Wie sicher Schweizer E-Mails reisen

E-Mail-Verschlüsselung steigt auf den Prioritätenlisten. Eine Studie der Zürcher Hochschule Winterthur hat die Verbreitung von verschlüsselungsfähigen Mail-Servern untersucht.

Zunehmend wird die herkömmliche Briefpost durch E-Mail ersetzt, welche zu einem unentbehrlichen Hilfsmittel des täglichen Lebens geworden ist. In analoger Weise wie ein Brief mit einer persönlichen Unterschrift versehen wird, um die Authentizität des Absenders zu bekräftigen und anschliessend in einem Couvert verschlossen wird, um den Inhalt vor fremden Augen zu schützen, so existieren bei der elektronischen Post kryptografische Verfahren. Diese erlauben es, die Identität von Sender und Empfänger eindeutig festzustellen, sowie den Inhalt vor unberechtigtem Zugriff durch Dritte zu bewahren.

User-zu-User-E-Mail-Sicherheit durch S/MIME

Der bekannteste Sicherheitsmechanismus ist S/MIME, der eine durchgehende User-zu-User-E-Mail-Sicherheit ermöglicht. Anna (anna@mars.ch) kann beispielsweise eine vertrauliche E-Mail, inklusive allfälliger MIME-Attachments mit einem zufällig gewählten symmetrischen Session-Key verschlüsseln und diesen geheimen Schlüssel verschlüsselt mit dem Public Key von Bruno, zusammen mit der chiffrierten Nachricht an bruno@pluto.ch senden. Da nur Bruno im Besitz des Private Keys ist, der zu seinem Public Key passt, kann er allein den geheimen Session-Schlüssel wieder extrahieren und anschliessend durch symmetrische Entschlüsselung die E-Mail von Anna lesen.

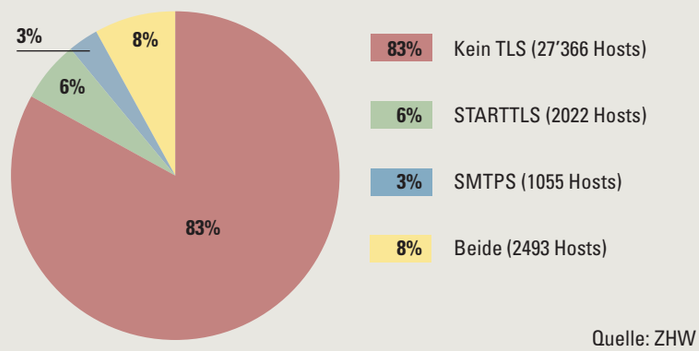
Ein grosse Hürde bei S/MIME ist die Beschaffung des Public Keys des Empfängers (Bruno) durch den Absender (Anna) vor dem Versenden der E-Mail. Ein Public Key ist normalerweise eingebettet in ein X.509-Zertifikat, das durch eine offizielle oder private Certification Authority (CA) herausgegeben wurde. In unserem Beispiel hat die Kool CA das Zertifikat von Bruno generiert und garantiert mit ihrer digitalen Signatur unter das Zertifikat, dass der enthaltene Public Key zur Identität von Bruno und seiner E-Mail-Adresse bruno@pluto.ch gehört. Hat Anna Vertrauen in die Kool CA, dann kann sie Brunos Zertifikat über einen unsicheren Kanal entweder von einem beliebigen Verzeichnisdienst (HTTP oder LDAP Server) oder per E-Mail direkt von Bruno beziehen. Da zur Zeit keine weltweiten Verzeichnisdienste für X.509-User-Zertifikate existieren, ist die S/MIME-Verschlüsselung heute meist auf geschlossene Benutzergruppen beschränkt.

Der unbestrittene Vorteil von S/MIME ist die End-to-End-Verschlüsselung, die garantiert, dass absolut niemand unterwegs die verschlüsselte E-Mail lesen kann. Nachteilig wirkt sich aus, dass jeder Benutzer sein Mail-Tool (Outlook, Mozilla, usw.) durch Laden seines persönlichen Zertifikates und Private Keys erst S/MIME-tauglich machen muss, was für viele Anwender ohne fremde Hilfe nicht zu schaffen ist.

