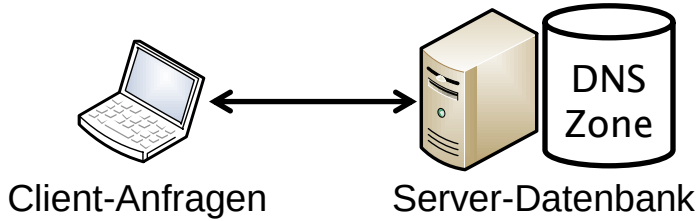


- Sicherheitsziele: Datenintegrität und Authentizität
- Signaturen über DNS-Einträge vorgeneriert
- Ende-zu-Ende-Sicherheit **Validator**↔**Signierer**

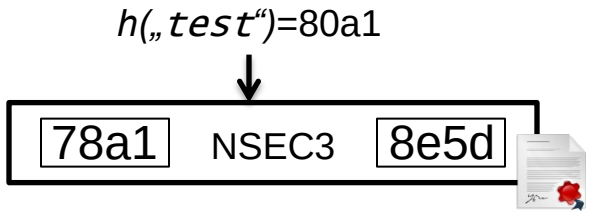
Privatheit und Vertraulichkeit

Veröffentlicht in:
IEEE NCA, 2014

- Client: keine Privatheit
  - Domainname im Klartext



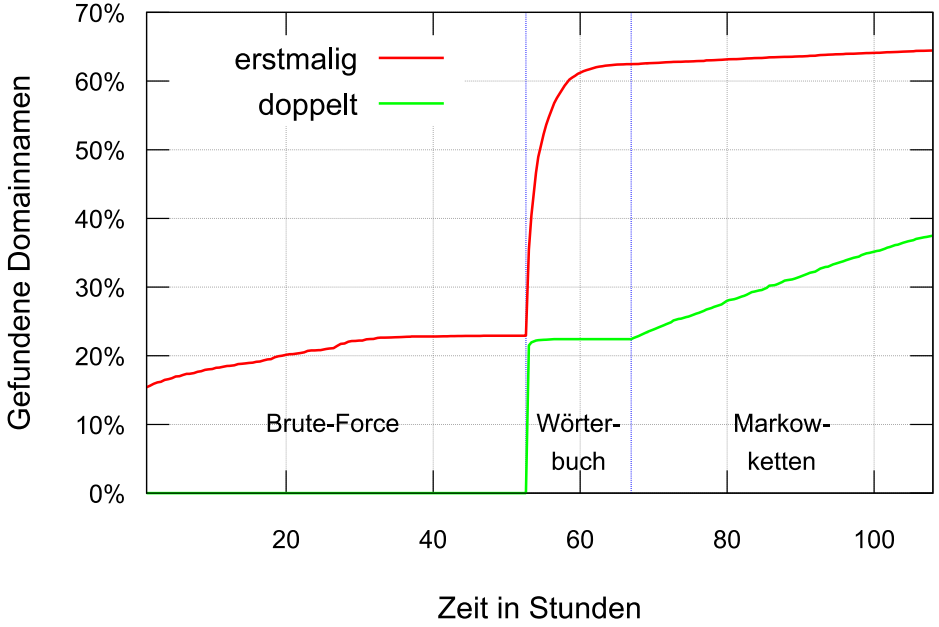
- Server: offenbart Hash-Werte von Domainnamen
  - Indirekter Beweis der Nichtexistenz
  - Hashing soll Namen verstecken
  - Domain *„test“* existiert nicht, da $h(x) < h(\text{„test“}) < h(y)$



