Bei Anruf Vertrag

Integrität und Nichtabstreitbarkeit von VoIP-Telefonanrufen

Kai-Oliver Detken

Das Szenario ist bekannt: Ein Versicherungsagent spricht mit einem potenziellen Kunden und beide Seiten sind sich einig. Doch der Vertrag kommt erst zustande, wenn das papierbasierte Vertragswerk zugeschickt, gelesen und unterzeichnet wurde. Eine intelligentere Methode wird im Forschungsprojekt INTEGER umgesetzt. Hier wird der Kommunikationspartner durch sichere Authentifizierung erkannt und das Gespräch in einem Archiv aufgezeichnet. Durch Integrität wird nun sichergestellt, dass der mündliche Vertrag (das Archiv) nicht nachträglich verändert werden kann. Der Kunde unterzeichnet sozusagen „smart" per Telefonanruf über sein Softphone. Der Artikel beschreibt diese Lösung und weitere Anwendungsszenarien.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Die vollständige Digitalisierung der Nachrichtentechnik erlaubt neue Angriffsszenarien, die mit bisherigen Telefontechniken nicht möglich waren, da für das Abhören analoger Telefonate oder Videosignale stets der physische Zugang zu dem Transportmedium notwendig war. Bei der internetbasierten Kommunikation, zu der auch Voice over IP (VoIP) gehört, die von einer prinzipiell unbegrenzten Anzahl zwischenliegender Knoten aus abgefangen werden kann, ist ein Abhören für einen Angreifer erheblich einfacher. Auch das Einspeisen unerwünschter Kommunikation (Spam, Spit) ist in digitalen Netzen wesentlich leichter zu bewerkstelligen.

Neben der nun notwendigen sicheren Kommunikation in VoIP-Netzen legen neue Anforderungen zusätzlich Wert auf Integrität (Fälschungssicherheit) und Nichtabstreitbarkeit (Wer ist der Gesprächspartner? Was ist der Inhalt?) von internetbasierter multimedialer Kommunikation. Die bei VoIP verwendeten offenen Übertragungsstandards ermöglichen neben der Sprachkommunikation auch weitere Anwendungen. Das Session Initiation Protocol (SIP) kann z.B. auch zum Initiieren der Übertragung von beliebigen Multimediadatenströmen dienen. Gerade aber im B2B- und B2C-Bereich fehlt den aktuellen Lösungen der Nachweis über die Vertraulichkeit und die Verlässlichkeit der Kommunikation.

Das INTEGER-Projekt

Die von INTEGER (www.integer-project.de) angestrebte, völlig neuartige Form der Nichtabstreitbarkeit mündlicher Kommunikation ermöglicht grundlegend effizientere Geschäftsabläufe (u.a. als Beweis für mündliche Vertragsabschlüsse) und wird zum Teil bereits heute im Finanzsektor von der EU gefordert. Auch im Verhältnis zwischen Unternehmen und Outsourcing-Dienstleistern, wie z.B. Call-Center, sind die geplanten Ergebnisse einsetzbar und ermöglichen durch die dargestellte Sicherheit eine verbesserte Arbeitsteilung. Das weitreichende Ziel, mündlich geschlossene Verträge zwischen zuvor unbekannten Partnern und ohne Zeugen zu beweisen, stellt zudem ein neues Paradigma in der Digitalisierung der Arbeitswelt dar und eröffnet neue Felder des verbindlichen „Collaborative Commerce".

Aber auch ohne die weitreichenden Ziele aus der Forschung muss VoIP dem Telekommunikationsgesetz (TKG) genügen, indem nur einzelne Gespräche gesetzeskonform auf richterliche Anordnung abgehört und aufgezeichnet werden. Dies wird heute von den meisten SIP-Providern aber nicht umgesetzt. Im Gegenteil, die Gespräche werden größtenteils völlig ungeschützt und im Klartext über das Internet übertragen. Ein Abhören ist daher auf Basis standardkonformer Technik auch Einzelnen möglich, die über kein Detailwissen verfügen. Dies sollte zukünftig auf jeden Fall geändert werden und ist auf Basis vorhandener Sicherheitsstandards auch möglich, erfordert aber entsprechende Investitionen der SIP-Provider.

Allgemein kann die multimediale Kommunikation zwischen zwei Parteien als eine Transaktion angesehen werden, die in verschiedenen Kontexten (z.B. bei der Entscheidungsfindung für einen Auftrag) einen hohen Schutzbedarf besitzt und deshalb vollständig geschützt werden muss. Die Nichtabstreitbarkeit einer Konversation ist hierbei eine grundlegende Voraussetzung. Um dies zu erreichen, müssen drei generelle Aufgaben mithilfe einer digitalen Signatur gelöst werden:

- Integritätsschutz der Konversation: Die Integrität einer digitalen Konversation unterscheidet sich im Vergleich zur Integrität von anderen di-

