DNSSEC

Security Layer für integre Namensauflösung

Andreas Schattney & Fabian Spahn
Hochschule Darmstadt
Andreas.Schattney@stud.h-da.de
Fabian.Spahn@stud.h-da.de

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Abstract

Domain **N**ame **S**ystem (DNS) ist ein System, das im OSI-Schichtenmodell auf der Applikationsschicht arbeitet. Die Hauptaufgabe dieses Systems besteht darin, von Menschen lesbare Domainnamen in IP-Adressen umzuwandeln. Demnach kann man DNS als Telefonbuch des Internets bezeichnen. Allerdings ist die Datenübermittlung über DNS nicht gegen Angreifer geschützt. Über einen Man-in-the-Middle Angriff könnte die Antwort eines DNS Servers abgefangen und eine gefälschte Antwort an den Client weitergeleitet werden. Durch DNSSEC Security Extensions (DNSSEC) sollen solche Angriffe verhindert werden. DNSSEC verwendet *Trust Chains* um die Authentizität der Antworten einer DNS Abfrage zu gewährleisten. Allerdings führt DNSSEC auch neue Schwierigkeiten ein und verhindert nicht alle bekannten Schwachstellen. In dieser Arbeit werden die, durch DNSSEC, gewonnenen Sicherheitsmerkmale den weiterhin vorhandenen Schwachstellen gegenübergestellt.

Introduction

Aliquam non lacus dolor, *a aliquam quam* [**?**]. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Nulla in nibh mauris. Donec vel ligula nisi, a lacinia arcu. Sed mi dui, malesuada vel consectetur et, egestas porta nisi. Sed eleifend pharetra dolor, et dapibus est vulputate eu. **Integer faucibus elementum felis vitae fringilla.** In hac habitasse platea dictumst. Duis tristique rutrum nisl, nec vulputate elit porta ut. Donec sodales sollicitudin turpis sed convallis. Etiam mauris ligula, blandit adipiscing condimentum eu, dapibus pellentesque risus.

Aliquam auctor, metus id ultrices porta, risus enim cursus sapien, quis iaculis sapien tortor sed odio. Mauris ante orci, euismod vitae tincidunt eu, porta ut neque. Aenean sapien est, viverra vel lacinia nec, venenatis eu nulla. Maecenas ut nunc nibh, et tempus libero. Aenean vitae risus ante. Pellentesque condimentum dui. Etiam sagittis purus non tellus tempor volutpat. Donec et dui non massa tristique adipiscing.

Mögliche Attacken auf das DNS Protokoll

- Man In The Middle.
- DNS Cache Poisoning
- ID-Guessing and Query Prediction.
- Name Chaining
- Kaminski-Angriff

Neue Resource Records Datentypen in DNSSEC

Fusce magna risus, molestie ut porttitor in, consectetur sed mi. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque consectetur blandit pellentesque. Sed odio justo, viverra nec porttitor vel, lacinia a nunc. Suspendisse pulvinar euismod arcu, sit amet accumsan enim fermentum quis. In id mauris ut dui feugiat egestas. Vestibulum ac turpis lacinia nisl commodo sagittis eget sit amet sapien.

Eingeführte Probleme durch DNSSEC

- Größe der Datenpakete
- Automatisierung
- Sicherheit der privaten Schlüssel
- Key Rollover

Results

Donec faucibus purus at tortor egestas eu fermentum dolor facilisis. Maecenas tempor dui eu neque fringilla rutrum. Mauris *lobortis* nisl accumsan. Aenean vitae risus ante. Phasellus imperdiet, tortor vitae congue bibendum, felis enim sagittis lorem, et volutpat ante orci sagittis mi. Morbi rutrum laoreet semper. Morbi accumsan enim nec tortor consectetur non commodo nisi sollicitudin. Proin sollicitudin. Pellentesque eget orci eros. Fusce ultricies, tellus et pellentesque fringilla, ante massa luctus libero, quis tristique purus urna nec nibh.

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table 1: Table caption

Nulla ut porttitor enim. Suspendisse venenatis dui eget eros gravida tempor. Mauris feugiat elit et augue placerat ultrices. Morbi accumsan enim nec tortor consectetur non commodo. Pellentesque condimentum dui. Etiam sagittis purus non tellus tempor volutpat. Donec et dui non massa tristique adipiscing. Quisque vestibulum eros eu. Phasellus imperdiet, tortor vitae congue bibendum, felis enim sagittis lorem, et volutpat ante orci sagittis mi. Morbi rutrum laoreet semper. Morbi accumsan enim nec tortor consectetur non commodo nisi sollicitudin.

