Dezentralisierte asymmetrische Verschlüsselung über Tor

Die Lösung für sicheres Messaging?

Hendrik Lind

Exposé zur Facharbeit

Windthorst-Gymnasium Meppen

Seminarfach Informatik

11. Dezember 2023

Inhaltsverzeichnis

1 Motivation

Mein Interesse zu diesem Themenkomplex erstreckt sich über mehrere Ebenen. Neben der asymmetrischen und der dahinterliegenden Mathematik, gehört die Programmierung selbst und die Umsetzung eines sicheren Messengers im Tornetzwerk zu meiner Hauptmotivation mich diesem komplexen Thema anzunehmen.

1.1 Tor-Netzwerk

Das Tor-Netzwerk und die Struktur dessen verfolge ich schon seit ein paar Jahren mit hohem Interesse. Oftmals ist das Tor-Netzwerk mit dem Begriff des Darknets verbunden, wodurch es bei den meisten Menschen negative Assoziationen hervorruft. Vor alldem die schwierige Rückverfolgung spielt eine große Rolle in dem Darknet. Sie ist der Grund für mein Interesse, die Struktur zu verstehen und darauf einen neuartigen Messenger zu programmieren.

1.2 Asymmetrische Verschlüsselung

Innerhalb der asymmetrischen Verschlüsselung steht für mich ein mathematischer Erklärungsansatz mitunter im Vordergrund meines Interesses: „Wie schafft es der Angreifer nur mit dem öffentlichen Schlüssel eine verschlüsselte Nachricht nicht entschlüsseln zu können“.

1.3 Programmatischer Aspekt

Die höchste Aufmerksamkeit gilt der Programmierung selbst. Die vielen Facetten des Tor-Netzwerkes mit der asymmetrischen Verschlüsselung zu verknüpfen, sodass am Ende ein funktionierender Messenger entsteht. Die Dezentralisierung des Messengers tragen nochmals zu der Schwierigkeit bei, sodass tiefe Kenntnisse der Informatik gefragt sind. Auch um dieses Wissen zu erlangen bin ich Feuer und Flamme.

2 Relevanz

In der heutigen Zeit spielt die Sicherheit in der Informatik eine immer größere Rolle. Besonders bei Messengerdiensten wird dieser Aspekt nochmals relevanter, da oftmals nicht nur personenbezogene Daten, sondern auch sensible Informationen als Chatnachrichten übertragen werden. Auch in Ländern mit eingeschränkter oder gar keiner Meinungsfreiheit wird Sicherheit und Anonymität wichtiger denn je. Über einen Tor-Messenger können oppositionelle Meinungen und Sichtweisen das autoritäre geführte Land verlassen. In diesem Kontext nimmt die asymmetrische Verschlüsselung eine bedeutende Rolle ein. Mit der Verschlüsselung wird verhindert, dass der Staat Nachrichten mitlesen bzw. Absender ausfindig machen kann. Nahezu jeder benutzt heutzutage Messenger, egal ob nur zum Verabreden mit einer Person oder zum Austausch von sensiblen Geschäftsdaten zwischen Unternehmen. Auch hier wird wieder die Frage wichtig: „Wie sicher ist das eigentlich?“

3 Methodisches Vorgehen

Dieser Abschnitt beschreibt, die Vorgehensweise meiner Facharbeit, die Struktur dieser und zudem der methodische Aufbau dieser.

3.1 Problemerfassung

Auf das Problem der heutigen Messengern aufmerksam zu machen ist das vorrangige Ziel der Einleitung. Es ist wichtig zu verstehen, was einen Messenger ausmacht bzw. wie er funktioniert. Die Verschlüsselungsmethode und der Netzverkehr steht im Vordergrund. Ein besonderer Fokus auf die Rückverfolgung und die Sicherheit sollte hier gelegt werden. Aufgrund der Vielzahl von Messengern ist hier ein umfangreiches Wissen angebracht. Je nach Schwerpunkt des Messengers sind verschiedene Verschlüsselungsmethodiken gewählt worden, welche sowohl ihre Vorteile als auch ihre Nachteile zur Folge haben. Ein Beispiel hierfür wäre Twitter (bzw. X), bei welchem die Direktnachrichten nur eine „Nebenfunktion “des Social-Media-Netzwerkes sind. Dennoch werden auch hier personenbezogene und sensible Daten verschickt, wie zum Beispiel bei Gewinnspielen die Adresse der Beteiligten. Aber auch bei WhatsApp ist durch fehlende Transparenz der Infrastruktur unklar, ob die Nachrichten wirklich ohne Hintertüren verschlüsselt sind. Ganz abgesehen von dem Fakt, dass sich Nachrichten rückverfolgen lassen.

3.2 Aneignung von Wissen

Eine weitreichende Wissensgrundlage für diesen Messengingdienst zu besitzen ist obligatorisch, um eine Rückverfolgung auszuschließen und die Sicherheit der Nachrichten zu gewährleisten. Unter Berücksichtigung wissenschaftliche Arbeiten müssen Schwachstellen diesbezüglich erkannt und behoben werden.

3.2.1 asymmetrische Verschlüsselung

Das Konzept der asymmetrischen Verschlüsselung muss im Zusammenhang mit dem Tor-Netzwerk aufgestellt werden und die mathematischen Verfahren geklärt werden, um die Sicherheit und die möglichen Bedenken dem Leser vorzustellen. Dazu werde ich die Mathematik der Verschlüsselungsmethode erläutern und ein weiteres Vorgehen des Messengers diesbezüglich klären. Der Fokus liegt auch hier auf der Sicherheit und der Dezentralisierung des Dienstes.

