Telekommunikation, bei der nicht nur Inhalte, sondern auch Metadaten geschützt sind

Hubert A. Jäger · Edmund K. Ernst

Uniscon GmbH – The Web Privacy Company
hubert.jaeger@uniscon.de

Zusammenfassung

Dieser Fachbeitrag beschreibt die Anforderungen, die an Unicast-Kommunikationssysteme gestellt werden, die nicht nur Inhalte, sondern auch Metadaten auf technische Weise schützen sollen. Mit Metadaten sind im Kommunikationskontext Verbindungsdaten gemeint, die aufzeigen, wer mit wem, wann und wie lange kommuniziert. Bislang war dies nur über einen asymmetrisch verschüsselnden Broadcast-and-Select-Ansatz oder mit Mix-Netzen möglich. Um ein Ausspähen von Daten zu verhindern, verlässt sich die Mehrheit der Systeme auf Verschlüsselung, so dass nur die jeweiligen Sender und Empfänger die kommunizierten Daten entschüsseln können. Allerdings benötigen Unicast-Systeme immer noch, dass eine Empfängeradresse an die vermittelnden Einheiten bekanntgegeben wird. Außerdem sind der Zeitpunkt der Übertragung und die Größe der Nachricht für den Netzbetreiber transparent. Solche Metadaten sagen viel über die Absichten der betroffenen Parteien aus und sind einfach zu analysieren. Aus diesem Grund erfordert der Datenverkehr zwischen Bürgern, privaten Unternehmen und öffentlichen Einrichtungen auch den Schutz der Metadaten. Verschlüsselung kann durch eine digitale, elektronische und mechanische Versiegelung der Datenverarbeitunganlagen ergänzt werden. Dabei wird auf technische Weise der Zugang zu Daten verhindert, und zwar auch dann, wenn sie in Klartext verarbeitet werden. Dennoch wären auch in einem solchen System die Mitarbeiter eines Anbieters in der Lage, Metadaten aus den Datenverkehrsvolumina und den Zeitkorrelationen, sowie aus den Fremdschlüsseln der Datenbank des Vermittlungssystems abzuleiten. Um eine betreibersichere, d.h. eine gegen den Betreiber gesicherte Kommunikation über die verschlüsselte und versiegelte Infrastruktur (genannt Sealed Cloud) zu gewährleisten, wird eine Dekorrelation der Daten vorgeschlagen, die in und aus der Sealed Cloud geleitet werden. Des Weiteren wird eine Methode zur Versiegelung von Fremdschlüsseln der Datenbank vorgestellt. Diese Ergebnisse haben nicht nur grundsätzliche Bedeutung, sondern sind für die Praxis relevant. Am Ende des Beitrags ist die Anwendung zum besonders einfachen Aufbau von sicheren Verbindungen zwischen verschiedenen Organisationen gezeigt, die nicht über eine gemeinsame abgesicherte Infrastruktur, wie z.B. ein Intranet, verfügen.

1 Einleitung

Die selbstverständlichste technische Möglichkeit, Kommunikationssysteme vor Spionage oder einer unbefugten Datenanalyse zu schützen, besteht darin, jeglichen Zugang zu den verwendeten Signalen – von der Quelle bis zum Kommunikationsabfluss – zu verhindern. Innerhalb geschlossener technischer Systeme (z.B. Inter- und Intraprozessor-Kommunikation) nimmt man meist an, dass ein unautorisierter Zugang zu jenen Signalen ausgeschlossen ist. Allerdings ist bei Telekommunikationssystemen bzw. einer Kommunikation über größere Entfernungen ei-

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 191-202.

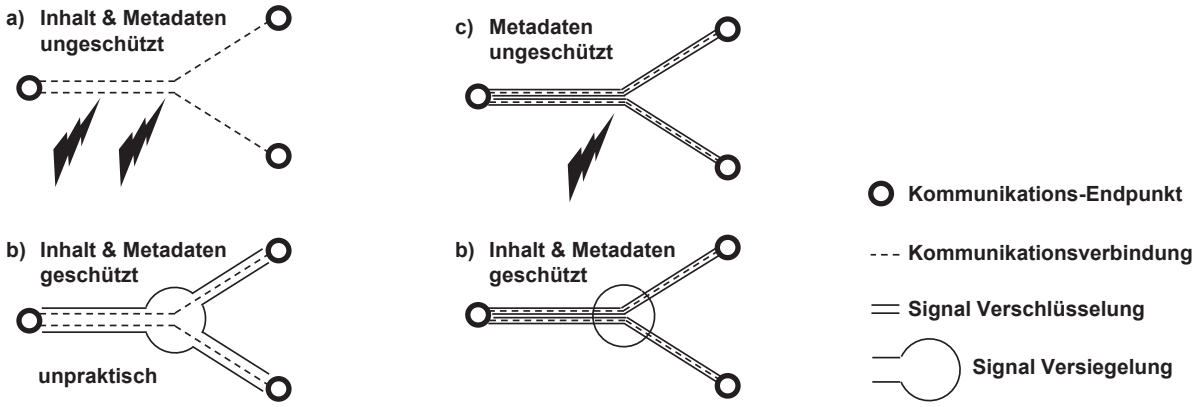

Abb. 1: Verschlüsselungs- und Versiegelungsfälle

ne Versiegelung dieser Signale/Daten kostspielig und daher unökonomisch. (Abbildung 1a): ungeschützte Kommunikation, Abbildung 1b): komplett versiegelte Kommunikation). Deshalb werden bereits seit Beginn der Telekommunikation Daten vor deren Übertragung verschlüsselt [Con07], was seitdem auch stets weiter entwickelt wird [NIS01].

Bei den verschiedenen Verschlüsselungsmethoden wird ein potentieller, nicht vertrauenswürdiger Zugang zu Telekommunikationssignalen toleriert, da das Lösen des jeweiligen Codes so extrem kostspielig wäre, dass man – bei Inhalten – von einer Verletzung des Datenschutzes nicht ausgeht. Dies betrifft die Metadaten jedoch nicht, welche wie in Abbildung 1c) dargestellt weiterhin eingesehen werden können. Diese Eigenschaft hat zu der Idee geführt, die Metadaten von den Mitteilungen in Broadcast- bzw. Multicast-Systemen zu verschleiern [CSWH00].

