Das Papier wurde vorgestellt auf dem 5. Workshop *Sicherheit in vernetzten Systemen* des DFN-CERT und DFN-PCA, Hamburg, 4.-5. März 1998

Sichere und erweiterte E-Mail für den Einsatz in Verwaltungen[1]

Teil 2 des Beitrages: *"Abgesicherte Internet-Umgebungen mit Hilfe rollenbasierter Zugriffsmechanismen für WWW- und Email-Dienste"*

Thomas Hildmann <hildmann@prz.tu-berlin.de>
Klaus Nagel <klausn@prz.tu-berlin.de>

Technische Universität Berlin

Februar 1998

1.0 Erweiterte Anforderungen an E-Mail-Systeme

Der Internet-Dienst E-Mail ist heute einer der wichtigsten Dienste in der Geschäftswelt. Er verbindet die Vorteile eines digitalen Datentransfers mit den Vorteilen eines klassischen Briefes. E-Mails sind asynchron und passen damit oft besser in Arbeitsabläufe als Telefonate. Spätestens seit Durchsetzung des MIME-Standards [2] haben E-Mails gegenüber der klassischen Post den entscheidenden Vorteil, daß es mit ihnen möglich ist, Daten auszutauschen, die einfach weiterbearbeitet werden können, ohne eine neue Erfassung notwendig zu machen und ohne lange Wartezeiten in Kauf zu nehmen. Das E-Mail-Netz ist heute weit genug gespannt, um in Projekten, bei Bestellungen, Auskünften oder Diskussionen eine beträchtliche Rolle zu spielen. In staatlichen, wie privaten Verwaltungen hat die E-Mail jedoch bislang nur interne Bedeutungen bekommen und das aus gutem Grund.

E-Mails in ihrer heutigen Form sind für den Einsatz in Verwaltungen, und das gilt sicherlich auch für andere Organisationen, nicht geeignet. Daran sind einige Eigenschaften schuld, die E-Mails in ihrer heutigen Form haben.

1. E-Mails sind nicht per se abhörsicher. Personenbezogene Daten dürfen aus diesem Grund nicht per E-Mail versendet werden. Abhilfe schaffen hier zahllose Erweiterungen. Secure E-Mail gehört zum Standardlieferumfang eines guten, zeitgemäßen E-Mail-Systems. Aber auch, wenn die Systeme schon im hohen Maße benutzungsfreundlich geworden sind, sind sie noch weit von dem Optimum entfernt, die Nutzerin oder der Nutzer würde nichts von der sicheren Übertragung mitbekommen.
2. E-Mails sind nicht per se fälschungssicher. Für diesen Punkt gilt praktisch das gleiche, wie für Punkt 1.

1. Die Arbeit entstand teilweise im Rahmen des ESPRIT-Projektes E2S (End-to-End Security over the Internet). Weitere Informationen: http://www.e2s.com