3.2.2 Tor-Netzwerk

Die Einbindung des Tor-Netzwerkes ist ein weiterer tragender Pfeiler für meine Facharbeit. Mithilfe des Tor-Netzwerkes lassen sich sicher und anonym Datenpakete verschicken, wobei die Schwierigkeit der Rückverfolgung für außenstehende maximiert wird. Ein tiefes Verständnis der Infrastruktur dieses Netzwerkes ist erfordert, um die Verknüpfungen und Verschlüsselungsvorgehen zwischen den Servern des Tor-Netzwerkes zu verstehen und somit eine nahtlose Einbindung zu garantieren.

Neben der fachlichen Komponente, soll auch durch eine klare und einfache Sprache ein Leser ohne spezielle Fachkenntnisse mit dem Aufbau und der Funktionsweise des Tor-Netzwerkes vertraut gemacht werden.

3.3 Aufbau

Die Facharbeit werde ich mit einer Einleitung beginnen, welche das ausarbeitete Problem vorstellt und das Interesse des Lesers erweckt, indem bei einem bekannten Beispiel eines Messengingdienstes auf ein Sicherheitsbedenken hingewiesen wird. Anschließend werde ich eine Definition für Messengingdienste angeben und mich auf statistische Grundlagen beziehen, sodass der Leser eine nötige Vorstellung solcher Dienste hat. Danach werde ich mögliche Lösungsvorschläge vorstellen und mich für einen dezentralisierten Ende-zu-Ende-verschlüsselten Messenger über das Tor-Netzwerk entscheiden, da dieser meiner Ansicht nach die möglichen Sicherheitsrisiken großflächig abdeckt. Folglich werde ich die asymmetrische Verschlüsselung vorstellen, welche sowohl im Tor-Netzwerk als auch in meinem Messenger eine große Rolle spielen wird. Wichtig ist es auch, die mathematische Ebene miteinzubeziehen und Berechnungen anzufertigen, wie lang ein möglicher Angreifer bräuchte, um ein Schlüsselpaar zu knacken. Aber auch auf mögliche Schwachstellen in Protokollen sollte aufmerksam gemacht werden, sodass es Angreifern schwerfällt, die Software im Tor-Netzwerk zu erkennen. Mit diesem erklärten Verschlüsselungsverfahren lässt sich nun zum Tor-Netzwerk überleiten. Die Infrastruktur und die Ziele des Tor-Netzwerkes sollten hervorgehoben werden, sodass der Leser versteht, inwiefern das Tor-Netzwerk eine Sicherheit liefert und wo selbst das Tor-Netzwerk seine Grenzen hat. Aber auch ein Fokus auf die Nutzbarkeit dieses Programms sollte gelegt werden. So soll die Software eine gut ausgeprägte Nutzerfreundlichkeit besitzen, sodass selbst einfache Nutzer ohne tiefgreifende Informatikkenntnisse eine solche Software benutzen können. Die Dezentralisierung sollte aber auch, wenn wir das Tor-Netzwerk benutzen, nicht in Vergessenheit geraten. Nur mit der Dezentralisierung ist es möglich, kompromittierte Server zu umgehen und sicherzustellen, dass Nutzer (*fast*) nicht gefasst werden können. Somit ist also ein dynamisches Netzwerkmodell zwischen Server und Client erforderlich, sodass hier eine sichere und kontrollierte Kommunikation herrscht. Um weitere Sicherheitsrisiken auszuschließen, wie zum Beispiel ein $BufferOverflow$, werde ich mich in meiner Facharbeit größtenteils auf die Programmiersprache $Rust$ beziehen. Ein weiterer Vorteil dieser ist, die Software in eine einzige ausführbare Datei kompilieren zu können.

4 Hypothesen

Aus meiner Sicht lassen sich drei Aussagen aus meinem Exposé herausarbeiten:

4.1 Zu viel Sicherheit - Kriminalität wird verstärkt

Durch einen Messenger über das Tor-Netzwerk ist es für die Behörden eines autoritär geführten Staates *fast* unmöglich den Absender bzw. den Empfänger ausfindig zu machen. Somit wird die

Kriminalität über das Tor-Netzwerk nur noch verstärkt und Kriminelle weichen von herkömmlichen Messengern aus, um deren Risiken zu minimieren.

4.2 Meinungsfreiheit wird gefördert

Die Meinungsfreiheit wird gestärkt, vor allem in Ländern mit starker Zensur, da die Anwendung dieses Messengers leicht ist und somit es für Nutzer umso einfacher wird, Informationen der Presse mitzuteilen. Ein besserer Einblick für außenstehende Länder ist somit gewährleistet.

4.3 Nicht umsetzbar in herkömmlichen Messengern

Diese Art des Messengers ist nicht in herkömmlichen Messengern umsetzbar, da dieser über das Tor-Netzwerk fungiert. Das Netzwerk zieht somit die Konsequenz einer langsamen Datenübertragung mit sich, da es mehrere Verschlüsselungsebenen hat. Die Dezentralisierung des Netzwerkes verlangsamt es nochmals. Das verschicken einer Nachricht wird somit sehr langsam.