Asymmetrisch verschlüsselte Daten werden hierbei nicht nur vom Sender an den Empfänger geschickt (wie bei Unicast-Systemen), sondern auch an mehrere Teilnehmer eines Kommunikationsnetzwerkes. Mit entsprechender Auswahl des öffentlichen Schlüssels kann aber nur der Empfänger mit seinem privaten Schlüssel die Nachricht entschlüsseln. Die anderen Empfänger der verschlüsselten Information können daraus nicht den Empfänger ableiten.

Leider ist diese Methode nur für Kommunikationen kleinerer Bandbreite geeignet, da dies dem Netzwerk und dem Empfänger jeweils hohe Übertraguns- und Verarbeitungskapazitäten abverlangt.

Bei Breitband-Unicast-Systemen muss die Information von der Quelle an das Ziel weitergeleitet werden. Metadaten, wie beispielsweise die Empfänger-Adresse, müssen den Weiterleitungseinheiten offenbart werden. Den Zeitpunkt, die Häufigkeit, das Volumen und noch andere Metadaten werden dem Betreiber zwangsläufig mitgeteilt. Die genannten Metadaten werden oft als Konnektivitäts- oder Verbindungsdaten bezeichnet.

Die andauernde politische Debatte, wie die Datenspeicherung verfassungskonform zu gestalten sei, zeigt eindeutig, wie sensibel das Thema für die Gesellschaft ist. Aus technischer Sicht ist klar, dass Metadaten viel über die Absichten, Ursachen und Ziele der Dialogpartner verraten. Diese sind auch relativ einfach zu analysieren: Nehmen wir einen Familienbetrieb als Beispiel. Der Eigentümer und Geschäftsführer erhält einen Anruf von der onkologischen Abteilung eines nahegelegenen Krankenhauses. Zehn Minuten später ruft der Unternehmer seinen Rechtsanwalt an und kurz darauf seinen Sohn. Aus den Metadaten von nur drei Anrufen lässt sich bereits

eine Geschichte konstruieren, die für den direkten Wettbewerber höchst interessant sein könnte [Hae12]. Folglich gilt es, auch diese Daten zu schützen, um die Vertraulichkeit aller Daten einer Mitteilung zu gewährleisten.

Das Fernmeldegeheimnis hat, z.B. in Deutschland [TKG13], jahrzehntelang sensible Daten vor Mißbrauch geschützt. Die Dienstanbieter waren gezwungen, organisatorische Maßnahmen zu ergreifen, die eine Einhaltung von Datenschutzgesetzen gewährleisten sollten. Beispielsweise werden die Personen, die technisch Zugang zu den Metadaten haben, vertraglich zur Geheimhaltung verpflichtet. Im besten Falle werden die Tätigkeiten mit Zugang zu den Metadaten, nach dem Vier-Augen-Prinzip durch mehrere, sich gegenseitig überwachende Personen, gemeinsam ausgeführt (siehe auch ISO/IEC 27001, 27002, 27018, BSI IT-Grundschutz, etc.). Die Datenskandale der letzten Monate zeigen, dass Metadaten mittels organisatorischer Maßnahmen praktisch nicht ausreichend sicher geschützt werden [MDE11]. Noch problematischer: Seit der Einführung des Telemediengesetzes, dessen Aufgabe es ist, Telemediendienste zu regulieren [TMG13], haben viele Dienste mit einem erweiterten Funktionsumfang, die u.a. über Kommunikationsfunktionen verfügen, den im Telemediengesetz beabsichtigten rechtlichen Schutz teilweise oder gänzlich verloren. E-Mail-Dienste werden in vielen Fällen nicht mehr als reine Telekommunikationsdienste eingestuft, sondern teilweise auch als Telemedien-Dienste. Die Nutzer stimmen in den AGBs meist der Analyse von Inhalten und Metadaten zu, ohne zu bedenken, was diese Zustimmung für sie bedeuten könnte. Ferner beweist die Leichtigkeit, mit der massenweise vertrauliche Daten von einer Betreiberfirma exportiert werden können, dass organisatorische Maßnahmen alleine noch lange nicht genügen, um Metadaten vor unbefugtem Zutritt zu schützen [TG13].

Ein weiterer Ansatz verhindert den Zugriff auf die Empfängeradressen gar nicht, sondern verschleiert die Absenderadresse. Dies erfolgt über so genannte Mix-Netze, in denen die Nachrichten von der Senderadresse entkoppelt und an mehreren Zwischenknoten - voneinander unabhängiger Betreiber - mit einer Mehrzahl anderer Nachrichten vermischt werden [Syv97]. Damit kann der Empfänger der Nachricht die Absenderadresse für eine verbindliche Kommunikation aus dem verschlüsselten Teil der Nachricht entnehmen. Einem einzelnen Betreiber der Knoten des Mix-Netzes bleibt dies aber verborgen. Auch dieser Ansatz ist aufgrund der hohen Verzögerungen in einem solchen Netz eher für Schmalband-Anwendungen geeignet. Zudem sind eine Mehrzahl von einander unabhängiger, aber technologisch kooperierender Betreiber nötig.

Das Konzept der Sealed Cloud, das mit dem Kommunikationsdienst IDgard Anwendung findet [IDG14], wurde entwickelt, um die zuvor beschriebenen Datenschutz-Herausforderungen für einen direkt ansteuerbaren Web-Dienst zu lösen ([JMRE13a] und detaillierter [JMRE13b]). In Kapitel 2 wird erklärt, wie mit Sealed Cloud den Mitarbeitern des Betreibers der Zugang zu den Daten - in allen Phasen - technisch verwehrt wird.