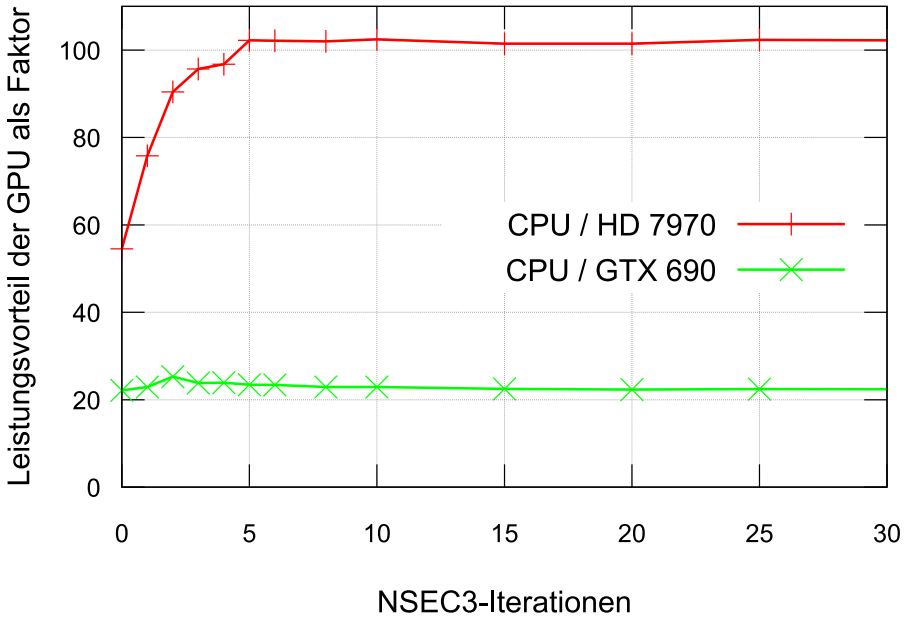
- NSEC3/SHA-1 Hash-Funktion durch GPU angreifbar

GPU-basierte NSEC3-Hash-Angriffe

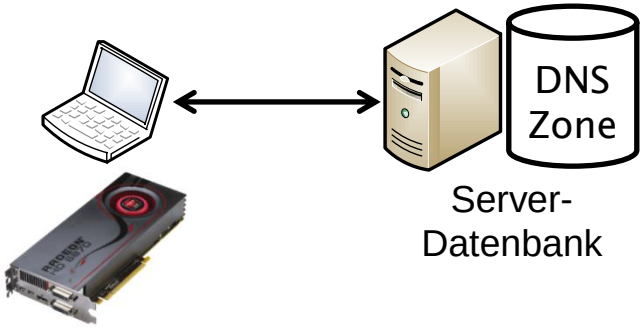
Veröffentlicht in:
IEEE NCA, 2014



Stand: Mai 2014



Verbreitung: Signierte Domains



Stand: März 2015

TLD	Domains		
1. nl	2,279,702	8. no	119,759
2. br	566,694	9. be	92,385
3. cz	448,984	10. net	81,391
4. com	426,182	11. org	46,382
5. se	349,514	12. ovh	29,372
6. eu	320,311	13. nu	21,126
7. fr	205,662	14. de	20,004

