Anlage zur Kurzinformation „Zum Brechen oder Umgehen von Ende-zu-Ende-Verschlüsselungen“ (WD 8 - 3000 - 089/20)

Antwortschreiben der Zentralen Stelle für Informationstechnik im Sicherheitsbereich vom 1. Dezember 2020 (per Email)

„Wie unterscheiden sich die Methoden hinsichtlich des Mitlesens verschiedener Ende-zu-Ende verschlüsselt übertragener Dateiformate (Bilder, Videos, Audios, Textnachrichten)?

Grundlage für alles weitere ist die Annahme, dass Unternehmen, die mobile Messaging-Dienste anbieten, die im Dokument vorgeschlagenen Lösungen in ihren Anwendungen implementieren würden. Da eine Kommunikation, die Ende-zu-Ende verschlüsselt wurde, nicht ohne Kenntnis der kryptographischen Schlüssel mitlesbar ist, sind andere Ansätze gewählt worden. Die in dem Dokument aufgeführten Methoden hinsichtlich des Mitlesens verschiedener Ende-zu-Ende verschlüsselt übertragener Dateiformate unterscheiden sich im technischen Ansatz und somit auch im Ort, an dem diese durchgeführt werden. Die Dateiformate selbst spielen grundsätzlich keine Rolle, allerdings gehen die Datenarten in die Betrachtung der im weiteren beschriebenen Endgerätemethoden ein.

Entgegen der Implikation der Überschrift setzen die Lösungsansätze nicht auf den Ende-zu-Ende verschlüsselten Daten an, sondern zielen auf die beteiligten Elemente im Rahmen der Ende-zu-Ende-Verschlüsselung nämlich Endgerät, Server und Verschlüsselungsart ab.

Die verschiedenen Methoden werden anhand von Effektivität, Machbarkeit, Privatsphäre, Sicherheit und Transparenz betrachtet.

1. Bei den vier Methoden, die am Endgerät ansetzen, erfolgt die Detektion

a. vollständig am Endgerät,

b. durch Abgleich mit bekanntem Material am Server, wobei Bilder und Videos nur als Hashwert d.h. in Form einer kryptografischen Prüfsumme am Endgerät vorliegen,

c. und durch teilweises Erzeugen des Hashwertes von Bild und Video am Endgerät und Erzeugen des restlichen Hashwertes am Server. Die Methode c) erscheint am ehesten umsetzbar. Allerdings ist dabei die Untersuchung von Text (z.B. bei Grooming) nicht möglich. Hashwert-basierte Ansätze haben allerdings den Nachteil, dass kleinste Änderungen in Bild- oder Videomaterial dafür sorgen, dass die Vergleichbarkeit fehl schlägt.

d. Die vierte Lösung d) unterscheidet sich gänzlich durch die Benutzung von Klassifikatoren auf dem Endgerät. Das Hauptproblem ist hier, dass diese noch nicht ausgereift sind; Text-Detektoren scheinen am besten machbar, wodurch sich die Lösungen d) und c) ergänzen würden.

2. Bei den drei serverseitigen Methoden handelt es sich um

a. eine Sicherheitsenklave auf dem Server des Providers, die die Nachricht unverschlüsselt erhält und erst nach Überprüfung Ende-zu-Ende-verschlüsselt verschicken lässt,
b. den Abgleich von Hashwerten (wie bei 1b) auf einem Third-party Server
c. oder auf mehreren Third-party Servern.

Methode a) würde als einzige auch Machine-Learning-basierte Klassifikatoren für unbekanntes KiPo-Material ermöglichen. Sicherheitsbedenken entstehen bei allen Methoden durch die Vertrauenswürdigkeit der Prüfstelle. Diese wären am ehesten unter Nutzung mehrerer Third-party Server (Lösung c) zu minimieren.

3. Die einzige Methode, die die Verschlüsselung betrifft heißt "On-device homomorphic encryption with server side hashing and matching" (Paper H. Farid). Aus einem so verschlüsselten Bild ließe sich ein verschlüsselter Hashwert berechnen, der dann mit bekanntem KiPo-Material abgeglichen werden könnte. Der Server darf die homomorphic decryption keys nicht besitzen, womit die Privatsphäre gewahrt bliebe. Diese Methode ist noch in der Entwicklung und aktuell zu aufwendig für Videos. Die Vorteile in Bezug auf Privatsphäre, Sicherheit und Transparenz wären jedoch hoch.

Am Ende des Papers gibt es eine tabellarische Übersicht über die Methoden inklusive 5 Metriken. Als am relevantesten ergeben sich die Methoden 1b, 1c und 2a.

Welche dieser Methoden ließe sich auch in anderen Kriminalitätsphänomenen zum Mitlesen Ende-zu-Ende verschlüsselter Textnachrichten einsetzen (Messenger Signal, Telegram, WhatsApp, Facebook betrachten)?

Welche dieser Methoden würde es auch ermöglichen, nicht über Anbieter proprietärer Messenger versandte Ende-zu-Ende verschlüsselte Textnachrichten, sondern mittels PGP in Mailprogrammen (etwa Outlook, Thunderbird) verschlüsselte Dateien mitzulesen?

Die eingesetzte Technologie ist unabhängig von den darüber transportierten Inhalten, insofern unabhängig von den Kriminalitätsphänomenen. Darüber hinaus kann keine dedizierte Aussage getroffen werden.“

Zentrale Stelle für Informationstechnik im Sicherheitsbereich
Zamdorfer Straße 88
81677 München