Unter normalen Umständen gilt für Anwendungen in der Sealed Cloud, dass der Betreiber nicht direkt erkennen kann, wessen Nachrichten an wen weiter geleitet werden. Wenn er aber den eingehenden und ausgehenden Verkehr genau überwacht, könnte er einen Großteil der Metadaten mithilfe von Zeit- und Volumenbezügen (Korrelation der Daten) ableiten. Aus diesem Grund wird in Kapitel 3 beschrieben, wie die versiegelnde Eigenschaft der Sealed Cloud durch angemessene De-Korrelation der Kommunikationssignale ergänzt werden kann. Aufgrund solcher und weiterer technischer Maßnahmen kann die entsprechende Datenverarbeitung innerhalb der Sealed Cloud stattfinden. Abbildung 1d) zeigt diesen Ansatz der versiegelten Kommunikation.

Schließlich wird in Kapitel 4 die sicherheitstechnische Relevanz anhand von praktischen Szenarien belegt, bevor in Kapitel 5 das Fazit gezogen wird.

2 System-Überblick

In diesem Kapitel wird ein Überblick zum System “Sealed Cloud” vermittelt. Zunächst werden anhand der Abbildung 2 die Bereiche der Cloud-Nutzer (beispielhaft Nutzer A und Nutzer B), des Cloud-Betreibers bzw. Dienstanbieters, des Anwendungs-Entwickler bzw. Software-Erstellers und der externen Auditoren definiert. Die verschiedenen Bereiche sind jeweils mit gestrichelten Linien umrahmt.

In diesen Bereichen sind dann jeweils die wichtigsten Komponenten als Funktionsblöcke dargestellt. Diese werden kurz vorgestellt und dann deren Zusammenspiel in drei Unterkapiteln behandelt.

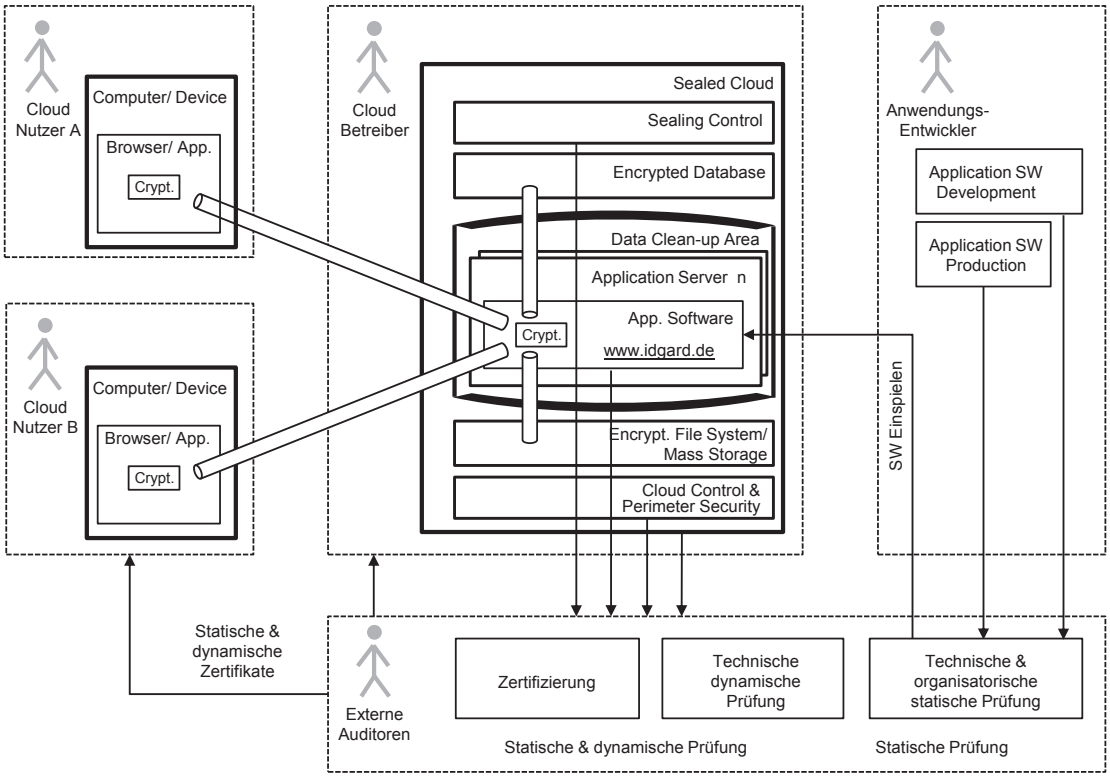

Abb. 2: Sealed Cloud System-Überblick

Die Cloud-Nutzer agieren mit Personal Computern oder anderen elektronischen Geräten, indem sie den gewöhnlichen Browser oder spezielle Applikationen (besonders bei mobilen Geräten wie Smart Phones) nutzen. Diese Anwendungen bauen eine verschlüsselte Verbindung zu den Anwendungs-Servern in der Sealed Cloud auf. Die Komponenten, die notwendig sind, um z.B. den Web-Dienst für sicheren Datenaustausch und Zusammenarbeit IDgard bereitzustellen, sind im innersten Kern – der so genannten “Data Clean-Up Area” – die Anwendungs-Server, darum gruppiert die jeweils redundant ausgeführten Datenbanken und die Server des File-Systems, sowie die Einheiten zur so genannten “Sealing-” und “Cloud-Control”. Der Entwicklung der in der Sealed Cloud zur Anwendung kommenden Software wird nach den besten Praktiken der

Software entwickelt und erst nach Prüfung durch unabhängige Auditoren in die Anwendungs-Server eingespielt. Auch der Betrieb der Software, wie auch der anderen Komponenten der Sealed Cloud werden dynamisch durch externe Auditoren überwacht.