3. Es ist nicht klar, ob eine E-Mail den Empfänger erreicht hat. Über das Header-Feld `Return-Receipt-To:` wird der letzten empfangenden E-Mail-Server in einer Kette angewiesen, eine Empfangsbestätigung zu schicken. Nicht immer ist das ausreichend und zwar genau dann, wenn bei einem Verlust festgestellt werden soll, an welcher Stelle eine Mail abhanden gekommen ist. Auch diese Information sollte nach Möglichkeit abgesichert den Sender erreichen und sollte von seiten des Absenders eine gewisse rechtliche Verbindlichkeit besitzen.
4. Ohne den Besitz der persönlichen E-Mail-Adresse der Empfängerin oder des Empfängers ist der Absender nicht in der Lage, eine E-Mail zu versenden. Bei einem Briefwechsel mit einer Verwaltungseinheit ist jedoch meist nur das Amt bzw. das Stellenzeichen der Sachbearbeiterin oder des Sachbearbeiters bekannt und nicht der Name. Benutzen Personen, die die gleiche Stelle besetzen, einen gemeinsamen Briefkasten, stellt sich die Frage nach der verantwortlichen Person für die Bearbeitung bzw. die gemeinsame Koordination des Briefkastens. Außerdem gibt es für solche gemeinsamen Vorhaben wenig Software, die solche Arbeiten unterstützt. Das tatsächlich parallele Arbeiten auf derselben Mailbox würde ohnehin zu Inkonsistenzen führen; die Arbeit auf Kopien birgt ebenfalls Gefahren. Es sollte sowohl die Möglichkeit einer Sammel-Mailbox als auch eine “private” Mailbox mit Zugang z.B. über ein Stellenzeichen geben.
5. Persönliche E-Mail bleibt im Krankheits- oder Urlaubsfall liegen. Besitzt eine Mitarbeiterin bzw. ein Mitarbeiter eine persönliche Mailbox und ist es ihr oder ihm aus irgendeinem Grund über einen bestimmten Zeitraum nicht möglich, die E-Mails zu bearbeiten, dann muß es einen intelligenten Mechanismus zur Weiterleitung geben. Dabei ist es praktisch nicht möglich, Post, die an die Person selbst und nicht deren Stelle geht, von der Post an die Stelle zu unterscheiden.
6. Wer auch immer ein E-Mail-System einer größeren Abteilung verwaltet, kennt den gewaltigen Aufwand, der betrieben werden muß, um Mailinglisten und Ämter auf dem laufenden zu halten. Läßt man den Arbeitsgruppen eigene Spielräume für ihre Mail-Verwaltung, stoßen diese schnell an die Grenzen ihres Know-Hows und der Verwaltungsaufwand bleibt untragbar hoch. Es sollte also möglich sein, Mailinglisten und Mailrouten von den Benutzerinnen und Benutzern selbst verwalten zu lassen. Dazu muß eine Mailinglistenverwaltung existieren, die einfach genug zu administrieren ist. Hierüber ließen sich auch Probleme wie Stellvertreterschaften lösen.
7. Ein E-Mail-System sollte nach Möglichkeit eine gewisse Unabhängigkeit von Anbietern wahren. Man möchte sich nicht auf einen Lieferanten festlegen und möchte für Neuerungen offen sein.
8. Das beste sichere E-Mail-System nützt nichts, wenn die Geschäftspartner einen anderen Standard benutzen. Das System sollte also in der Lage sein, ggf. auch zwischen verschiedenen Formaten zu konvertieren.
9. Ein verbessertes E-Mail-System muß in der Lage sein, die alten Infrastrukturen zu benutzen, und muß auch in der Lage sein, klassische E-Mails ohne Verschlüsselung und ohne Signatur zu versenden.

2.0 Absicherung der E-Mail Verbindung

Auf die Frage, wie man E-Mails sicher macht, ist heute eine grundsätzliche Antwort gegeben: Public-Key-Verfahren sind die anerkannte Lösung. Dabei wird der öffentliche Schlüssel an alle potentiellen Absender verteilt und der private Schlüssel unter Verschluß gehalten. Mails werden dann mit dem öffentlichen Schlüssel kodiert und ein Hashwert über den Text, der mit dem privaten Schlüssel kodiert ist, stellt sicher, daß die Mitteilung nicht verändert oder ausgetauscht wurde.

Bei diesem Verfahren gibt es grundsätzlich zwei Schwachpunkte:

1. Der öffentliche Schlüssel: Beim Austausch der öffentlichen Schlüssel könnte eine dritte Person die Schlüssel austauschen und eine Man-in-the-Middle-Attacke durchführen. Es muß also sichergestellt sein, daß jeder Absender auch den richtigen öffentlichen Schlüssel besitzt.
2. Der private Schlüssel: Kommt der private Schlüssel erst einmal in die Hand eines Angreifers/einer Angreiferin, liegen ihm/ihr alle Korrespondenzen offen.