Bei geschäftlicher Korrespondenz kommt noch ein weiterer schwerwiegender Nachteil dazu. Bei Abwesenheit (Urlaub, Unfall, Stellenwechsel, etc.) des E-Mail-Empfängers kann ein Stellvertreter eingehende verschlüsselte Nachrichten nicht ohne Zugriff auf den Private Key des ursprünglichen Adressaten lesen. Entsprechende Key-Recovery-Prozesse müssen deshalb in einer Firma fest etabliert sein, damit in einem Notfall ein Zugriff überhaupt noch möglich ist. Weiter ist es aus rechtlichen Gründen wünschenswert und zunehmend notwendig, dass E-Mails verbindlichen Charakters, mit einem beglaubigten Zeitstempel versehen, über mehrere Jahre hinweg zentral archiviert werden können. Diese Anforderungen können dazu führen, dass eine Firma, um jederzeit den vollen Zugriff auf den geschäftlichen E-Mail-Verkehr zu gewährleisten, eine Mailserver-zu-Mailserver-Sicherheitslösung der Benutzer-zu-Benutzer-Verschlüsselung vorziehen wird.

Anteil der verschlüsselungsfähigen Mailserver

Die Maildienste von 387'000 .ch- und .li-Domains werden auf nur 33'000 Rechnern gehostet. Davon unterstützen 5570 Hosts oder 17 Prozent eine verschlüsselte E-Mail-Übertragung.



Quelle: ZHW

Server-zu-Server-E-Mail-Sicherheit durch SSL/TLS

Mailserver versenden und empfangen E-Mails über das Internet mit Hilfe des standardisierten «Simple Mail Transfer Protokolls» (SMTP). Dabei horcht jeder SMTP-Server ständig auf dem TCP Port 25 auf eingehende Nachrichten, die dann im Normalfall unverschlüsselt als ASCII-Text übermittelt werden. Mit der steigenden Verbreitung des ursprünglich von Netscape entwickelten «Secure Socket Layer»-Protokolls (SSL), sowie des von der IETF standardisierten Nachfolgers «Transport Layer Security» (TLS) in Web-basierten E-Commerce-Applikationen, kam bald der Vorschlag auf, SSL/TLS auch zur Sicherung von SMTP-Verbindungen zu nutzen. Dafür wurde ursprünglich der SMTPS Port 465 vorgesehen, über den direkt eine verschlüsselte SMTP-Verbindung aufgebaut wird, falls der empfangende Mailserver auf diesem Port antwortet. Der SMTPS-Ansatz wurde jedoch rasch durch das STARTTLS-Keyword abgelöst, das vom anfragenden Mailserver gleich zu Beginn über den normalen SMTP Port 25 gesendet werden kann, um zu sondieren, ob der Empfänger SSL/TLS unterstützt. Antwortet der Empfänger mit «220 Ready to start TLS», dann wird eine gesicherte Verbindung aufgebaut. Ansonsten wird die E-Mail wie gehabt im Klartext übertragen.

Wie eine TLS-geschützte SMTP-Verbindung aufgebaut wird, zeigt das folgende Beispiel, bei dem der für die mars.ch-Domäne zuständige Mailserver mail.mars.ch eine Mail an bruno@pluto.ch ausliefern soll. Ein DNS-Lookup gibt als MX-Eintrag für die Domäne pluto.ch den zuständigen Mailserver mail.pluto.ch zurück. Dank des MX-Record-Mechanismus kann eine E-Mail also direkt an den Mailserver des Empfängers verschickt werden. Wird diese Durchquerung des Internets mittels TLS geschützt, ist schon ein grosser Schritt in Richtung Vertraulichkeit der übermittelten Daten getan.

TLS beruht auf einem Client/Server-Prinzip. In unserem Beispiel nimmt der Mailserver mail.mars.ch als Absender die Rol-

le des Clients ein und der Mailserver mail.pluto.ch als Empfänger die Rolle des Servers. Im Rahmen des TLS-Verbindungsaufbaus sendet der Server sein Zertifikat an den Client, damit dieser einen geheimen Session-Key verschlüsselt mit dem im Zertifikat enthaltenen Public Key an den Server zurücksenden kann und damit ein symmetrisch verschlüsselter Kommunikationskanal aufgebaut werden kann. Optional kann der Client aufgefordert werden, sein eigenes Zertifikat zu verwenden, um sich gegenüber dem Server ebenfalls zu authentisieren.

Damit dennoch die gesamte Übertragungsstrecke von Benutzerzu-Benutzer geschützt ist, kann TLS auf einer Hop-to-Hop-Basis verwendet werden. Das Mail-Tool des Absenders Anna benutzt dabei STARTTLS oder SMPTS, um die E-Mail an den eigenen Mailsever mail.mars.ch abzusetzen und der Mail-Browser des Empfängers Bruno kann Annas E-Mail via POPS oder IMAPS zum Lesen vom Mailserver mail.pluto.ch gesichert runterladen.