2.1 Sichere Verbindung zur Sealed Cloud

Damit keine besondere Software installiert werden muss, erfolgt die Verbindung vom Gerät des Nutzers aus zum Cloud-Dienst mit klassischer SSL-Verschlüsselung. Allerdings werden nur starke Verschlüsselungssysteme, d.h. solche, mit langen Schlüsseln und ohne bekannte Implementierungsschwächen, akzeptiert. Da – anders als bei gewöhnlicher Web-Servern – keine privaten Schlüssel auf Server-Seite bekannt sein dürfen, kommt ein spezifisches Verfahren zum Einsatz, das – zertifiziert durch externe Auditoren – den Import privater Schlüssel absichert und eine dauerhafte Speicherung ausschließt. Als Schutz gegen 'man-in-the-middle'-Attacken stehen optional eine Browser-Erweiterung und, für Smart Phones und Tablets, Apps zur Verfügung, die bei falschen Zertifikaten sofort den Nutzer alarmieren. Ebenfalls optional, können Nutzer mit einem Einmalpasswort-Generator in Scheckkartenformat oder Verifizierung mit sicherer SIM-Karte einen zweiten Faktor zur Absicherung der Authentisierung verwenden.

2.2 Schutz vor Zugriff auf Daten während der Verarbeitung

Damit nun sowohl der Betreiber der Infrastruktur als auch der Anbieter des Dienstes während der Verarbeitung auf technische Weise gehindert werden, auf die Nutzerdaten zuzugreifen, kommt ergänzend zur Verschlüsselung die im Folgenden beschriebene Versiegelung zum Einsatz. Hierzu sind alle Anwendungsserver des Dienstes, in der so genannten "Data-Clean-Up-Area", in mechanischen Einheiten (Käfigen) untergebracht, die mit speziellen elektromechanischen Schlössern versehen sind. Auch sind alle elektronischen Schnittstellen zu den Servern entweder entfernt oder mit Filtern versehen, die nur den Nutzer-Zugriff gestatten; es ist kein direkter Administrator-Zugang vorgesehen. Keiner dieser Server hat einen persistenten Speicher. Die elektronischen Schnittstellen wie auch die mechanischen Komponenten der Käfige sind mit einer Vielzahl von Sensoren ausgestattet, die unmittelbar einen Alarm auslösen, sobald ein Zugang zu einem der Käfige initiiert wird.

Im Falle einer solchen Alarmierung wird dann der "Data-Clean-Up" ausgelöst. Das heißt, die Sitzungen der Nutzer auf den betroffenen Servern werden automatisch auf nicht betroffene Segmente umgelenkt und sämtliche Daten in den betroffenen Segmenten gelöscht. Zur Absicherung der Löschung wird sogar die Stromversorgung zu den Servern 15 Sekunden lang unterbrochen. Diese Prozedur wird sowohl bei unautorisierten Zugriffen wie auch zur Vorbereitung von Servicearbeiten eingesetzt.

Im Einzelnen können die Einheiten des "Cloud-Control" bzw. sowie des "Perimeter"-Schutzes den Alarm auslösen. Es ist dann die Verantwortung der "Sealing Control" den "Data-Clean-Up" anzustoßen. Bevor ein Segment der "Data-Clean-Up-Area" nach einem Zugriff und dem folgenden "Data-Clean-Up" wieder starten kann, wird eine Überprüfung der gesamten Software durch ein lückenlose "Vertrauenskette" (chain of trust) - ausgehend vom individuellen "Fingerabdruck" des einzelnen Anwendungs-Servers - durchgeführt. Wird hierbei eine Abweichung vom signierten, geprüften Status der Anwendungs-Software festgestellt, kann der entsprechende Anwendungs-Server nicht starten und wird nicht in die Lastverteilung der "Cloud-Control" eingegliedert.

Die Verarbeitung unverschlüsselter Daten findet ausschließlich in den Anwendungs-Servern statt, die über keine persistenten Speichermedien verfügen. Daten, die dauerhaft gespeichert werden müssen, werden entsprechend der im nächsten Unterkapitel behandelten sicheren Speicherung verschlüsselt.

2.3 Sichere Speicherung

Das Prinzip der ”Versiegelung” umfasst des Weiteren eine besondere Schlüsselverteilung, bei der der Betreiber keinen Schlüssel zur Entschlüsselung der Profile in der Datenbank und auch der Dateien in den File-Systemen hat. Konkret werden die Schlüssel für die Profile in der Datenbank durch Hashketten aus Nutzername und Passwort erzeugt. Sobald die Hashwerte ermittelt sind, werden Nutzername und Passwort sofort wieder verworfen. Am Ende der Sitzung wird auch der ermittelte Hashwert gelöscht. Diese beiden Prozeduren sind spezielle Fokus-Punkte im Prüfprogramm der unabhängigen Auditoren.

Eine detaillierte Beschreibung der Versiegelungstechnik zum sicheren Betrieb von zentralen Recheninfrastrukturen ist in [JMRE13a] und [JMRE13b] zu finden. Im Weiteren sei auf die zusätzlichen Maßnahmen Bezug genommen, die notwendig sind, um nicht nur die Inhalte der verarbeiteten Daten vor unbefugtem Zugriff, sondern auch die Metadaten vor dem Betreiber der Sealed Cloud, zu schützen.

3 Versiegelte Dekorrelation

Um die zuvor genannten Sealed Cloud-Eigenschaften ausreichend zu ergänzen, müssen die Zeiten, zu denen Nachrichten in die Sealed Cloud ein- und ausgehen (gemäß Absatz 3.1) sowie die Längen ein- und ausgehender Nachrichten (entsprechend Absatz 3.2), dekorreliert werden.

3.1 Zeit-Dekorrelation

Angenommen wird ein Sealed-Cloud-Knotenpunkt mit eingehendem Datenverkehr, welcher aus Nachrichten und Dateien besteht und diese, wie in Abbildung 3 dargestellt, hochgeladen werden.