2.1 Überblick über bestehende sichere E-Mail-Systeme

Vorreiter in der Diskussion um sichere E-Mail war in letzter Zeit Philip Zimmermann, der Entwickler von PGP (Pretty Good Privacy) [3]. Als eine unabhängige freie und für nahezu jede Plattform erhältliche Software war PGP schnell ein Quasi-Standard für Insider. Leider ist die Benutzung dieser Software zu komplex, um brauchbar zu sein für den täglichen Umgang in Verwaltungen. PGP geht den Weg des Individuums, das nur sich selbst trauen muß und seine Schlüsselverwaltung als aufgeklärter und kompetenter Mensch selbst in die Hand nimmt. Dies ist ein guter und nicht zu ersetzender Ansatz. In der Wirtschaftswelt geht man jedoch nicht so weit, eine Sicherung gegen alle Angriffe (auch evtl. von innen oder von staatlicher Seite) abwehren zu wollen, vielmehr benötigt man für den Abschluß von Verträgen oder bei Auskünften eine rechtsverbindliche Korrespondenz. Anderen Mitarbeitern kann weitestgehend vertraut werden und die Angst vor staatlicher Einmischung sei hier einmal unbeachtet gelassen.

Einen zumindest organisatorisch völlig anderen Weg gehen die großen kommerziellen Hersteller von E-Mail-Tools. Genannt seien hier z.B. Microsofts Outlook-Express oder der Netscape Communicator. Eine vertrauenswürdige Organisation generiert die Schlüssel und stellt diese zur Verfügung. Durch die Signierung/Zertifizierung der öffentlichen Schlüssel von der Organisation ist gewährleistet, daß es sich bei dem vorliegendem Schlüssel um keine Fälschung handelt. Außerdem kann der Schlüssel bei Bedarf aus einer Datenbank abgefragt werden.

2.2 Ein mögliches Alternativmodell

Im Rahmen des E2S-Projektes sind wir einen anderen Weg gegangen. Unser Ziel war, daß eine Verwaltung nicht von einer dritten vertrauenswürdigen Organisation abhängig sein sollte. Eine Unabhängigkeit bietet ggf. finanzielle Vorteile; jedoch nur, wenn die Verwaltung des Sicherheitssystems keinen großen zusätzlichen Personalaufwand bedeutet. Sie bietet aber auch organisatorische Vorteile, wie die Unabhängigkeit bei der Schlüsselverwaltung, der Erteilung/Wegnahme von Zertifikaten und der Umsetzung

einer eigenen Sicherheitspolitik. Bei einer eigenen Schlüsselverwaltung ist das Vertrauen in eine dritte Organisation nicht notwendig.

Um weder das Problem zu haben, daß jeder Benutzer der sicheren E-Mail-Umgebung einen Satz Schlüssel verwalten muß, noch daß Schlüssel über einen sicheren Kanal übertragen werden müssen, entschieden wir uns für eine zentrale Lösung. Jedes Mitglied der sicheren E-Mail-Umgebung kennt genau einen Schlüssel (z.B. einen Firmenschlüssel). Mit diesem Schlüssel wird jede ausgehende Mail verschlüsselt und an den zentralen Server gesendet. Oft besitzen Firmen, oder bei größeren Firmen kleinere Verwaltungseinheiten, ohnehin einen Mail-Server für die Abwicklung der Internet E-Mails. Die Struktur würde hier kaum geändert werden, nur würde der E-Mail-Server um einige Funktionen erweitert werden.

3.0 Erweiterung von Adressen und Mailinglisten

Das von Jörg Bartholdt [4] entwickelte Modell zur Beschreibung von Firmenhierarchien und zur Beschreibung von Rollen und Rechten kann genutzt werden, um dynamische Mailinglisten zu verwalten. Die bereits beschriebenen Probleme der Abhängigkeiten in Firmen, diversen Aliases und sogar Vertretungsangelegenheiten können mithilfe des Access-Control-Modells (ACM) gelöst werden.

