

Einfluss von Sicherungsmaßnahmen auf die Übertragungsqualität von VoIP

Peter Backs, Sirrix AG

Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit if(is)
p.backs@sirrix.com, norbert.pohlmann@internet-sicherheit.de

Abstract: Mit zunehmender Verbreitung von Voice over IP (VoIP) steigt auch das Interesse am Schutz dieses neuen Dienstes, so dass mehrere Ansätze entwickelt wurden, um diesem Schutzbedarf nachzukommen. Während die Sicherheit vieler dieser Verfahren anerkannt ist, ist bisher nicht ausführlich untersucht, in wie weit diese Sicherungsmaßnahmen die Benutzung von VoIP beeinflussen. Der Schwerpunkt dieser Arbeit liegt daher nicht nur in der Analyse und Gegenüberstellung der Sicherheitsverfahren, sondern betrachtet auch deren Einfluss auf die Übertragungsqualität. Das sich die Sicherheitsmaßnahmen hauptsächlich auf die benötigte Übertragungsbandbreite auswirken, ist das wichtigste Ergebnis dieser Arbeit.

1 Einleitung Voice over IP

Als VoIP wird allgemein die Übertragung von Sprachdaten über das Internet Protocol (IP) bezeichnet. Wie auch beim leitungsvermittelten öffentlichen Telefonnetz gibt es bei VoIP Signalisierungsdaten zum Anrufauf- und abbau, sowie zur Anrufsteuerung und die eigentlichen Sprachdaten. Durch Abhören der Signalisierung lassen sich die Verbindungsdaten einer Nebenstelle ermitteln. Angriffe auf die Sprachdaten betreffen vorrangig das Mithören von Gesprächsinhalten; Manipulationsangriffe gegen den übertragenen Sprachstrom sind möglich, gestalten sich aufgrund des schwer vorhersehbaren Gesprächsverlaufs jedoch als schwierig.

Sprachdaten sind Echtzeitdaten, die mit möglichst geringer Verzögerung übertragen werden sollten, um eine gute Sprachqualität und einen flüssigen Dialog via VoIP zu ermöglichen. Dieser Tatsache muss beim Schutz von VoIP Rechnung getragen werden.

2 Möglichkeiten zur Sicherung von VoIP

Es gibt zwei unterschiedliche Ansätze den Schutzbedarf von VoIP zu decken.

Der erste Ansatz ist die Nutzung von VoIP über ein Virtual Private Network (VPN). In vielen Unternehmen mit mehr als einer Niederlassung existieren VPNs, um den Datenaustausch zwischen diesen Geschäftsstellen zu schützen. Gerade wenn eine solche Sicherheitsinfrastruktur schon vorhanden ist, liegt es nahe, diese auch für die VoIP-Daten – Signalisierung und Medienstrom - zu nutzen; die aufwendige Einrichtung einer speziellen Lösung würde wegfallen.

Die andere Möglichkeit zur Sicherung von VoIP ist der Schutz durch VoIP-spezifische Sicherungsmaßnahmen, die Ende-zu-Ende-Sicherung der VoIP-Daten bieten. Für die Absicherung von Signalisierung und Medienstrom gibt es verschiedene Verfahren, die allerdings die Schaffung einer neuen Infrastruktur voraussetzen. Für die Sicherung des Medienstroms kommt häufig SRTP (Secure Real-time Transport Protocol) zum Einsatz.

3 Einfluss von Sicherungsmaßnahmen auf die Übertragungsqualität von VoIP

VPN-basierte VoIP-Sicherung lässt sich in Bezug auf die Quality of Service (QoS) Parameter gut messen und analysieren, da die VPN-Gateways transparent in den Übertragungsweg geschaltet werden. Diese Parameter sind Ende-zu-Ende-Verzögerung (Delay), Schwankungen in der Übertragungszeit (Jitter), Paketverluste (Packet Loss, PL) und die benötigte Bandbreite. Die wesentlichen Ergebnisse sind nachfolgend zusammen gefasst.

3.1 Versuchsaufbau

VPNs koppeln üblicherweise Subnetze an deren Grenzen Security Gateways stehen. Für diese wurden im Versuchsaufbau verschiedene Arten von VPN-Boxen oder einfache Router ohne Sicherheitsfunktionen eingesetzt. Als repräsentative Auswahl an Security Gateways wurde die frei verfügbare Implementierung des IPSec-Protokolls OpenSWAN und das ebenfalls freie OpenVPN gewählt und einer Referenzmessung, in der einfache Router anstelle der VPN-Gateways eingesetzt wurden, gegenübergestellt.