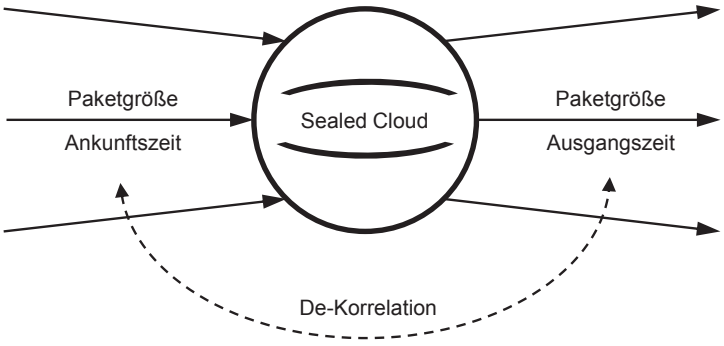

Abb. 3: Ein- und ausgehender Datenverkehr eines Sealed-Cloud-Knotenpunktes

Der eingehende Verkehr kann dem Nutzer lediglich als Online-Speicherbereich dienen, ohne dass eine Kommunikation mit Dritten stattfindet. In diesem Fall ist die Korrelationsthematik unkritisch. Gewöhnlich aber löst der eingehende Verkehr sofort Benachrichtigungen an weitere Sealed-Cloud-Nutzer und den Download von Nachrichten oder Dateien durch diese Nutzer

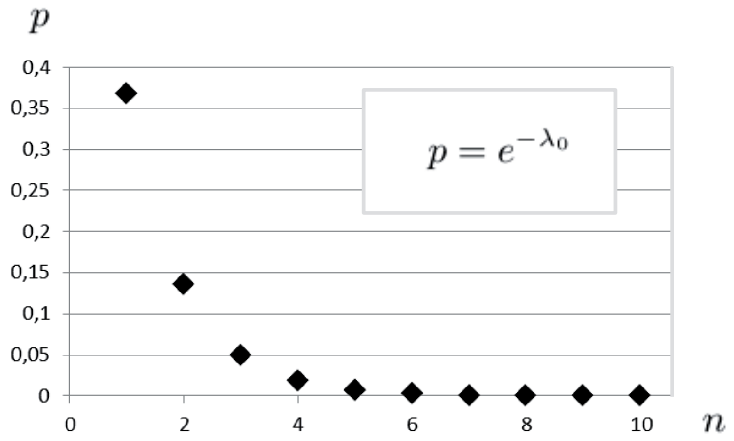

Abb. 4: Wahrscheinlichkeit, keine Antwort vor Eingang der darauffolgenden Nachricht zu erhalten

aus. Die Ankunft von Nachrichten oder Dateien kann durch die folgende Poisson-Verteilung beschrieben werden,

$$P(k) = \frac{e^{-\lambda_a} \lambda_a^k}{k!},$$

wobei λ_a die durchschnittliche Ankunftshäufigkeit der Nachrichten bzw. Dateien beschreibt und jedes p von P die Wahrscheinlichkeit von k Nachrichten bzw. Dateien darstellt, die innerhalb des nächsten Zeitintervalls eingehen. Die vorgeschlagene Strategie besteht darin, die Reaktionen auf eine gesendete Nachricht, also den ausgehenden Verkehr, zu verzögern – und zwar so, dass in der Wahrscheinlichkeitsdichtefunktion mit dem Parameter $\lambda_o = n \cdot \lambda_a$ der Wert für n so gewählt wird, dass die Dekorrelation in notwendigem Ausmaß gewährleistet wird. Die Wahrscheinlichkeit p, keine Antwort auf eine eingehende Nachricht oder einen Datei-Upload innerhalb des Zeitintervalls zu erhalten, ehe die nächste Nachricht bzw. der nächste Datei-Upload eintrifft, ist, sogar für kleine Werte für n, hinreichend niedrig.

Natürlich möchte man die Verzögerungen auf ein Minimum reduzieren. Die aktuelle Ankunftshäufigkeit λ_a wird gemessen und der Verzögerungsdichte-Parameter für den ausgehenden Verkehr λ_o entsprechend gewählt, während n konstant bleibt.

Je höher das Verkehrsvolumen ist, desto kleiner kann die Zeitspanne der Dichtefunktion sein. Um es noch einmal zu betonen: λ_o stellt nur den Parameter der Wahrscheinlichkeitsverteilung der gewählten Verzögerungen und nicht den durchschnittlichen Wert des ausgehenden Verkehrs dar. Die Durchschnittswerte des jeweils eingehenden und ausgehenden Datenverkehrs sind natürlich gleich. Längere Verzögerungen benötigen entsprechend größere Puffer.

Die beschriebenen Verzögerungen können von jeder Sealed-Cloud-Anwendung eingefügt werden, ohne dass dies vom Anbieter nachvollzogen werden kann.

3.2 Dateilängen-Dekorrelation

Entsprechend ist es notwendig, Maßnahmen zu ergreifen, die verhindern, dass Metadaten durch die Korrelation von Volumenmessungen ein- und ausgehender Daten abgeleitet werden können. Wenn die Längen ausgehender und eingehender Nachrichten und Dateien miteinander verglichen werden würden, könnte leicht daraus abgeleitet werden, welche IP-Adresse

mit welcher anderen IP-Adresse gerade kommuniziert. Die einfachste Strategie wäre, alle auftretenden Längen der maximalen Länge s_{max} zuzuordnen. Allerdings wird eine hohe Übertragungskapazität benötigt, um diesen zusätzlichen Datenverkehr übertragen zu können.

Im Gegensatz zu dem oben erwähnten Broadcast-and-Select-Verfahren, gemäß [CSWH00], und dessen Kapazitätsbedarf

$$C_{multicast} = m \cdot \sum_{i=1}^{I} s_i,$$

wobei m die Multiplizität des Multicast-Systems und s_i die individuellen Größen der übertragenen Nachrichten und Dateien beschreiben - ist die benötigte Kapazität für das vorgeschlagene Unicast-System mit

$$C_{unicast1} = \sum_{i=1}^{I} s_{max} = I \cdot s_{max},$$

immer noch deutlich kleiner für hinreichend großes m.