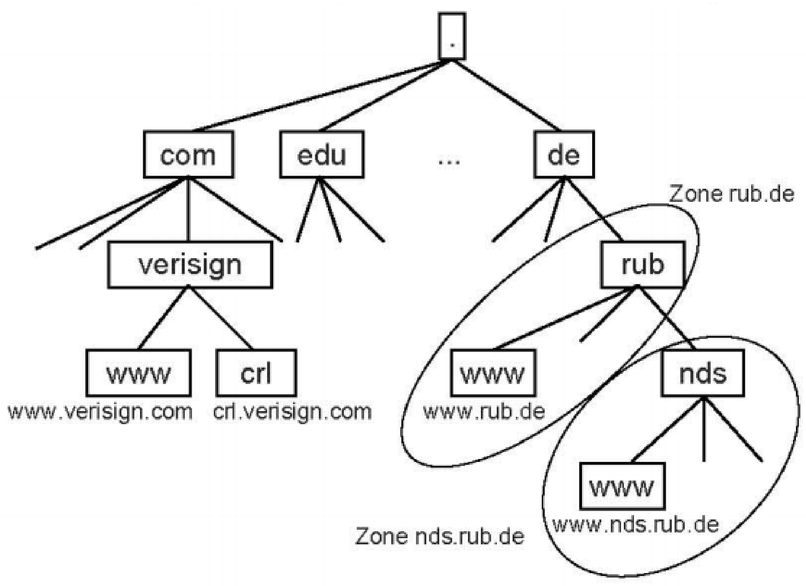

Figure 1: Beispielhafte Darstellung der Einteilung von Domains in einzelne Zonen [1]

In hac habitasse platea dictumst. Etiam placerat, risus ac.
Adipiscing lectus in magna blandit:

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table 2: Table caption

Vivamus sed nibh ac metus tristique tristique a vitae ante. Sed lobortis mi ut arcu fringilla et adipiscing ligula rutrum. Aenean turpis velit, placerat eget tincidunt nec, ornare in nisl. In placerat.

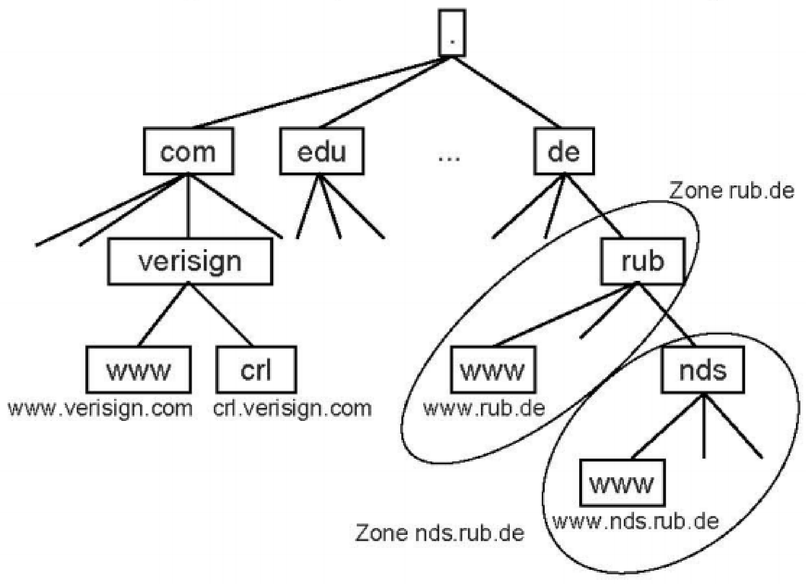

Figure 2: Figure caption

Conclusions

- Pellentesque eget orci eros. Fusce ultricies, tellus et pellentesque fringilla, ante massa luctus libero, quis tristique purus urna nec nibh. Phasellus fermentum rutrum elementum. Nam quis justo lectus.
- Vestibulum sem ante, hendrerit a gravida ac, blandit quis magna.
- Donec sem metus, facilisis at condimentum eget, vehicula ut massa. Morbi consequat, diam sed convallis tincidunt, arcu nunc.
- Nunc at convallis urna. isus ante. Pellentesque condimentum dui. Etiam sagittis purus non tellus tempor volutpat. Donec et dui non massa tristique adipiscing.

Forthcoming Research

Vivamus molestie, risus tempor vehicula mattis, libero arcu volutpat purus, sed blandit sem nibh eget turpis. Maecenas rutrum dui blandit lorem vulputate gravida. Praesent venenatis mi vel lorem tempor at varius diam sagittis. Nam eu leo id turpis interdum luctus a sed augue. Nam tellus.

References

[1] Jörg Schwenk. *Sicherheit und Kryptographie im Internet*. Springer Vieweg, 4te edition, 2014.

[2] Matthäus Wander. The Impact of DNSSEC on the Internet Landscape. http://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate-39547/Wander_Diss.pdf, 2015. [Online; Letzter Zugriff: 18.10.2016].

Acknowledgements

Etiam fermentum, arcu ut gravida fringilla, dolor arcu laoreet justo, ut imperdiet urna arcu a arcu. Donec nec ante a dui tempus consectetur. Cras nisi turpis, dapibus sit amet mattis sed, laoreet.