Gesamt: 5.146.705 signierte Domains

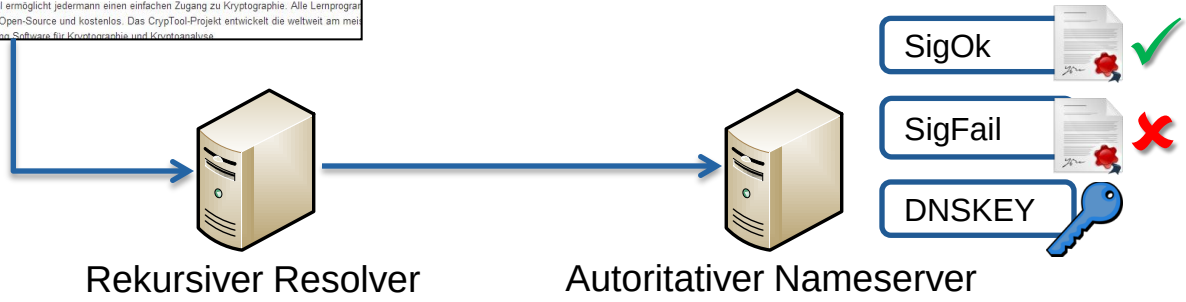
Verbreitung: Validierende Clients

Veröffentlicht in:
LNCS PAM, 2013

`https://SigOk.verteiltesysteme.net/a.png`

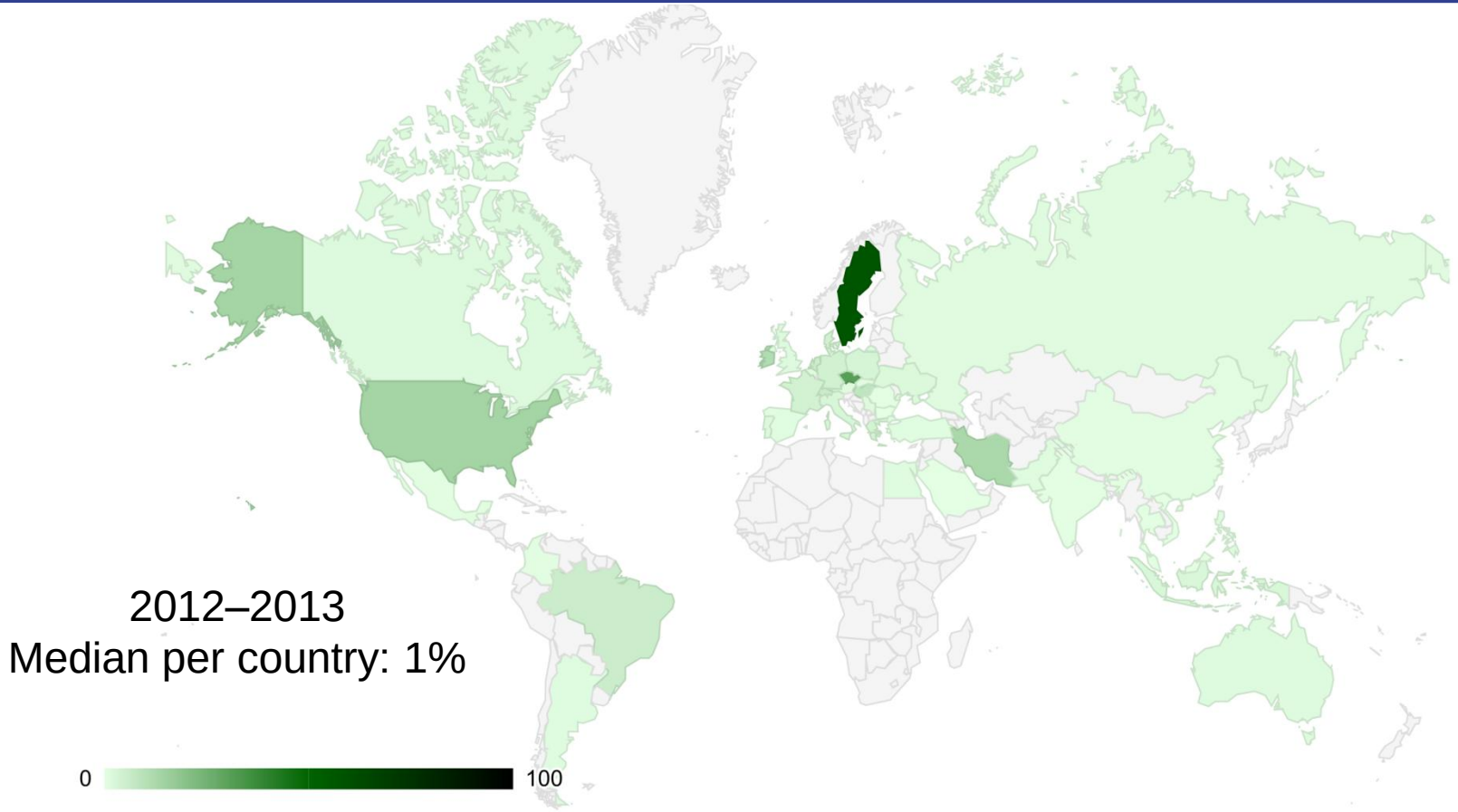
`https://SigFail.verteiltesysteme.net/b.png`