3.1 Zusammenspiel von Access-Control-Modell und E-Mail-System

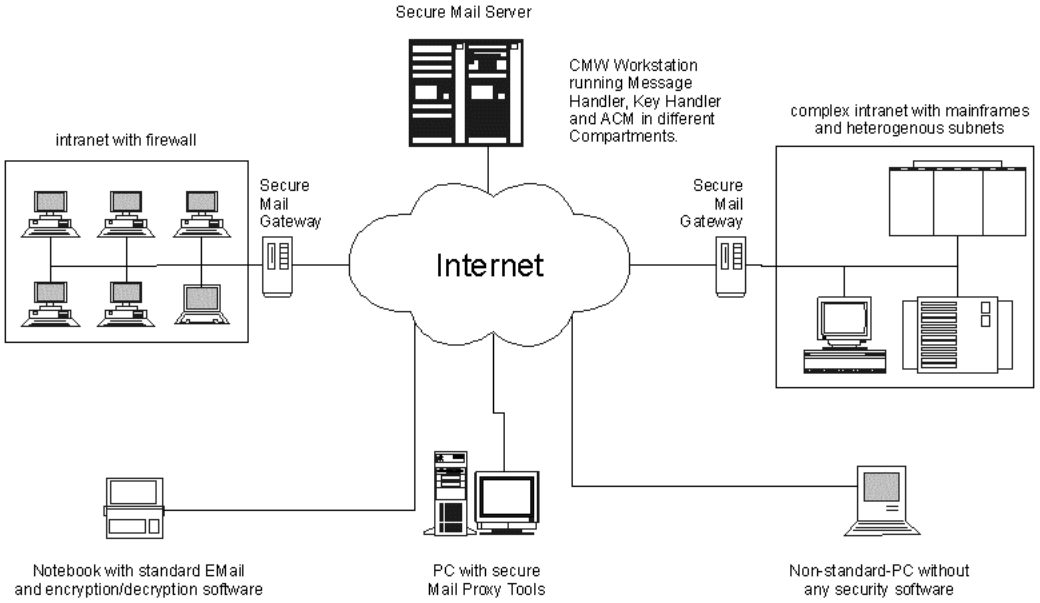
Egal, ob ein Verwaltungsmodell schon wegen der WWW-Nutzung erstellt wurde oder das Modell nur zur Verwaltung der E-Mail-Umgebung genutzt wird, der sichere Mail-Server (SMS) nutzt allein die Informationen über Objektnamen, Mail-Adresse und das Feld für die Schlüsselverwaltung.

Bei der Weiterleitung einer E-Mail wird die virtuelle Empfängeradresse an den ACM Interpreter (ACMI) gesendet. Dieser wird nach einer Auflösung der Adresse gefragt. Mit Hilfe der Informationen über die Mitgliedschaften des besagten Modells (die virtuelle Empfängeradresse entspricht dem Objektnamen im Modell) ist der ACMI in der Lage, die Adressen in physikalische Adressen aufzulösen. Dabei werden Zyklen in Adressauflösungen auf Grund gegenseitiger Referenzierung schon im ACMI vermieden.

Ferner wird zu jeder E-Mail-Adresse auch gleich die Information über den Schlüssel übertragen. Im Fall von PGP reicht hier zur eindeutigen Identifizierung die E-Mail-Adresse aus, da wir aber auch andere Verschlüsselungsverfahren mit anderen Adressierungen, wie z.B. PEM [5] benutzen, war ein erweitertes Feld zwingend erforderlich. Das zentrale System ist also in der Lage, virtuelle Mail-Adressen aufzulösen und zusätzliche Informationen über Schlüssel zu speichern.

4.0 Architektur der erweiterten, sicheren E-Mail-Umgebung

Neben dem zentralen Mail-Server besteht unsere sichere E-Mail-Umgebung noch aus zwei weiteren Komponenten: Einem sicheren E-Mail-Gateway und einer Lösung für Stand-Alone-PCs.



4.1 Sicherer E-Mail-Gateway

Einzelne Abteilungen einer größeren Organisation besitzen in der Regel ein eigenes Netzwerk (LAN). Die Abteilungsnetze sind über Gateways dann mit dem Internet verbunden. Bei einer solchen Konfiguration ist es nicht notwendig, irgendwie in die Konfiguration der Arbeitsstationen einzugreifen. Auf den Gateways, in unserem Fall Linux PCs, wird ein Mail-Server mit einer Secure Mail Gateway (SMG)-Erweiterung eingerichtet. Die Arbeitsstationen senden immer nur an den eigenen SMG. Zum Abfragen der Mails kann der SMG-eigene POP3-Server [6] genutzt werden. Um die Sicherheit des LANs zu gewährleisten, wird auf dem SMG ein Firewall konfiguriert bzw. der SMS wird hinter einer Firewall aufgestellt. Das LAN selbst wird dann als sicher angenommen. Damit ist es unbedenklich, Mails unverschlüsselt über das LAN zu versenden. Der SMG übernimmt die Ver- und Entschlüsselung der nicht-lokalen Mails. Dabei kennt der SMG selbst nur seinen eigenen Abteilungsschlüssel und den der Organisation. Alle ausgehenden Mails werden mit dem Schlüssel der Organisation verschlüsselt und an den SMS gesendet.