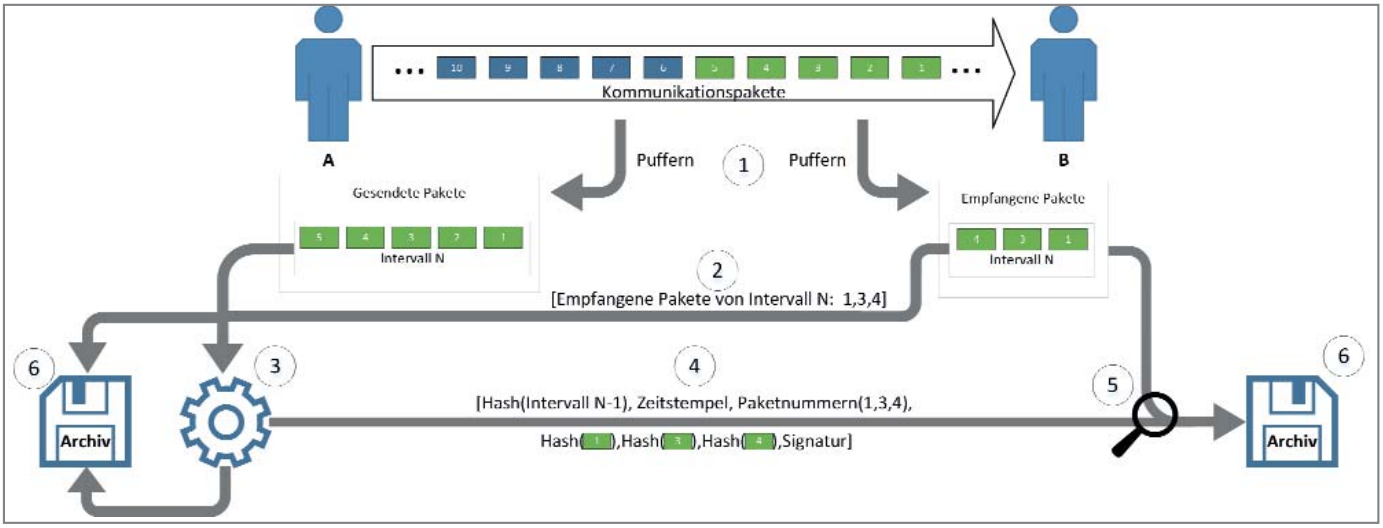

Bild 1: Kommunikationsdarstellung zwischen zwei Vertragsparteien

gitalen Daten in Bezug auf die Bedeutung des zeitlichen Kontextes. Eine digitale Konversation wird in einem direkten zeitlichen Zusammenhang geführt. Daher erfordern insbesondere die Folge der übertragenen Pakete, der Verlust von Paketen auf dem Transportweg und der Zeitpunkt der Kommunikation eine besondere Betrachtung.

- Authentifizierung der Kommunikationspartner: Um ein Gespräch auf seine Teilnehmer zurückführen zu können, ist deren Authentifizierung notwendig. Wünschenswert ist dabei, dass das gesamte Gespräch und die vorhergehende Authentifizierung durch authentifizierte Geräte geführt wird, um Integritätsschutz „Ende zu Ende" gewährleisten zu können.
- revisionssichere Speicherung der Kommunikation: Die revisionssichere Dokumentation der Kommunikation und damit maßgeblich das sichere und unveränderliche Speichern der Inhalte ist in diesem Zusammenhang ein zentraler Punkt für die Nichtabstreitbarkeit der Konversation. Hierbei muss insbesondere auch auf die Sicherung gegen mutwillige Manipulation geachtet werden.

Zur Erfüllung der ersten beiden Punkte hat das INTEGER-Projekt gezeigt, dass mithilfe eines Vertrauensankers (z.B. Trusted Platform Module – TPM) die Nichtabstreitbarkeit einer Aufzeichnung erreicht werden kann, ohne eine aufwendige Public-Key-Infra-

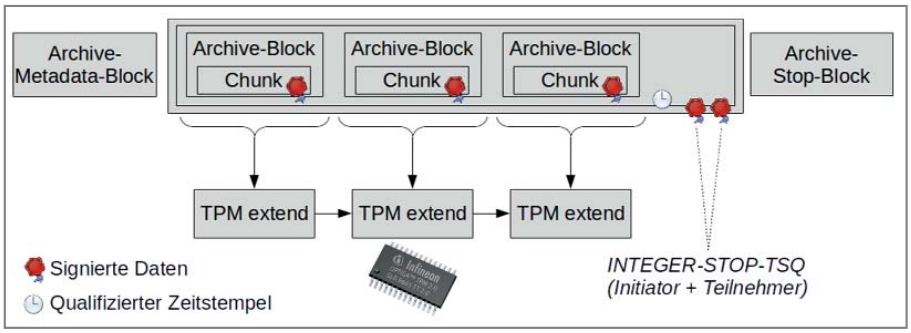

Bild 2: Erzeugung einer Hash-Kette mittels Trusted Platform Module (TPM)

struktur nutzen zu müssen. Der dritte Punkt, die revisionssichere Speicherung der Kommunikationsdaten, erfolgt. Der erste Block enthält die Metadaten, wie z.B. SIP-URL der Teilnehmer, und den Zeitpunkt des Gesprächsbeginns. Danach folgen die Blöcke mit den Gesprächsdaten, wobei jeder Block signiert wird. Ist das Gespräch beendet, wird beim Auflegen ein spezieller Block hinzugefügt, der die Zeit und den Grund des Gesprächsabbruches enthält. Die jeweiligen Kommunikationspartner speichern die gesammelten Pakete zusammen mit der Signatur und können diese Aufzeichnung später vorlegen und somit die Existenz einer Kommunikation zweifelsfrei belegen.