Die Messungen wurden mit zwei unterschiedlichen Messtools durchgeführt: eine Beta-Version des Produkts NetGage des Projektes QoSSIP der FH Köln und der „VoIP Test Suite“ der ITD Informationstechnologie GmbH & Co. KG. Die VoIP Test Suite unterstützt verschiedene Sprach-Codecs nach den ITU-T Recommendations G.711, G.726, G.723.1 und G.729a sowie GSM. NetGage verwendet ausschließlich G.711.

3.2 Die Parameter Delay, Jitter und Packet Loss

Die Messungen ergaben, dass die eingesetzten Sicherungsmaßnahmen keinen messbaren Einfluss auf Jitter oder Packet Loss haben. Darüber hinaus hat sich der Delay der VoIP-Verbindungen nur unkritisch erhöht. Dies zeigt Abbildungen 1.

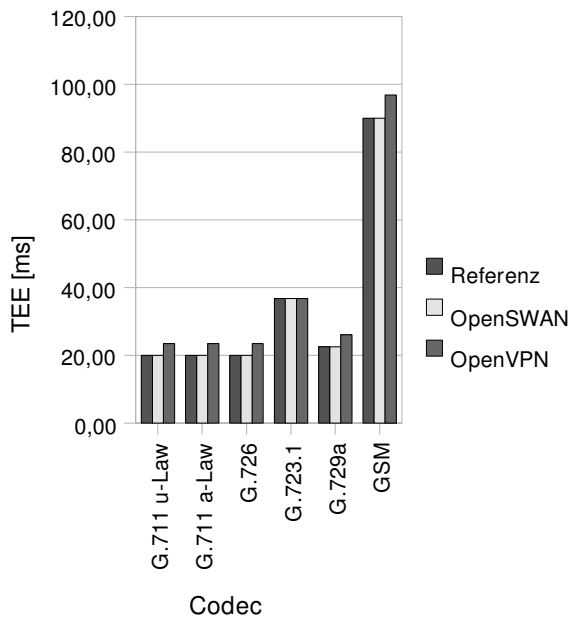


Abbildung 1: Verzögerung gesicherter und ungesicherter VoIP-Übertragung.

Die geringen Unterschiede sind nicht zuverlässig reproduzierbar und durch Messfehler zu erklären. Die Kontrollmessung mit dem zweiten Tool bestätigt – unter Berücksichtigung von Messfehlern – eine Erhöhung der Verzögerung um lediglich 1-2 ms, was nahezu unerheblich ist. Die Wahl des Sprach-Codecs hat keinen Einfluss auf Delay, Jitter oder Packet Loss.

Beim VoIP-spezifischen Ansatz treten aufgrund der Ende-zu-Ende-Sicherung Probleme bei der QoS-Analyse auf, denn in diesem Fall muss die eingesetzte Messsoftware die entsprechenden Sicherungsprotokolle unterstützen, was zur Zeit bei keiner Lösung der Fall ist. Es läßt sich vorrangig nur der QoS-Parameter Bandbreite zuverlässig messen.

3.3 Der Parameter Bandbreite

Da der Overhead der VPN-basierten und VoIP-spezifischen Sicherheitslösungen stark von den verwendeten VoIP- und Sicherheitseinstellungen abhängt, kann durch folgende Parameter die Bandbreite einer VoIP-Verbindung beeinflusst werden:

- Paketierung der Sprachsegmente. Werden mehrere Sprachsegmente pro IP-Paket übertragen, werden insgesamt weniger Pakete gesendet. Es entsteht weniger Overhead durch IP, UDP, RTP, aber auch weniger Overhead durch die Sicherheitslösungen. Werden mehrere Segmente pro Paket übertragen, ist die benötigte Bandbreite geringer, die Verzögerung der Sprachverbindung nimmt jedoch erheblich zu, da die Sprachsegmente länger beim Sender zwischengespeichert werden.
- Wahl des Codecs.
 - Codec-Bandbreite. Die Codecs unterscheiden sich grundsätzlich in der benötigten Bandbreite, aber auch in der Sprachqualität.
 - Segmentgröße. Abhängig von der Segmentgröße werden mehr oder weniger Pakete übertragen, was den Overhead beeinflusst. Hier gilt dasselbe wie für den ersten Punkt.
- Blockgröße der verwendeten Verschlüsselung. Die Blockgröße eines Verschlüsselungsalgorithmus stellt die Menge an Bytes dar, in der der Algorithmus Nutzdaten verschlüsselt. Die Menge der Nutzdaten muss daher ein ganzzahliges Vielfaches der Blocklänge sein. Ist das nicht der Fall, wird dieser Zustand durch Auffüllen von Padding-Bytes erreicht. Abhängig von der Blockgröße und der Größe und Anzahl der Sprachsegmente pro Paket kann daher unterschiedlich viel Padding entstehen. Die gängigsten Blockgrößen sind 8 Byte (z.B. DES) und 16 Byte (z.B. AES).