Die Mitarbeiter, die hinter einem SMG arbeiten, besitzen keinen eigenen Schlüssel. Ihnen wird im AC-Modell der Schlüssel des SMG zugeordnet. Auch dies ist ein Grund, weshalb es notwendig ist, E-Mail-Adressen von Schlüsselidentifizierern zu trennen.

Technisch gesehen besteht der SMG aus einem Standard-Sendmail/Procmail. Jede ausgehende Mail wird durch einen Procmail-Filter geschickt. Von diesem Filter aus wird die eigentliche SMG-Applikation gestartet. Diese ist recht einfach gestaltet. Die einzige Aufgabe besteht darin zu prüfen, ob es sich evtl. um eine E-Mail handelt, die unverschlüsselt versendet werden soll. Das wird in unserer Prototypkonfiguration durch Voranstellen eines Underline-Zeichens vor der E-Mail-Adresse gekennzeichnet. Im anderem Fall wird das externe Verschlüsselungsprogramm aufzurufen.

Die Signierung der E-Mail im nächten Arbeitsschritt unterscheidet sich etwas von der üblichen Methode. Warum und wie diese Signierung aussieht wird im Kapitel “Vermeidung von Klartext” beschrieben.

Auch für den Empfang von Mails ist im SMG ein Procmail-Script konfiguriert. Hier gibt es nur zwei Möglichkeiten:

1. Es handelt sich um eine verschlüsselte Mail oder
2. es handelt sich um eine Klartext-Mail.

Im ersten Fall wird die Signatur der Mail überprüft (es werden nur E-Mails angenommen, die vom SMS signiert wurden) und die E-Mail entschlüsselt. Es wird dann eine Zeile in der Mail eingefügt, die dem Empfänger anzeigt, daß es sich bei der Mail um eine “sichere Mail” handelt. Dieses Vorgehen verstößt jedoch gegen die Datentransparenz.

Die Mail erreicht die Empfängerin oder den Empfänger nicht in der Form, in der sie abgesendet wurde. Diesem Problem kann auf verschiedene Arten begegnen. Zum einen läßt sich die Sicherheitsinformation mittels Attachment einbringen (somit bleibt der eigentliche Mailtext unberührt), zum anderen ließen sich Sicherheitsinformationen auch in X-Header-Zeilen unterbringen. Letztere Alternative würde jedoch von den Benutzerinnen und Benutzern fordern, die Header zu beachten, was in der Praxis kaum der Fall ist.

Aus diesem Grund ist es ebenfalls möglich, einfach unverschlüsselte Mails gar nicht zuzulassen und sie bei Eingang an den Absender zuzrückzusenden oder zu vernichten oder wahlweise nur mit Klartext-Mails zu arbeiten und alle anderen abzuweisen (das ist für Länder notwendig, in denen das Verschlüsseln von E-Mails untersagt ist). Liegt eine Klartext-Mail vor, so wird diese normalerweise mit einer Meldung versehen, daß diese E-Mail “unsicher” ist. Je nach Konfiguration kann sie auch abgelehnt werden.

Die unverschlüsselten Mails werden dann als Klartext auf dem SMG abgelegt. Wird diese Variante als zu unsicher gesehen, da es sich bei dem POP3-Server gleichzeitig um die Firewall handelt, können Firewall und SMG selbstverständlich auch getrennt werden. Das LAN ist so gegen Angriffe aus dem eignem Netz nicht geschützt. Es wäre möglich, das Netz bei der Übertragung abzuhören, in den SMG einzubrechen, um dort lagernde Mails zu lesen oder zu verändern oder sich einfach fremde Mails per POP3 anzufordern oder mit einem fremden Namen zu versenden.