Die VoIP-Kommunikation wird auf der Protokollebene durch das SIP- und RTP-Protokoll umgesetzt. Für die Signierung des Gesprächs ist es hierbei wichtig, dass SIP (Aushandlung der Kommunikationsparameter) und RTP (der Kommunikationsinhalt) erfasst werden. Im Unterschied zu einer konventionellen Signatur wird allerdings ein Dokument signiert, noch bevor es vollständig erstellt ist. Das INTEGER-Projekt setzt daher eine Signatur des Gesprächs im Endgerät um, was der frühestmögliche Zeitpunkt in der Kommunikationskette ist.

Anwendungsszenario

Zwei Geschäftspartner einigen sich auf Bedingungen und Konditionen eines Vertrages über eine VoIP-Telefonverbindung. Das heißt, zu einem bestimmten Zeitpunkt innerhalb dieser Verhandlung wird durch die Geschäftspartner beschlossen, den Vertrag mündlich abzuschließen, um Zeit und Ressourcen zu sparen. Beide Parteien müssen dafür ein zur sicheren Archivierung und Signierung der Gesprächsdaten geeignetes Endgerät (z.B. Softphone) besitzen, das eine PIN-Eingabe ermöglicht, mit der sie den Beginn der Signierung einleiten können. Beiden Seiten wird ab diesem Zeitpunkt signalisiert, z.B. über eine entsprechende Anzeige am Telefon, dass nun die Aufzeichnung beginnt. Der Signier-

prozess wird am Ende der Verhandlung explizit beendet oder abgebrochen, wenn der Hörer aufgelegt wird. Der aufgezeichnete Vertrag wird zur Beweissicherung und Dokumentation durch die beteiligten Gesprächspartner archiviert (z.B. in einem Cloud-Archiv des Anbieters), *Bild 1*.

Im Fall eines Rechtsstreits über die Inhalte oder die Existenz des Vertrags kann diese Aufzeichnung auch vor Gericht verwendet und durch sogenannte Inaugenscheinnahme zur Feststellung beweiserheblicher Tatsachen dienen. Eine Inaugenscheinnahme ist jede sinnliche Wahrnehmung von Beweismitteln, zu der auch akustische Abläufe gehören. Ein technischer Gutachter kann anhand der Aufzeichnung nachweisen, dass die digitale Signatur gültig und in einem unveränderten Zustand ist. Auf dieser Basis können die Existenz und der Inhalt des Vertrags durch ein Gericht zwischen möglicherweise zuvor unbekannten Gesprächspartnern über eine VoIP-Verbindung festgestellt werden.

Der Schutz von Geheimnissen kann durch die Mechanismen des Trusted Computing erreicht werden, wie sie von der Trusted Computing Group (TCG) definiert werden. Das Trusted Platform Module als spezieller Hardwarebaustein kann dabei Schlüssel erzeugen, speichern und ermöglicht die Benutzung der Schlüssel auf sichere Weise (*Bild 2*). Beim Einsatz eines TPM kann vor Gebrauch sichergestellt werden, dass die verwendete Hard- und Software nicht manipuliert wurde bzw. dass eine Manipulation vorher bemerkt wird. Damit eine Manipulation der Daten nachgewiesen bzw. entdeckt werden kann, wird eine Hash-Kette über die ausgetauschten Datenblöcke (Chunk-Paare) gebildet. Diese Kette wird parallel zu dem Prozess der erfolgreichen Signierung erstellt. Hierbei wird auf das TPM nur asynchron zugegriffen, da die Zugriffszeiten auf das TPM keine Echtzeitverarbeitung erlauben. Die Realisierung über ein Softphone ist dabei relativ einfach möglich, da aktuelle Rechnersysteme standardmäßig TPM-Chips besitzen und diese bei Windows 10 inzwischen für die Festplattenverschlüsselung vorausgesetzt werden.

Fazit

Die Möglichkeit, mit der hier vorgestellten Lösung per Telefon verbindlich Verträge abzuschließen, bedeutet eine Unterstützung und Erleichterung für Unternehmen, da sie Ressourcen sparen, schnell und effizient mit einem System rechtsverbindliche Verträge abschließen und Angebote abgeben können. Die Einfachheit der Lösung beim Einsatz für den Anwender, der zum Signieren und Aufzeichnen eines Gesprächs nur eine entsprechende Taste drücken und seine PIN eingeben muss, kann zu einer hohen Akzeptanz bei den Anwendern führen. Eine weitere Verschärfung der Call-Center-Gesetzesrichtlinien, die Vertragsabschlüsse am Telefon ohne Beweiskraft zukünftig untersagen, könnte auch zu einer entsprechenden Verbreitung der INTEGER-Lösung führen. *(bk)*