

Zensor-resistente, Anonyme Mitteilungsübertragung

Ausgangslage

Die Anonyme Mitteilungsübertragung ist sehr anspruchsvoll. Speziell wenn sie Zensoren-resistent sein soll. Bei dieser Arbeit handelt es sich um eine Vorbereitung für ein nationales Forschungsprojekt. Die Plattform MessageVortex existiert bereits als wissenschaftlicher Prototyp. Sie ist aber nur mit sehr viel Umständen nutzbar und hat noch diverse Schwächen. Sie läuft auf der Basis von Java und trotz anspruchsvoller kryptografischer Operationen läuft sie sogar auf einem RasPI Zero.

MessageVortex ist ein existierendes, Zensoren-resistentes System, dass derzeit Mitteilungen via E-Mail unter Verwendung von Steganografie und raffinierten Routingblöcken versendet. Die Routingblöcke sind so aufgebaut, dass nicht einmal eine Routing-Node (Router) die Möglichkeit hat zu detektieren, welcher Verkehr zu einer Mitteilung gehört und welcher nicht. Eine versendende Node versieht eine reguläre Mitteilung mit einem speziell auf die Mitteilung zugeschnittenen Routingblock. Dieser legt die Mitteilungsoperationen auf den einzelnen Routing-Nodes fest. Damit dies getan werden kann, muss vorgängig auf einzelnen Routing-Nodes ein Proof-of-Work erbracht werden, damit diese auch für die Mitteilung routen.

In die theoretischen Grundlagen des Protokolls werden Sie zum Beginn der Arbeit eingearbeitet und an das Protokoll und deren Funktion wird Ihnen gezeigt und erklärt.

Zielsetzung / Methodik / Vorgehen

Im Rahmen dieser Arbeit sind diverse Verbesserungen vorgesehen. Das Projekt stellt wie oben erklärt komplizierte Onion-Routingblöcke zusammen, die derzeit nicht oder nur kaum visualisiert werden können. Diese Visualisierung soll komplett überarbeitet werden und an ein zeitgenössisches Design angepasst werden.

Ferner gibt es Erweiterungen und Anpassungen im Protokoll, die nie realisiert wurden (z.B. die anonymen Upgrade-Möglichkeiten oder eine flexible API zum Versenden von Mitteilungen auf applikatorischem Weg). Auch die intelligente Generierung von Decoy-Traffic oder das automatische Harvesting von geeignetem Bildmaterial fehlt in der gegenwärtigen Version. Ebenfalls ein Betätigungsfeld wäre die Erweiterung um neue Transportprotokolle (derzeit werden Email-Protokolle unterstützt und eine Erweiterung zu XMPP ist bereits vorbereitet). Des Weiteren gilt es eine Infrastruktur von Routing-Nodes im Internet aufzubauen. Sie sollen effizient gehandhabt und gewartet werden können.

Die genauen Aufgaben im Umfeld des Protokolls und der Infrastruktur können anhand der Fähigkeiten und der Interessen des Masterstudenten angepasst und ausgelegt werden.

Verlangte Skills: Analytische Ingenieurfähigkeiten, Freude an der Anonymisierung und Akribie beim Ändern von Algorithmen, Java

Teilaufgaben

Das Projekt kann in 2 bis 3 Stufen durchgeführt werden: Fortlaufende Projekte 7 (Erweiterung des Protokolls mit Visualisierung und neuen Fähigkeiten), 8 (Aufbau der öffentlichen Routinginfrastruktur) und 9 (Protokolloptimierung, Analyse und ggf. weitere Erweiterung)

Studienart:	☒ Vollzeitstudium ☐ Teilzeitstudium 50% mit Assistenzanstellung
Projektorganisation:	Arbeit in einem Projektteam / Einzelarbeit
Projektfinanzierung:	keine
Arbeitsort:	Windisch
Advisor:	Martin Gwerder

