Dezentralisierte asymmetrische Verschlüsselung über Tor

Die Lösung für sicheres Messaging?

Hendrik Lind

Facharbeit

Windthorst-Gymnasium Meppen

Seminarfach Informatik

16. Januar 2024

Inhaltsverzeichnis

1 Einleitung

Nord Korea, China, Russland. In all diesen totalitären Staaten herrscht eine starke Zensur [vgl. Am23]. Rund 1,6 Milliarden Menschen sind nur in diesen drei Staaten von der Einschränkung der Meinungsfreiheit betroffen [vgl. Un22]. Wie können Bürger dieser Staaten ihre Meinung also verbreiten und andere Staaten auf jetzige Probleme aufmerksam machen ohne sich selber in Gefahr zu bringen?

Damit die Außenwelt mit Bürgern und Reportern in totalitären Staaten kommunizieren kann, braucht der Empfänger bei den meisten Messengern (wie WhatsApp, Signal und co) eine Telefonnummer um jenen zu kontaktieren. Allerdings könnte ein Staat, welcher die Meinungsfreiheit beschränkt und Maßnahmen ergreift, sich als dieser Empfänger ausgeben, sodass Bürger/Reporter ihre private Nummer an den Staat überreichen und somit dieser die Nummer rückverfolgen kann [vgl. Fä23]. Und genau hier liegt das Problem: Bürger und Reporter können nicht durch alltägliche Messenger mit der Außenwelt kommunizieren, da der Staat deren Nummer zurückverfolgen kann und somit weiter die Meinungsfreiheit einschränkt und unterbindet.

Durch die zentrale Infrastruktur, welche die meisten Messenger, wie zum Beispiel WhatsApp und Signal verwenden, ist es für totalitäre Staaten, wie China, möglich, die IP-Adressen jener Server zu blockieren und somit für Bürger und Reporter unzugänglich zu machen [vgl. Wu+23].

Ein dezentralisierter Messenger, welcher Ende-zu-Ende verschlüsselt ist und über das Tor-Netzwerk kommuniziert, könnte bei diesem Problem eine Lösung sein. Die Frage, ob ein solcher Messenger die Lösung für Bürger eines totalitären Staates ist, sodass diese ihre Meinung frei äußern können, soll in dieser Arbeit geklärt werden. Um diese Frage beantworten zu können, beschäftigt sich diese Arbeit in dem zweiten Kapitel mit der Ende-zu-Ende-Verschlüsselung, welche durch asymmetrische Verschlüsselung umgesetzt werden kann, und dessen Definition. Das dritte Kapitel beinhaltet eine mögliche Lösung, um eine Anonymität über das Internet zu gewährleisten, wobei das Tor-Netzwerk eine wichtige Rolle spielt. Das vierte Kapitel befasst sich mit einer Dezentralisierung der Infrastruktur, um eine weitere Sicherheitsebene zu schaffen. Zuletzt werden im fünften Kapitel die Vor- und Nachteile eines sol-

chen Messengers betrachtet, im sechsten Kapitel wird eine mögliche Umsetzung des Messengers beschrieben und im siebten Kapitel wird ein Fazit gezogen.

2 Ende-zu-Ende-Verschlüsselung

Ende-zu-Ende-Verschlüsselung (E2EE) bedeutet im Kern, dass nur die Kommunikationspartner die Nachrichten, welche sie senden lesen können und kein dazwischenliegender Knotenpunkt, wie zum Beispiel ein Server [vgl. Gre14]. Die Nachrichten werden also bereits bei dem Sender der Nachricht verschlüsselt, über den Server an den Empfänger gesendet, und schließlich entschlüsselt der Empfänger die Nachricht [vgl. Gre14]. Der Server konnte aber, da die Nachricht verschlüsselt ist, und der dementsprechende Schlüssel nicht auf dem Server abgespeichert ist, die Nachricht nicht entschlüsseln bzw. mitlesen [vgl. Gre14].

Für die Ende-zu-Ende-Verschlüsselung eignet sich die asymmetrische Verschlüsselung [vgl. LB21]

Literatur

[Gre14] Andy Greenberg. „Hacker Lexicon: What Is End-to-End Encryption?“ In: *WIRED* (Nov. 2014). URL: https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption (besucht am 16. 01. 2024).

[LB21] Ben Lutkevich und Madelyn Bacon. „end-to-end encryption (E2EE)“. In: *Security* (Juni 2021). URL: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE (besucht am 16. 01. 2024).

[Un22] United Nations. *World Population Prospects - Population Division*. Jan. 2022. URL: https://population.un.org/wpp/Download/Files/1_Indicators%20(Standard)/EXCEL_FILES/1_General/WPP2022_GEN_F01_DEMOGRAPHIC_INDICATORS_COMPACT_REV1.xlsx (besucht am 13. 01. 2024).

[Am23] Amnesty International. *Amnesty International Report 2022/23*. London WC1X 0DW, United Kingdom: International Amnesty Ltd, 2023. ISBN: 978-0-86210-502-0. URL: https://www.amnesty.org/en/wp-content/uploads/2023/04/WEBPOL1056702023ENGLISH-2.pdf (besucht am 13. 01. 2024).

[Fä23] Jan Fährmann. „Rechtliche Rahmenbedingungen der Nutzung von Positionsdaten durch die Polizei und deren mögliche Umsetzung in die Praxis–zwischen Strafverfolgung und Hilfe zur Wiedererlangung des Diebesguts“. In: *Private Positionsdaten und polizeiliche Aufklärung von Diebstählen*. Nomos Verlagsgesellschaft mbH & Co. KG. 2023, S. 141–176. ISBN: 978-3-8487-5905-7.

[Wu+23] Mingshi Wu, Jackson Sippe, Danesh Sivakumar, Jack Burg, Peter Anderson, Xiaokang Wang, Kevin Bock, Amir Houmansadr, Dave Levin und Eric Wustrow. „How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic“. In: *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, S. 2653–2670. ISBN: 978-1-939133-37-3. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/wu-mingshi (besucht am 14. 01. 2024).