TLS-fähige Mailserver in den .ch- und .li-Domänen

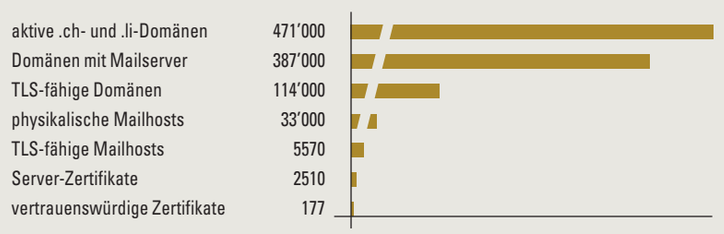
Die Studenten Christian Brauchli und Jakob Furrer, zur Zeit Diplomanden im Studiengang Kommunikation und Informatik der Zürcher Hochschule Winterthur, haben im Juli 2004 im Rahmen einer Projektarbeit ermittelt, wie viele Mailserver in den .ch- und .li-Domänen in der Lage sind, eine gesicherte TLS-Verbindung entgegenzunehmen. Um allfälligen Missverständnissen vorzugreifen: Es ging in keiner Weise darum, Sicherheitslücken in der Konfiguration der Mailserver auszuschnüffeln, sondern das Interesse galt allein der Verbreitung der Zusatzdienstleistung «TLS-Verschlüsselung und Authentifizierung». Sämtliche erfassten Daten wurden anonymisiert, so dass keine Rückschlüsse auf spezifische Domänen getätigt werden können.

Zu Beginn des Projekts wurden die DNS-Einträge von 471'000 aktiven .ch- und .li-Domänen abgefragt, um via MX Records die zuständigen Mailserver zu ermitteln. 76'000 oder 16 Prozent der Domänen besassen keinen MX-Eintrag und wurden deshalb nicht weiter verfolgt, obwohl nicht ausgeschlossen werden kann, dass dennoch ein Mailserver direkt via den registrierten Domainnamen erreicht werden kann. 277'000 Domänen oder 58 Prozent besassen nur einen MX Eintrag, während immerhin 118'000 oder 26 Prozent aller Domänen zwei oder mehr Mailserver vorweisen konnten.

In einem nächsten Schritt wurden die verbleibenden 395'000 Domänen mit mindestens einem MX Record getestet, ob alle eingetragenen Mailserver auch effektiv über den SMTP Port 25 kontaktiert werden konnten. Dieser Test ergab, dass nur bei 8000 oder zwei Prozent der Domänen Probleme auftauchten, in dem auf dem SMTP Port entweder gar keine Antwort erfolgte oder eine Fehlermeldung retourniert wurde. Es wurde festgestellt, dass 276'000 oder 69Prozent über einen einzigen aktiven SMTP-Server verfügen, aber 111'000 oder 29Prozent zwei oder mehr Mailserver besitzen.

Die eigentliche Abklärung der TLS-Fähigkeit wurde mit den 387'000 Domänen vorgenommen, die mindestens einen erreichbaren SMTP-Server besassen. Auf das STARTTLS-Schlüsselwort reagier-

TLS-fähige Mailserver in den .ch- und .li-Domänen



Quelle: ZHW

ten 87'000 oder 23 Prozent der Domänen mit einer positiven «220 Ready to start TLS»-Meldung, während auf dem veralteten SMTPS-Port 465 noch 63'000 oder 17 Prozent der Domänen Antwort gaben. Kombiniert man die beiden TLS-Methoden, so resultieren 114'000 Domänen, die mit mindestens einem Mailserver entweder auf Port 25 oder Port 465 oder beiden ihre TLS-Fähigkeit signalisieren. Dieses doch erstaunliche Resultat kann so interpretiert werden, dass 30Prozent aller aktiven Mail-Domänen eine TLS-Verbindung entgegennehmen und damit E-Mails verschlüsselt ausgetauscht werden können. Ob dies sendeseitig auch der Fall ist, konnte mit dem Test-Setup nicht überprüft werden. Wir vermuten allerdings, dass viele Internet Service Provider aus Performancegründen abgehende E-Mails nicht automatisch verschlüsseln oder deshalb darauf verzichten, um den Forderungen des Fernmeldegesetzes, dass der E-Mail-Verkehr den Strafverfolgungsbehörden zugänglich gemacht werden muss, Genüge zu tun.

