Bachelor These

für Hn. Ano N'dri Jean Michel Ekra

Informations- und Kommunikationstechnik

Prof. Dr.-Ing. Ulf Niemeyer

Netzwerkemulation zur Untersuchung von Secure DNS

Die Namensauflösung in Internet-Netzwerken geschieht meist mittels Domain Name Service (DNS). Dieser Dienst ist vielschichtig und verteilt realisiert. Er bietet ein beliebtes und lohnendes Ziel für Angriffe: Veränderungen in der Datenbasis oder dem Abfrageverkehr erlauben bspw. das Umleiten von Netzwerkverkehren und eröffnen so gute Möglichkeiten zu weitergehenden Manipulationen. Die Analyse von DNS-Verkehr kann einerseits helfen, Anomalien und Angriffe aufzudecken, bietet aber auch weitreichende Einblicke in das Verhalten und die Interessen der Nutzer und ermöglicht Zensur.

Daher wird im Sinne von Security und Privacy der DNS in jüngerer Zeit verstärkt abgesichert.

Ziel dieser Arbeit ist es, DNSsec aufzuarbeiten und in einer aufzubauenden Emulationsumgebung zu demonstrieren. In einer vergleichenden Betrachtung soll anschließend DNSsec gegenüber anderen Absicherungsverfahren – DNS over TLS, DNS over HTTPS, DANE – abgegrenzt und beurteilt werden.

Zu diesem Zweck sind folgende Arbeiten notwendig:

- Eine Literaturrecherche fasst den Stand der Technik zu den jeweiligen Verfahren zusammen:
  - Die relevanten RFCs und ggf. andere standardartige Dokumente werden gesichtet, geordnet und katalogartig zusammengestellt und die jeweilige Relevanz kurz beschrieben.
  - Weitere Quellen – insbesondere auch Daten und Dokumentensammlungen im Internet – zur Funktionsweise und zu Absicherung von DNS werden aufgefunden und zusammengestellt.
- Basierend auf der Literaturrecherche und deren Ergebnisse eng referenzierend werden die Absicherungsverfahren – insbesondere DNSsec – hinsichtlich ihrer Funktionsweise, Komponenten, jeweiligen Zielsetzung und Schwachstellen beschrieben.
- Auf Grundlage der Verfahrensbeschreibungen werden ein Testaufbau für ein Netzwerk und die für die anschließenden Untersuchungen zu realisierenden Netzwerkszenarien definiert. Dabei wird auf eine realitätsnahe Strukturierung des Netzes mit mehreren zusammenwirkenden DNS-Servern auf unterschiedlichen Hierarchiestufen und mit mehreren Teilnetzen geachtet.
- Bspw. basierend auf Docker Containern wird dieser Testaufbau realisiert, der die Emulation der zur Demonstration notwendigen Netzelemente und deren Vernetzung ermöglicht. Zu diesem Zweck soll GNS3 verwendet werden, damit die Emulationsumgebung auf einfache Weise dokumentierbar ist, reproduzierbare Ergebnisse liefert und zugleich leicht verändert und damit auch auf andere Untersuchungsgegenstände ausgerichtet werden kann.
- Mit der Emulationsumgebung werden die zuvor definierten Netzwerkszenarien und

Untersuchungsfälle aufgebaut und praktisch erprobt. Die Ergebnisse werden dokumentiert, diskutiert und mit den Erwartungen aus der Literatur verglichen.

- Im Lichte der vorgenommenen und dargestellten Untersuchungen wird DNSsec abschließend mit anderen Absicherungsverfahren verglichen und gegen diese abgegrenzt.

Neben der Erreichung der inhaltlichen Ziele hat die möglichst einfache und exakte Reproduzierbarkeit der Ergebnisse hohe Priorität. Daher werden im Rahmen der Ausarbeitung sämtliche Ergebnisse und Zwischenergebnisse schriftlich und auf Datenträger so dokumentiert und festgehalten, dass eine spätere Reproduktion der Ergebnisse problemlos und einfach möglich ist.

Als Programmiersprache für die Erstellung eigener Anwendungen und Skripten ist grundsätzlich Python zu verwenden. Die Untersuchungen finden auf Linux-Systemen statt. Virtuelle Maschinen werden per Virtualbox betrieben.

Die Aufgabenstellung kann über die Laufzeit der Arbeit angepasst werden.
Über den Fortgang der Arbeit wird wöchentlich schriftlich berichtet.