Eine Strategie, die Effizienz der Bandbreite weiter zu erhöhen, ist es, eine Anzahl von I Größenkategorien zu definieren, wobei alle Nachrichten und Dateien in ihrer Größe der oberen Grenze der betreffenden Kategorie angepasst werden. Unter der Annahme, dass eine gleichmäßige Verteilung der Größen über die Kategorien vorliegt, ergibt sich

$$C_{unicast2} = \sum_{q=1}^{l} \sum_{i=\frac{(q-1)I}{l}}^{\frac{qI}{l}} q \cdot \frac{s_{max}}{l} = I \cdot \frac{s_{max}}{l}.$$

Große Netzwerke und ein hoher Verkehr auf den betreffenden Netzen erlauben es, eine große Anzahl von I zu wählen und damit mit dem vorgeschlagenen Unicast-Verfahren zum Metadaten-Schutz einen Vorteil bei der Effizienz der Bandbreite zu erreichen, welcher einer ausreichenden Multiplizität m eines Multicast-Systems genügt.

3.3 Pseudonymisierng von Fremdschlüsseln

Damit schließlich auch aus den Fremdschlüsseln in der Datenbank keine Rückschlüsse auf die Nutzungsstrukturen der Anwendung möglich sind, wird innerhalb der erwähnten Data-Clean-up-Area ein rein volatiler Meta-Mapping-Server betrieben. In diesem kann die Anwendung Datenstrukturen abbilden, ohne dass der Betreiber der Infrastruktur oder der Anbieter der Anwendung Zugriff darauf hätte. Würden diese einen Zugriff versuchen, würde der beschriebene Data-Clean-up automatisch ausgelöst. Da dieser Server jedoch rein volatil betrieben wird, ist für eine hohe Verfügbarkeit erstens eine redundante Gestaltung in einem Cluster notwendig, und müssen zweitens die Datenstrukturen im Falle eines Ausfalls der gesamten Infrastruktur nach und nach durch aktive Nutzersitzungen neu aufgebaut werden können.

4 Anwendung

Die in Kaptitel 2 und 3 vorgestellten Ergebnisse haben nicht nur grundsätzliche Bedeutung für den Schutz der Metadaten, sondern sind für die Praxis insofern relevant, als durch den Ansatz der Sealed Cloud besonders einfach Verbindungen über Organisations- oder Firmengrenzen hinweg aufgebaut werden können. Die herrschende Sicherheitsproblematik ist ja in erster Linie nicht der fehlende Schutz für die Metadaten, obwohl das steigende Verkehrsvolumen die Möglichkeiten verschärft, aus Metadaten auf Teile der kommunizierten Inhalte zurückzuschließen. Die Problematik ist, dass die Mühen zur Einrichtung und Nutzung von sicheren Verbindungen generell gescheut werden. Im Folgenden sind zwei Szenarien geschildert, wie solche Verbindungen einfach aufgebaut und genutzt werden können.

4.1 Einladung von neuen Teilnehmern

In einem Unternehmen oder einer Organisationseinheit besteht die Verpflichtung, sicher zu kommunizieren. Ein Administrator dieser Einheit, in Abbildung 5a) durch das graue Quadrat symbolisiert, registriert sich hierfür bei einem geeigneten Web-Dienst [IDG14]. Dieser Administrator kann nun interne Mitarbeiter, in Abbildung 5 durch gefüllt Kreise gekennzeichnet, oder externe Gäste, leere Kreise, durch folgenden Ablauf zu diesem Dienst einladen: IDgard erzeugt

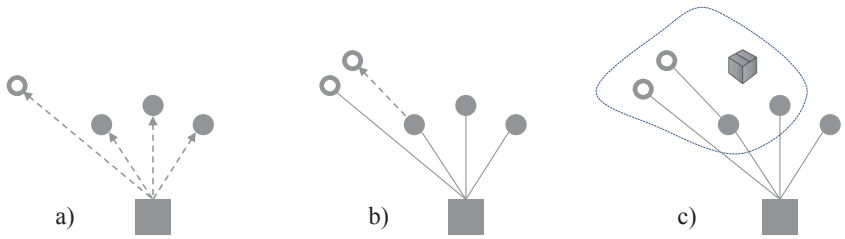

Abb. 5: a) Ein Gast (leerer Kreis) und drei Mitarbeiter (gefüllte Kreise) werden zu einem Netz durch einen Administrator (Quadrat) geladen. b) Auf die gleiche Weise können Mitarbeiter Gäste hinzuladen. c) Ohne Weiteres können die von der gewundenen Linie umfassten Netzteilnehmer in einen Kommunikationskreis (Privacy Box) verbunden werden.

automatisch jeweils einen Einladungslink (URL), der den Mitarbeitern bzw. den Gästen auf potentiell unsicherem Wege (beispielsweise E-Mail) mitgeteilt werden kann. Dieser Einladungs-Link führt zu einem Registrierungsformular, auf dem ein dem Administrator wie auch dem Betreiber des Web-Dienstes nicht einsehbares Passwort gewählt und ein Pass-Code eingegeben werden kann, der auf einem zweiten unabhängigen Kanal (z.B. SMS) übermittelt wurde. Dieser Pass-Code kann auch ein Einmalpasswort eines entsprechenden Generators (Login-Card) sein. Sobald ein Einladungslink genutzt wurde, ist er automatisch obsolet. Selbst wenn diese URL dem Betreiber des Web-Dienstes bekannt wäre, könnten keine Rückschlüsse auf irgendwelche Datenbank-Einträge gezogen werden. Wie in Abbildung 5b) gezeigt, können Mitarbeiter analog auch externe Gäste zum einfachen Aufbau sicherer Verbindungen über Firmengrenzen hinweg einladen. Da jeder Mitarbeiter- und Administrator-Account den Schlüssel des spezifischen Unternehmens bzw. der Organisationseinheit in sich trägt, kann, wie in Abbildung 5c) gezeigt, jeder Mitarbeiter aus den Mitarbeitern und den Gästen in sich geschlossene Kommunikationskreise, so genannte “Privacy Boxes” generieren. In ihnen teilen die Nutzer Dateien und Nachrichten, vereinbaren Termine und können weitere Funktionen des Austausches und der Zusammenarbeit abwickeln. Dafür ist es nicht nötig, Schlüssel oder Identitäten über potentiell

unsichere Medien zu übertragen. Die Schlüsselverteilung erfolgt geschützt und für den Nutzer unsichtbar innerhalb der Sealed Cloud.

