Projektarbeit 2

für Hn. Ano N'dri Jean Michel Ekra

Informations- und Kommunikationstechnik

Prof. Dr.-Ing. Ulf Niemeyer

Netzwerkemulation zur Untersuchung von 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 für weitergehende 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 das DNS in jüngerer Zeit verstärkt abgesichert.

Ziel dieser Arbeit ist es, DNS grundlegend aufzuarbeiten und in einer aufzubauenden Emulationsumgebung zu demonstrieren.
Damit wird die Grundlage geschaffen, verschiedene Absicherungsverfahren wie DNSsec, DNS over TLS, DNS over HTTPS, DANE zu implementieren und zu untersuchen.

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 wird das DNS hinsichtlich seiner Funktionsweise und Komponenten beschrieben. Im Hinblick auf die Betrachtung von Absicherungsverfahren werden dabei insbesondere auch die Schwachstellen beschrieben.
- Auf Grundlage der Verfahrensbeschreibungen wird ein gemeinsamer Testaufbau und die darauf zu realisierenden Netzwerkszenarien für die späteren Untersuchungen definiert. Dabei wird auch auf eine realitätsnahe Strukturierung des Netzes in mehrere Ebenen und mehrere Teilnetze geachtet.
  Als DNS-Software wird Bind verwendet. Die Konfigurationen der einzelnen Bind-Instanzen im Testaufbau werden entwickelt.
- Basierend auf Docker Containern wird der Testaufbau realisiert, der die Emulation der zur Demonstration notwendigen Netzelemente und deren Vernetzung ermöglicht.
  Die Emulationsumgebung soll so gestaltet werden, dass sie leicht verändert und 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.

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.