Die Studie

Die Resultate der Studie «TLS-fähige Mailserver in den .ch und .li Domänen» werden am 26. Oktober im Rahmen des 3. IT-Security Forums an der Zürcher Hochschule Winterthur vorgestellt. Info: *www.zhwin.ch/aktuell/events/detail/IT-SecurityForum3_04.pdf*

Erfreulicherweise wurden von den 143'000 erfolgreich aufgebauten TLS-Verbindungen nur gerade sechs mit einer ungenügenden 40-Bit-RC4-Verschlüsselung betrieben. Die angefragten Mailserver einigten sich praktisch immer auf die kryptografisch sichere 128-Bit-Variante des RC4-Algorithmus. Erstaunlicherweise wurde SSL mit dreifacher DES-Verschlüsselung und TLS mit dem modernen AES-Algorithmus fast nie gewählt. Es könnte eventuell sein, dass die in unserem Abfrage-Tool verwendete Java-basierte SSL/TLS-Implementation die starken TLS-Methoden nicht an die Spitze der Prioritätsliste gestellt hat. Die tagtägliche Erfahrung des Autors mit einem Open Source Postfix-Mailserver hat nämlich ergeben, dass relativ häufig die äusserst starke AES-Verschlüsselung mit 256-Bit-Schlüssel gewählt wird, wenn die Gegenstelle ebenfalls einen TLS-fähigen Postfix-Server betreibt.

Da zum Aufbau einer TLS-Verbindung ein Server-Zertifikat benötig wird, interessierte uns die Anzahl der eingesetzten Zertifikate sowie deren Eigenschaften. Und hier ergab sich ein höchst überraschendes Resultat: Die 114'000 Domänen mit TLS-Support teilen sich nur gerade 2510 eindeutige Zertifikate. Um diesem Rätsel auf den Grund zu gehen, ermittelten wir in einem nächsten Schritt die Anzahl der physikalischen Mailserver, auf dem die 387'000 Mail-Domänen gehostet werden. Die Auswertung auf der Basis der IP-Adressen ergab, dass dies nur gerade 33'000 Hosts sind. Dabei wurde nicht berücksichtigt, dass einzelne Rechner über mehr als eine IP-Adresse erreicht werden können. Jede IP-Adresse wurde als ein Mailhost gezählt. Die Analyse der TLS-Fähigkeit dieser 33'000 physikalischen Mailhosts ergab, dass 5570 Server oder 17 Prozent entweder STARTTLS, SMTPS oder beide Verbindungsarten unterstützen. Das dabei 2510 unterschiedliche Zertifikate eingesetzt werden war nun wesentlich plausibler. Eine vertiefte Untersuchung ergab aber, dass die Zertifikate höchst ungleich auf die Hosts verteilt sind. Auf der einen Seite sind 2283 oder 91 Prozent aller Zertifikate genau einer IP-Adresse zugeordnet, während im anderen Extrem ein einzelnes Zertifikat auf 807 Mailhosts eingesetzt wird. Dieses Phänomen konnte dadurch erklärt werden, dass zum Beispiel die Plesk-Web-Hosting-Server-Administration-Software, die mit einem Default-Zertifikat ausgeliefert wird, auf mehr als 1400 Mailhosts installiert ist.

Dass 114'000 Domänen mit TLS-Unterstützung aufwarten, kann dadurch erklärt werden, dass einzelne Internet Service Provider bis zu 20'000 Domänen auf einem einzelnen physikalischen Rechner hosten, der dann mit einem einzigen Zertifikat betrieben wird. Da der Mailservername einer gehosteten Domäne meistens die Form mail.domain.ch besitzt, wird er nur in den seltensten Fällen mit dem im Zertifikat aufgeführten Servernamen übereinstimmen, so dass kein Vertrauensverhältnis aufgebaut werden kann. Überhaupt sind 93Prozent aller Zertifikate selbstgestrickt und nur 177 oder sieben Prozent sind von einer offiziellen Certification Authority wie Thawte, Equifax, Comodo, TrustCenter.de, oder Verisign ausgestellt worden.

Zertifikate am Anfang

Die Studie der Zürcher Hochschule Winterthur hat ergeben, dass 30 Prozent aller aktiven Mailserver in den .ch-und .li-Domänen zumindest empfangsseitig eine TLS -Verbindung aufsetzen können und die Stärke der Verschlüsselung durchwegs gut bis sehr gut ist. Möchte man in Anbetracht des täglich zunehmenden SPAM-Volumens auch eine Authentifizierung der Mailserver auf der Basis von Zertifikaten vornehmen, so stehen wir hier erst am Anfang. Nur eine verschwindende Anzahl von Domänen besitzt ein Zertifikat, das erstens von einer vertrauenswürdigen Zertifizierungsstelle herausgegeben wurde und zweitens eine Übereinstimmung des Mailservernamens mit einem entsprechenden Eintrag im Zertifikat besitzt.

Prof. Dr. Andreas Steffen ist Dozent für Sicherheit und Kommunikation an der Zürcher Hochschule Winterthur.