Dieser Problematik kann man auf zwei Wegen begegnen:

1. Die Mitarbeiter innerhalb einer Abteilung sind als vertrauenswürdig anzusehen, deshalb ist es unnötig, sich vor solchen Attacken zu schützen.
2. Die Relevanz der Daten ist so hoch, daß von einem SMG Abstand genommen wird und nur Stand-Alone-Lösungen installiert werden.

Für den Benutzer hinter einem SMG ist von der sicheren Mail-Umgebung nur so viel zu sehen, daß einkommende E-Mails entweder als “sicher” oder “unsicher” markiert sind und es, je nach Policy, möglich ist, Mails mit vorangestelltem Underline zu versenden oder nicht.

Sicherlich wäre es noch interessant, eine weitere Abstufung zu integrieren, so daß es möglich ist, nicht nur zu verschlüsseln oder mit Klartext zu arbeiten, sondern wahlweise die Abstufungen “signiert/unverschlüsselt”, “signiert/verschlüsselt” oder “unsigniert/unverschlüsselt” auszuwählen.

4.2 Sicherer E-Mail-Server

Der E-Mail-Server (SMS) ist das Kernstück des Systems. Seine Aufgabe ist das Umverschlüsseln der E-Mails. Es müssen jedoch verschiedene Kontrollen durchgeführt werden, da das zentrale System einen perfekten Angriffspunkt darstellt.

Eine mit dem Firmenschlüssel gesicherte Mail wird mit dem Schlüssel des Empfängers verschlüsselt und an diesen weitergesendet. Dabei werden zunächst die virtuellen Adressen mit Hilfe des AC-Modells aufgelöst. Wie beschrieben, soll es möglich sein, auch registrierten Benutzern außerhalb der Organisation E-Mails zu senden.

Hierzu muß der Schlüssel der Person von außen dem Schlüsselverwalter der Organisation zugängig gemacht werden. Dieser kann die Vertraulichkeit dann einstufen und die externe Person als Objekt im AC-Modell eintragen. Der externen Person übergibt der Schlüsselverwalter den Firmenschlüssel. Damit verhält sich aus sich der externen Person jede Mail in die Organisation, wie eine gewöhnliche Secure-Mail. Aus sicht der Organisation ist die Person nun Mitglied der Organisation mit besonderen Gruppenzugehörigkeiten (z.B. Gruppe Extern).

Gelingt es einem Angreifer, innerhalb der Firma oder über eine externe Registrierung irgendeinen eigenen öffentlichen Schlüssel in die sichere Mail-Umgebung zu schleusen, wäre es ihm möglich, jede Mail, statt an einen bestimmten Empfänger an sich selbst zu schicken oder sich selbst Kopien zukommen zu lassen. Jedes zur Zeit übliche E-Mail-System verschlüsselt lediglich den Body einer E-Mail, was kein Problem darstellt, solange jeder seinen eigenen Schlüssel besitzt, den er auch selbst überprüft. In unserem Fall übernimmt aber der SMS eine automatische Umverschlüsselung! Ein Angreifer könnte eine E-Mail abfangen, den Header so umgestalten, daß in der `To:`-Zeile seine eigene virtuelle oder physikalische Adresse auftaucht und diese dann an den SMS leiten. Dieser hätte keine Möglichkeit, die Manipulation zu bemerken. Ein Ausweg aus diesem Dilemma bietet das Unterschreiben der Header-Zeilen. Problem: Eine Änderung des Headers würden die Mails der sicheren E-Mail-Umgebung inkompatibel machen. Aus diesem Grund wie im folgenden näher beschreiben vorgegangen.

