

DNSSEC

Sichere Namensauflösung im Internet

Marcus Obst*

marcus.obst@etit.tu-chemnitz.de

<http://www.tu-chemnitz.de/~maob/nt>

Heiko Schlittermann†

hs@schlittermann.de

<http://www.schlittermannn.de>

Chemnitzer Linux-Tage 2010 (13. - 14. März)

<http://chemnitzer.linux-tage.de>

Zusammenfassung

Die Auflösung von Hostnamen in IP-Adressen mit Hilfe des Domain Name System (DNS) ist fundamentaler Bestandteil des Internets, so wie wir es heute kennen. Dass die Entwicklung von DNS keinesfalls stillsteht, sondern rasant voranschreitet, soll in diesem Vortrag am Beispiel der Protokollerweiterung DNS Security Extension (DNSSEC) gezeigt werden. DNSSEC ist eine umfassende Möglichkeit zur Sicherstellung der Authentizität und Integrität von DNS-Abfragen, die in Zukunft wohl immer mehr an Bedeutung gewinnen wird.

*Professur für Nachrichtentechnik, Technische Universität Chemnitz

†schlittermann – internet & unix support, Dresden

DNSSEC – Sichere Namensauflösung im Internet

Das *Domain Name System*, ein hierarchisches dezentralisiertes System, ist der zentrale Dreh- und Angelpunkt im Internet wenn es um die Auflösung von Hostnamen in IP-Adressen geht. Neben der einfachen Vorwärtsauflösung spielt *DNS* auch eine wichtige Rolle im Zusammenhang mit der Zustellung von Email. Aufgrund der fundamentalen Bedeutung des *DNS* steht es auch immer wieder im Fokus verschiedenen Angriffsszenarien. Neben illegalen Manipulationen wie z.B. DNS-Spoofing oder Cache Poisoning, sind aber auch „behördlich legitimierte“ Eingriffe wie z.B. das „Stoppschild“ oder transparente DNS-Proxies technisch möglich. Dass an dieser Stelle Handlungsbedarf besteht,¹ hat auch die *Internet Engineering Task Force (IETF)* erkannt und einen neuen Standard, die *Domain Name System Security Extension (DNSSEC)*, erarbeitet. Im Jahr 2005 wurde erstmals eine Top Level Domain (.se, heute sind es auch einige andere (.cz, .bg, ...)) mit einer digitalen Signatur auf Basis von DNSSEC versehen.

Dieser Vortrag möchte einen eher theoretisch gehaltenen Einblick in die Grundlagen und Funktionsweise von DNSSEC geben. Nach einer kurzen Vorstellung des aktuellen Stands der Technik bezogen auf DNS und den damit verbundenen Unzulänglichkeiten folgt eine knappe Einführung in die Public Key Kryptographie.

Anschließend werden die notwendigen Komponenten und Schritte für das Aufsetzen einer signierten Zone erläutert. Das Verhalten des Resolvers bzw. eines DNS-Servers, der die DNS Security Extension benutzt, soll exemplarisch mit einer „echten“ signierten Zone im Internet demonstriert werden. Serverseitig werden die DNS-Implementierung des ISC Bind9 und die damit verbundenen Werkzeuge vorgestellt.

Da DNSSEC einen ganzheitlichen Ansatz zur Sicherung der Authentizität und Integrität von DNS-Transaktionen im Internet darstellt, ist eine schrittweise Einführung nicht ohne weiteres möglich. Wie dies dennoch erreicht werden kann, soll mit Hilfe der sogenannten *Domain Lookaside Validation*, die im Bind9 und aktuellen ISC-Clients eingebaut ist, gezeigt werden.

Im Anschluss daran folgt eine Zusammenfassung, was DNSSEC leisten kann, wie eine mögliche Migration durchzuführen wäre und welche Probleme noch offen bleiben.

Ein kurzer Blick auf die deutschen Bestrebungen, auch die .de-Zone mit DNSSEC abzusichern, sowie die damit momentan noch verbunden Probleme sollen den Vortrag abrunden. Zusätzlich zu diesem Vortrag wird im Rahmen der Chemnitzer Linux-Tage 2010 auch noch ein Workshop mit dem Schwerpunkt auf praktische Anwendung von DNSSEC angeboten.

