Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

**Fakultät für
Mathematik, Informatik
und Naturwissenschaften**

UHH · FB Informatik · SVS · Prof. Dr. Hannes Federrath
Vogt-Kölln-Str. 30 · 22527 Hamburg

Prof. Dr. Hannes Federrath

MIN-Fakultät
Fachbereich Informatik
Sicherheit in Verteilten Systemen (SVS)
Vogt-Kölln-Str. 30
22527 Hamburg

Tel. +49 (0)40 - 42883 - 2358
Fax +49 (0)40 - 42883 - 2086
federrath@informatik.uni-hamburg.de
www.informatik.uni-hamburg.de/svs

An den
Innen- und Rechtsausschuss des
Schleswig-Holsteinischen Landtages

per E-Mail: innenausschuss@landtag.ltsh.de

Schleswig-Holsteinischer Landtag
Umdruck 18/5413

08.01.2016

Stellungnahme zum Antrag der Fraktion der PIRATEN, Drucksache 18/3311, Bundesratsinitiative zur technischen Sicherung des Fernmeldegeheimnisses – Ende-zu-Ende-Verschlüsselung für das Telefon

Sehr geehrte Damen und Herren,

gerne komme ich dem Wunsch nach, Stellung zu dem o.g. Antrag zu nehmen.

Zusammenfassung

Mit der Umstellung analoger und digitaler Telefonanschlüsse auf IP-Telefonie, wie sie derzeit in Deutschland betrieben wird, besteht die Möglichkeit, die bereits vorhandenen technischen Standards zur Umsetzung einer Ende-zu-Ende-Verschlüsselung von Gesprächsdaten zu nutzen und somit zum Grundrechtsschutz von Bürgern, Amtsträgern und zum Schutz der Wirtschaft vor Industriespionage einen wichtigen und notwendigen Beitrag zu leisten.

Die technischen Protokolle für IP-Telefonie sehen die Möglichkeit vor, sowohl Signalisierungsdaten (Verkehrsdaten) als auch Gesprächsdaten (Inhaltsdaten) im Klartext oder verschlüsselt zu übertragen. Die Realisierung der Ende-zu-Ende-Verschlüsselung aller Gesprächsdaten bei der IP-Telefonie ist in Deutschland sowohl technisch möglich als auch wirtschaftlich machbar. In öffentlichen Telefonnetzen können und sollten alle Signalisierungsdaten durch Verbindungsverschlüsselung geschützt werden.

Technische Hintergründe

Ein IP-Telefonat läuft in den zwei Phasen „Signalisierung des Verbindungswunschs“ und „Übermittlung der Gesprächsdaten“ ab, die nachfolgend kurz bzgl. der Umsetzung von Verschlüsselung analysiert werden.

Signalisierung des Verbindungswunschs: Zunächst erfolgt mittels des Protokolls SIP (Session Initiation Protocol, standardisiert im RFC 3261) die Signalisierung eines Verbindungswunschs vom Anschluss des rufenden Teilnehmers A zu seinem Provider (hier: sein SIP-Registrar). Der SIP-Registrar von A vermittelt den Verbindungswunsch zum Provider des gerufenen Teilnehmers B.

Dessen SIP-Registrar signalisiert dem Anschluss des gerufenen Teilnehmers den Verbindungswunsch. Die genannten drei Kommunikationsschritte (Teilnehmer A zu SIP-Registrar, SIP-Registrar zu SIP-Registrar, SIP-Registrar zu Teilnehmer B) können jeweils verschlüsselt erfolgen, allerdings müssen in den heutigen Protokollen bei den SIP-Registraren die Signalisierungsdaten unverschlüsselt vorliegen. Es handelt sich somit um eine sog. Verbindungsverschlüsselung der Signalisierungsdaten. Die Verbindungsverschlüsselung der Teilabschnitte von SIP kann mittels des sehr weit verbreiteten und universellen Protokolls TLS (Transport Layer Security, standardisiert in zahlreichen RFCs) oder des verbindungslosen DTLS (Datagram Transport Layer Security, standardisiert in RFC 6347) erfolgen, ist jedoch nicht verpflichtend vorgesehen. Zudem bietet Verbindungsverschlüsselung allgemein wenig Transparenz für den Endnutzer, d.h. es ist nicht überprüfbar, ob und ggf. welche Teilabschnitte bei der Signalisierung verschlüsselt sind.