4.2 Verbindungsaufbau mit bestehenden Teilnehmern

In Abbildung 6 ist der zweite Fall illustriert: Zwei Nutzer nehmen bereits am sicheren Web-Dienst teil und vernetzen sich miteinander. Die Zugehörigkeit zu zwei unterschiedlichen Unternehmen bzw. Organisationseinheiten ist durch die unterschiedliche Graustufe bzw. Schraffur des den Administrator repräsentierenden Quadrats angedeutet. Der eine Nutzer erzeugt, wie in

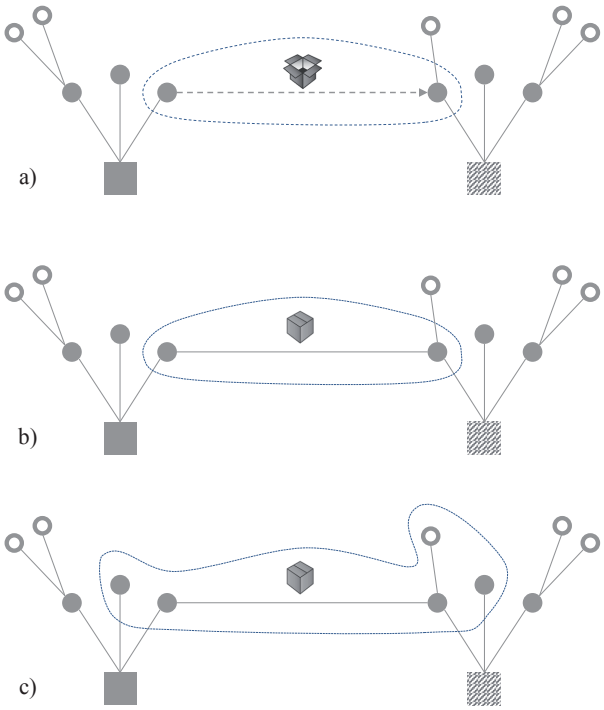

Abb. 6: a) Zwei Nutzer aus unterschiedlichen Unternehmen oder Organisationseinheiten verbinden sich mit einer offenen Privacy Box. b) Diese Privacy Box kann verschlossen bzw. versiegelt werden. c) Weitere Nutzer können von beiden Nutzern dem Kommunikationskreis hinzugefügt werden.

Abbildung 6a) gezeigt, eine neue Privacy Box, und zwar im Zustand “offen”. Dieser Zustand ist dadurch charakterisiert, dass es einen Box Link (URL) gibt, mit dem anderen Nutzern der Zugriff zu dieser Privacy Box vermittelt werden kann. Das kann durchaus über potentiell unsichere Kanäle wie z.B. per E-Mail erfolgen, da die Privacy Box wie in Abbildung 6b) gezeigt, verschlossen bzw. versiegelt werden kann.“ Versiegeln” bedeutet, dass der Box Link unbrauchbar wird, da alle Inhalte der Privacy Box mit einer Schlüsselinfrastruktur, die nur innerhalb der Sealed Cloud verfügbar ist, neu verschlüsselt werden. Während die Privacy Box noch “offen” ist, befindet sich der Verbindungsaufbau in einer vulnerablen Phase. Jeder, der den Box Link mithört, könnte auf die noch offenen Privacy Box zugreifen. Ist jedoch die Identität der während dieser vulnerablen Phase der Privacy Box hinzugetretenen Nutzer geklärt (diese sind aus dem Kommunikationskontext i.d.R. ohne großen Aufwand eindeutig), so endet die vulnerable Phase durch das Schließen der Privacy Box. Um die Anfälligkeit zu verringern, dass ungebetene Nutzer auf die Box und deren Inhalte zugreifen, kann der Zugriffslink (Einladungslink) noch mit einem Passwort abgesichert werden.

Verglichen mit herkömmlich verschlüsselnden Übertragungssystemen ist der Aufbau einer sicheren Verbindung über eine vulnerable Phase anstatt über vulnerable Kanäle deutlich einfacher in der Handhabung.

Schließlich können beide so miteinander verbundene Nutzer durch einfache Auswahl im Web-Dienst, wie in Abbildung 6c) gezeigt, weitere Nutzer aus der einen Organisation in den Kommunikationskreis bzw. die Privacy Box hinzuziehen, ohne dass die Privacy Box hierfür geöffnet werden müsste. Die in der Praxis erforderlichen Prozesse lassen sich deshalb mit den Privacy Boxen so gut abbilden, da der Ersteller einer Privacy Box eines Unternehmens Mitarbeiter eines anderen Unternehmens zu Verwaltern dieser Privacy Box einsetzen kann und daher beide weitere Nutzer ohne explizite Einladung hinzu ziehen können.

Im Ergebnis sind nun innerhalb solcher Privacy Boxes Wege der Kommunikation möglich, von denen, wie in Abbildung 7 gezeigt, auch der Betreiber der Kommunikationsinfrastruktur die Metadaten nicht extrahieren kann. Nutzt man die besten heute verfügbaren Systeme, die