Mit welcher Bandbreite abhängig von oben genannten Einstellungen gerechnet werden muss, kann Abbildung 2 entnommen werden.

	Sprache,		RTP	RTP + IPSec		RTP + OpenVPN		SRTP
Codec	leitungs vermittelt	Segm. / Paket	n/a	BL 16	BL 8	BL 16	BL 8	n/a
G.711	64	1	96	147,2	140,8	166,4	153,6	102,4
		2	80	105,6	102,4	115,2	108,8	83,2
G.723.1	5,3	1	16	32	29,87	38,4	34,13	18,13
		2	10,67	20,27	18,13	21,33	20,27	11,73
	6,3	1	17,07	36,27	32	38,4	36,27	19,2
		2	11,73	20,27	19,2	23,47	21,33	12,8
G.726	16	1	48	96	89,6	115,2	102,4	54,4
		2	32	60,8	54,4	64	60,8	35,2
	24	1	56	108,8	102,4	115,2	108,8	62,4
		2	40	67,2	60,8	70,4	67,2	43,2
	32	1	64	121,6	108,8	128	121,6	70,4
		2	48	73,6	70,4	83,2	76,8	51,2
	40	1	72	121,6	115,2	140,8	128	78,4
		2	56	80	76,8	89,6	83,2	59,2
G.729a	8	1	40	96	83,2	102,4	96	46,4
		2	24	48	44,8	57,6	51,2	27,2
GSM (FullRate)	13	1	29,2	54,4	51,2	64	57,6	32,4
		2	21,2	33,6	32	38,4	35,2	22,8
iLBC	13,33	1	24	40,53	38,4	46,93	42,67	26,13
		2	18,67	26,67	25,6	29,87	27,73	19,73
	15,2	1	31,2	60,8	54,4	64	57,6	34,4
		2	23,2	36,8	33,6	38,4	36,8	24,8

Abbildung 2: Bandbreitenbedarf [KBit/s] der Sprachcodecs in Abhängigkeit der Codeceinstellungen beim Einsatz verschiedener Sicherungsmaßnahmen mit unterschiedlichen Verschlüsselungsblocklängen (BL).

Die VoIP-spezifische Verschlüsselung SRTP verwendet im Gegensatz zu den VPN-Lösungen standardmäßig eine Stromverschlüsselung, die keinen Overhead durch Padding erzeugt. Außerdem entsteht hier kein Overhead durch das Tunneln der IP-Pakete.

4 Fazit

Die Messungen haben gezeigt, dass sich die Sicherheitsmaßnahmen vorrangig auf die benötigte Bandbreite bei der Übertragung von VoIP auswirken. Abhängig von den oben dargestellten Einstellungen kann sich die Größe der VoIP-Pakete mehr als verdoppeln. Für Benutzer mit schmalbandiger Internetanbindung sowie für Unternehmen mit vielen VoIP-Nutzern kann dies ein erhebliches Problem darstellen. Durch Einstellungen der VoIP- und Verschlüsselungssoftware bzw. der Wahl selbiger lässt sich jedoch die Bandbreite direkt beeinflussen (siehe Tabelle).

Stellt eine zu hohe Bandbreite ein kritisches Problem dar, so ist das VoIP-spezifische SRTP einer tunnelnden VPN-Lösung vorzuziehen. Spielt die Bandbreite dagegen keine entscheidende Rolle und eine VPN-Infrastruktur ist in genügender Abdeckung vorhanden, so kann auch VoIP problemlos auf diese Art gesichert werden. In diesem Fall besteht der Schutz jedoch nur auf der Übertragungsstrecke zwischen den Security Gateways.

Da die verbreiteten Sicherungsverfahren jedoch allesamt PKI-basiert sind oder eine andere Infrastruktur für kryptographische Schlüssel vorhanden sein muss, die es jedoch nicht in weitgehender organisationsübergreifender Umfassenheit gibt, wird VoIP auch in nächster Zeit nur in Insellösungen sicher übertragen werden.