Das SIP-Protokoll sieht die Möglichkeit vor, den Verbindungsaufbau direkt vom rufenden zum gerufenen Teilnehmer durchzuführen, d.h. Ende-zu-Ende-Verschlüsselung wäre technisch möglich. Davon ist jedoch in öffentlichen Netzen abzuraten: Dem rufenden Teilnehmer muss die aktuelle IP-Adresse des gerufenen Teilnehmers bekannt sein, d.h. anstelle der herkömmlichen Telefonnummer wird die IP-Adresse des gerufenen Teilnehmers verwendet. In geschlossenen (etwa firmen- oder behördeninternen) VoIP-Systemen ist dies ggf. möglich, in öffentlichen Netzen wäre ein öffentlich zugängliches Online-Register der aktuellen IP-Adressen aller VoIP-Kunden erforderlich. Auf diese Weise würde ein nicht unterdrückbares Kennzeichen aller Anschlüsse öffentlich abrufbar sein, was selbst bei regelmäßigem Wechsel der IP-Adresse (dynamische IP-Adressen) zu einer Verringerung des Datenschutzniveaus beitragen würde. Eine Ende-zu-Ende-Verschlüsselung der Signalisierungsdaten scheidet somit bei den derzeitigen technischen Möglichkeiten aus.

Übermittlung der Gesprächsdaten: Die Inhaltsdaten werden direkt zwischen den Geräten der Teilnehmer mittels des Protokolls RTP (Real-Time Transport Protocol, standardisiert im RFC 3550) ausgetauscht. Anstelle von RTP kann zum Datenaustausch auch das verschlüsselte SRTP (Secure Real-Time Transport Protocol, standardisiert im RFC 3711) verwendet werden. Sofern IP-Telefone als Endgeräte verwendet werden, ist eine mit SRTP realisierte Telefonverbindung sicher Ende-zu-Ende-verschlüsselt, wobei der Schlüsselaustausch wiederum von anderen Protokollen übernommen wird, z.B. vom Protokoll ZRTP (RFC 6189) oder vom MIKEY (RFC 3830).

Bei den auf IP-Telefonie umgestellten Anschlüssen können herkömmliche Analog-, Schnurlos- oder ISDN-Telefone an den Heimrouter angeschlossen werden. In diesem Fall wird eine mit SRTP realisierte Telefonverbindung im Heimrouter entschlüsselt und auf herkömmliche Weise an das Endgerät weitergeleitet. Insb. bei den bisher noch immer verbreiteten Zwangsroutern, die einige Provider als ihren Netzabschluss ansehen, würde somit die Entschlüsselung bereits im Verfügungsbereich des Providers erfolgen (wenngleich dieser sich üblicherweise im Gebäude des Teilnehmers befindet), zumal Zwangsrouter ohne Zustimmung und Wissen des Teilnehmers mit neuer Firmware versehen werden können. Dementsprechend hat der Teilnehmer keine Transparenz über das tatsächlich erreichte Schutzniveau, sodass streng genommen eine Verschlüsselung im Router keine Ende-zu-Ende-Verschlüsselung darstellt.

Wenn die an einer Kommunikation beteiligten Endgeräte und Provider die entsprechenden technischen Funktionen zur Verschlüsselung besitzen und diese aktiviert sind, kann ein IP-Telefonat somit auch verschlüsselt erfolgen.

Schlussbemerkungen

Gerätehersteller und Provider sind bisher nicht verpflichtet, technische Kommunikationsstandards vollständig umzusetzen. In der Praxis wird es daher, solange eine Umsetzung freiwillig wäre, zu technischen Problemen kommen, da etwa ein Kommunikationspartner oder ein Provider über die notwendigen Geräte oder Funktionen zur Verschlüsselung bisher nicht verfügt. In diesem Fall ist es

in den Kommunikationsprotokollen notwendig, auf einen von allen Beteiligten unterstützen Modus (hier: unverschlüsselte Kommunikation) zurückzufallen.

Eine im Sinne der Transparenz verlässliche Lösung sollte daher nicht nur technisch und kryptographisch sicher sein, sondern muss den Kommunikationspartnern geeignete Rückmeldungen über das erreichte Schutzniveau der Kommunikation geben – etwa durch ein angezeigtes Schlüsselsymbol im Display des Telefons.

Jenseits der klassischen Telefonie mittels eines normalen Telefonanschlusses (IP-basiert oder nicht) existieren ohnehin bereits zahlreiche Dienste, die Ende-zu-Ende-Verschlüsselung ermöglichen.

Dem etwaigen Argument, die Strafverfolgung sei bei Einführung von Ende-zu-Ende-Verschlüsselung in der IP-Telefonie erschwert, kann nicht gefolgt werden, da Kriminelle bereits heute auf zuverlässige und abhörsichere Alternativen zum normalen Telefon ausweichen können. Deshalb hat der Gesetzgeber die Voraussetzungen geschaffen, mittels Quellen-TKÜ ggf. zu ermitteln.

Eine sichere Ende-zu-Ende verschlüsselte Telefonie stellt somit eindeutig einen notwendigen Grundrechtsschutz dar, der wirtschaftlich machbar, technisch längst überfällig und – da die gesetzlichen Voraussetzungen für die Quellen-TKÜ gegeben sind – auch rechtsstaatlich verhältnismäßig ist.

08.01.2016

gez.
Prof. Dr. Hannes Federrath
Universität Hamburg