Unsichtbare 1px Grafik

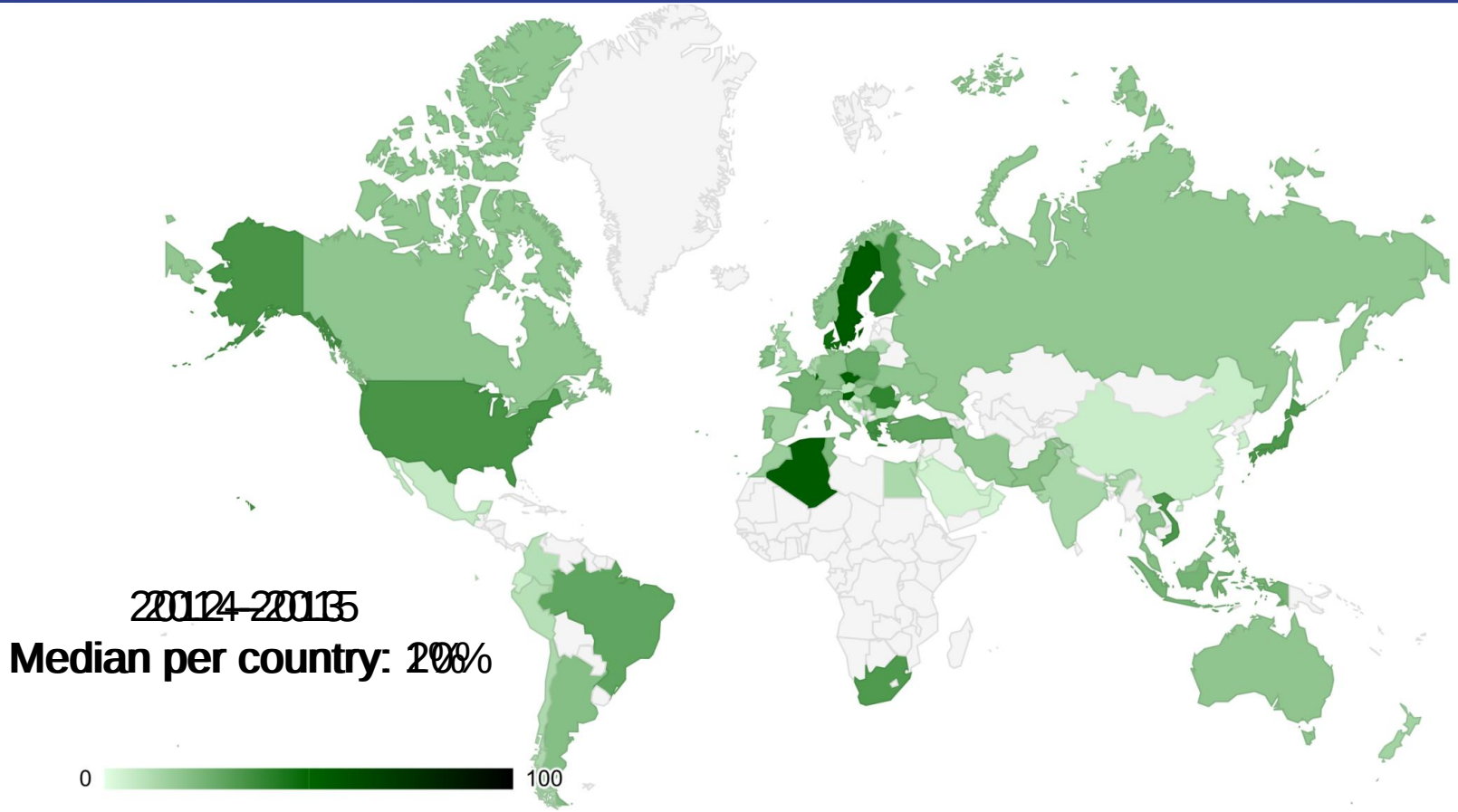


DNSSEC-Validierung nach Land

Veröffentlicht in:
LNCS PAM, 2013



DNSSEC-Validierung nach Land



Fazit

- DNS-Spoofing wird tagtäglich praktiziert
  - China und Iran: großflächiges DNS-Injection auf Routern
  - Kann Dritte betreffen — Beobachtung von außen möglich
- DNSSEC sichert Authentizität, aber keine Privatheit
  - NSEC3/SHA-1 Hash-Funktion effizient mit GPU angreifbar
- Verbreitung von DNSSEC nimmt zu
  - 5M signierte Domains, 20% Validierung pro Land im Median

Referenzierte Publikationen

- M. Wander, T. Weis:
  Measuring Occurrence of DNSSEC Validation,
  Passive and Active Measurement (PAM), LNCS Springer, 2013.
- M. Wander, C. Boelmann, L. Schwittmann, T. Weis:
  Measurement of Globally Visible DNS Injection,
  IEEE Access, 2014.
- M. Wander, L. Schwittmann, C. Boelmann, T. Weis:
  GPU-based NSEC3 Hash Breaking,
  IEEE NCA, 2014. Ausgezeichnet als **Best Student Paper**.