Der Vortrag richtet sich an diejenigen, die mit den Grundlagen von DNS vertraut sind, möglicherweise auch bereits einen DNS-Server eingerichtet haben und nun den Fokus auf Sicherheit im Sinne von Authentizität legen wollen. Das Grundverständnis der Public Key Kryptographie (z.B. auch ssh und gnupg) ist nützlich aber nicht zwingend notwendig.

¹Hier sei exemplarisch auch auf die Anstrengungen von google hingewiesen, einen eigenen sichereren DNS-Service anzubieten.

DNSSEC – Eine praktische Einführung zur Sicherung von DNS

Das *Domain Name System*, ein hierarchisches dezentralisiertes System, ist der zentrale Dreh- und Angelpunkt im Internet wenn es um die Auflösung von Hostnamen in IP-Adressen geht. Neben der einfachen Vorwärtsauflösung spielt *DNS* auch eine wichtige Rolle im Zusammenhang mit der Zustellung von Email. Aufgrund der fundamentalen Bedeutung des *DNS* steht es auch immer wieder im Fokus verschiedenen Angriffsszenarien. Neben illegalen Manipulationen wie z.B. DNS-Spoofing oder Cache Poisoning, sind aber auch „behördlich legitimierte“ Eingriffe wie z.B. das „Stoppschild“ oder transparente DNS-Proxies technisch möglich. Dass an dieser Stelle Handlungsbedarf besteht, hat auch die *Internet Engineering Task Force (IETF)* erkannt und einen neuen Standard, die *Domain Name System Security Extension (DNSSEC)*, erarbeitet. Im Jahr 2005 wurde erstmals eine Top Level Domain (.se, heute sind es auch einige andere (.cz, .bg, ...)) mit einer digitalen Signatur auf Basis von DNSSEC versehen.

Dieser Workshop möchte den Teilnehmern die Funktionsweise von DNSSEC praktisch verständlich machen. Dazu wird nach einer kurzen theoretischen Einführung zuerst einmal der Umgang mit *dig* im Zusammenhang mit DNSSEC vorgestellt und geübt.

Daran anschließend wird ein validierender DNS-Server aufgebaut, welcher für eine gegebene ihm vertrauende Infrastruktur die Authentizität von erhaltenen Daten prüfen kann. Als Ersatz für eine vorhandene vertrauenswürdige Infrastruktur zur Verteilung der öffentlichen Signatur-Schlüssel wird die Verwendung von *Domain Lookaside Validation (DLV)* vorgestellt.

Abschließend soll das Absichern einer eigenen autonomen Zone, die durch einen Bind9-Nameserver verwaltet wird, durchgeführt werden. Es wird exemplarisch eine eigene Infrastruktur zum Verwalten einer über DNSSEC abgesicherten Zone aufgebaut.

Der Vortrag richtet sich an diejenigen, die mit den Grundlagen von DNS vertraut sind, möglicherweise auch bereits einen DNS-Server eingerichtet haben und nun den Fokus auf Sicherheit im Sinne von Authentizität legen wollen - sowohl für die Clientseite als auch für eigene publizierte DNS-Records. Das Grundverständnis der Public Key Kryptographie (z.B. auch ssh und gnupg) ist nützlich aber nicht zwingend notwendig.

Um am Workshop erfolgreich teilnehmen zu können, sollte ein eigener Rechner mit Internet-Zugang (vorzugsweise Laptop mit WLAN) vorhanden sein. Eine Linux-Umgebung mit installiertem Bind9 und Dig ist vorteilhaft, kann aber je nach Distribution auch vor Ort über Internet nachinstalliert werden. Die Beherrschung eines Texteditors und der sichere Umgang mit der Kommandozeile sind obligatorisch.

Ziel des Workshops ist es, die Teilnehmer auf die aktuellen Sicherheitsprobleme von DNS aufmerksam zu machen und ihnen mit DNSSEC ein mögliches Gegenmittel in die Hand zu geben. Nach dem Besuch des Workshops sollten die Teilnehmer in der Lage sein, DNS-Anfragen einer signierten DNSSEC-Zone zu validieren, sowie eine eigene DNS-Zone mit DNSSEC abzusichern.