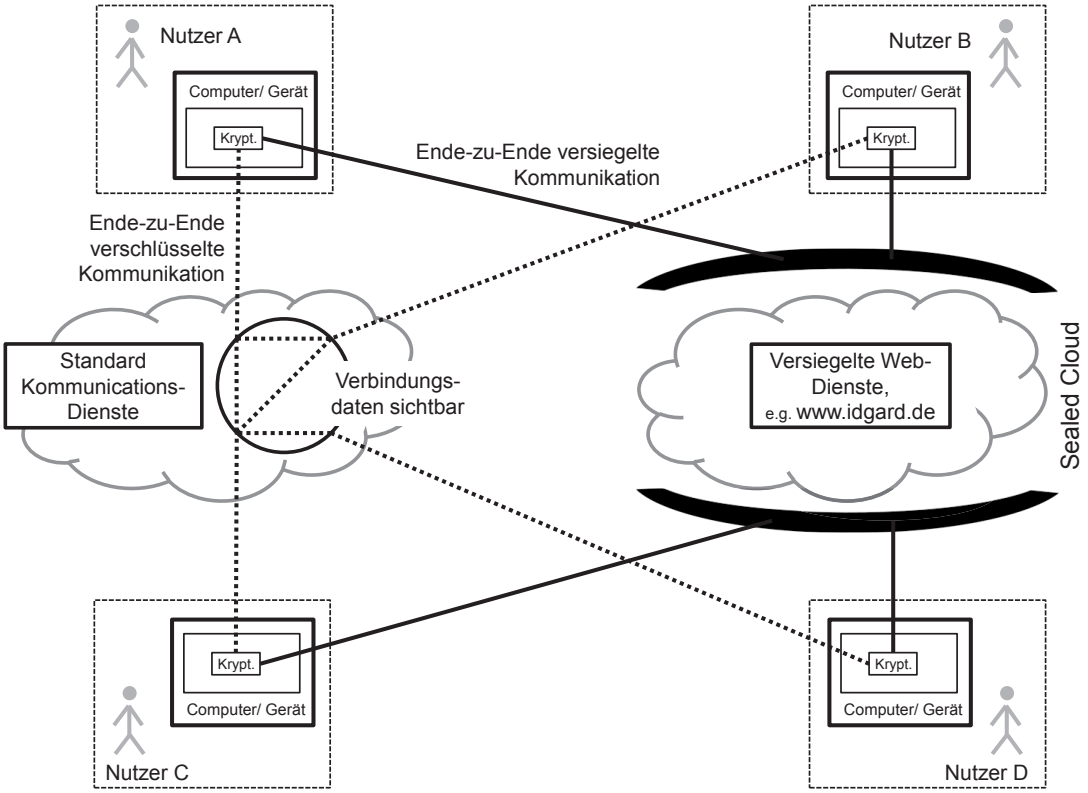

Abb. 7: Metadatenschutz durch die Sealed Cloud

Ende-zu-Ende-Verschlüsselung implementieren, so bleiben doch dem Netzbetreiber, wie im linken Teil der Abbildung 7 gezeigt, die Verbindungsdaten zugänglich. Da das Verkehrsvolumen und die Kommunikationshäufigkeit kontinuierlich steigen, lassen sich aus diesen Daten immer leichter Rückschlüsse auf die eigentlichen Inhalte der Kommunikationen ziehen. Bei der im rechten Teil der Abbildung 7 gezeigten Sealed Cloud kann jedoch der Betreiber nicht mehr unterscheiden, ob z.B. die Nutzer A und Nutzer B nur Daten zum Zweck der Verfügbarkeit auf mehrere Geräte in die Sealed Cloud laden, oder, ob Nutzer A und Nutzer B über die Sealed Cloud miteinander kommunizieren bzw. wie selten oder häufig sie miteinander kommunizieren.

5 Fazit

Metadaten sind vertraulich; sie können sogar Betriebs- oder Berufsgeheimnisse verraten. Sie bedürfen daher geeigneter Schutzmaßnahmen. Unicast-Systeme verfügten bislang über kein Konzept, das solche Metadaten schützt. Das System der Sealed Cloud sichert dagegen die Metadaten vor einer Beobachtung des Betreibers folgendermaßen ab: mit einer speziellen Schlüsselverteilung, einem Data Clean-up und der Dekorrelation der Routing-Eingangs- und -Ausgangszeiten einerseits und der ein- und ausgehenden Datenlängen andererseits. Sogar die Fremdschlüssel in der Datenbank können vor dem Betreiber verborgen werden. Die zusätzlichen Kosten dieser Technologie betragen nur einen Bruchteil der Systemkosten, verglichen mit den Kosten bei Multicast/Broadcast Systemen. Folglich ist eine breite Anwendung der Basistechnologie Sealed Cloud zu erwarten.

Literatur

[Con07] E. Conrad. Explanation of the three types of cryptosystems. *CISSP Papers*, page 1 to 6, 2007.

[CSWH00] I. Clarke, O. Sandberg, B. Wiley, and T.W. Hong. Freenet: A distributed anonymous information storage and retrieval system. *Proceedings International Workshop on Design Issues in Anonymity and Unobservability*, page 46 to 66, 2000.

[Hae12] David Haertzen. *The Analytical Puzzle: Profitable Data Warehousing, Business Intelligence and Analytics*. Technics Publications, LLC, USA, 1st edition, 2012.

[IDG14] www.idgard.de, 2014.

[JMRE13a] Hubert A. Jäger, Arnold Monitzer, Ralf O. G. Rieken, and Edmund Ernst. A novel set of measures against insider attacks – sealed cloud. *Proceedings of Open Identity Summit 2013, Lecture Notes in Informatics*, 223, ISBN 978-3-88579-617-6:185–195, 2013.

[JMRE13b] Hubert A. Jäger, Arnold Monitzer, Ralf O. G. Rieken, and Edmund Ernst. Sealed cloud - a novel approach to safeguard against insider attacks. *Scientific Results of the Trusted Cloud Initiative, http://se.fzi.de/wtc/, to be published as a Springer book*, 2013.

[MDE11] I. Muench, C. Doubrava, and A. Essoh. Eine gefährdungsanalyse von private clouds. *Datenschutz und Datensicherheit DuD, 35*, page 322 to 328, 2011.

[NIS01] NIST: Advanced Encryption Standard (AES). *Federal Information Processing Standards Publication 197*, 2001.

[Syv97] P.F. Syverson et al. Anonymous connections and onion routing. *Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA*, pages 44–54, 1997.

[TG13] J. Taeger and D. Gabel. *Kommentar zum BDSG und den einschlägigen Vorschriften des TMG und TKG in Schriftenreihe Kommunikation & Recht; Band 27, ISBN 978-3-8005-1485-4*. Verlag Recht und Wirtschaft, 2013.

[TKG13] German Telekommunikationsgesetz (TKG), 2013.

[TMG13] German Telemediengesetz (TMG), 2013.