Einige Standardzeilen, die fälschungssicher gemacht werden sollen, wie `To:`, `From:`, `Date:` und `Subject:` werden zusammengefaßt und unterschrieben. Eine solche Signierung besteht klassischerweise aus einem mit dem Secret-Key des Absenders unterschriebenen Hash-Wert. Die BASE64-Darstellung dieser Unterschrift wird in einer X-Headerzeile mitgesendet. Beim Empfänger einer solchen E-Mail wird die X-Signature-Zeile wieder extrahiert. Störend bei diesem Vorgehen ist die Tatsache, daß im RFC 822 [7] zwar definiert ist, welche Zeilen eine Internet-Message ausmachen und in welchen Formen sie interpretiert werden können; es ist jedoch nicht gesagt, daß nicht auf dem Weg zum Empfänger die Repräsentation geändert wird. Für den Hash-Wert würde ja schon das Austauschen oder Hinzuführen eines Leerzeichens ausreichen, um die Unterschrift ungültig zu machen. Aus diesem Grund definiert die sichere E-Mail-Umgebung eine Normalform für die o.g. Felder. Vor der Bildung des Hash-

Wertes werden die Zeilen in diese Form überführt. So ist es beim Empfang möglich, erneut diese Form zu erzeugen und über den Hash-Wert zu vergleichen. Dieser läßt sich mit Hilfe des Public-Keys extrahieren und vergleichen. Die Normalform, über die die Signatur gemacht wird, ist z.Z. über einen Algorithmus definiert. Dieser beinhaltet zunächst ein Parsing des Headers und dann eine definierte Ausgabe der gelesenen Tokens.

4.3 Einzelplatzlösung

Nicht alle Arbeitsstationen hängen über ein LAN am Internet. Es sollte also auch eine Möglichkeit geben, diese Stationen mit in die sichere E-Mail-Umgebung eingliedern zu können. Auch gibt es noch andere im vorangegangenen Kapitel beschriebene Bedenken, die Einzelplatzlösungen erfordern würden. Solche Lösungen sollen aber auf keinen Fall benutzungsunfreundlicher als jene über die SMGs sein. Wie, so war unsere Fragestellung, ist es möglich, auch bei einer Einzelplatzlösung den Mail-Client unverändert zu lassen und trotz allem den Benutzer Mails völlig transparent, aber sicher senden und empfangen zu lassen.

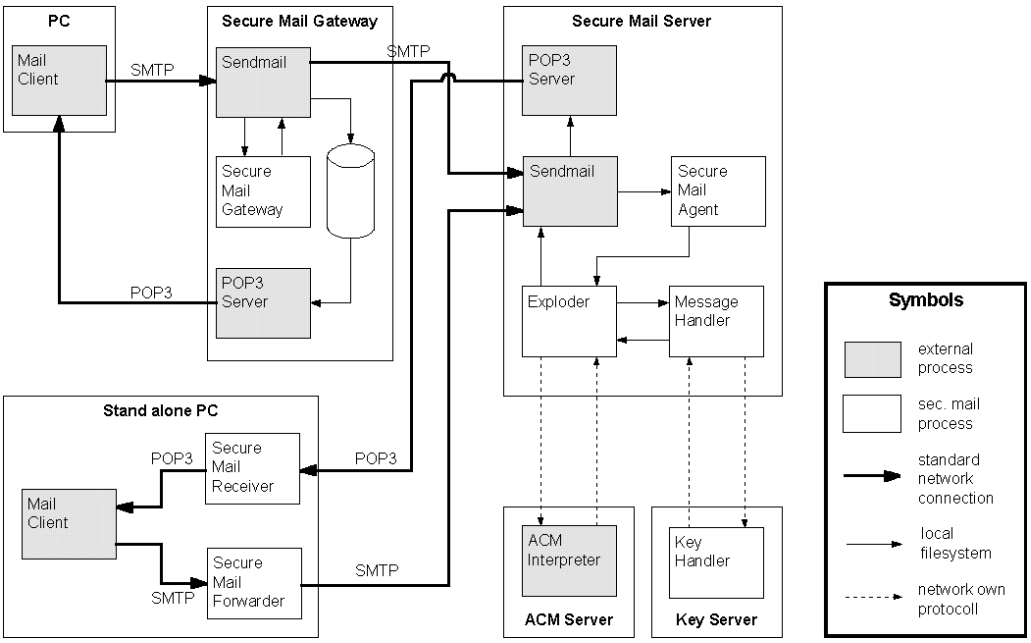
Die Lösung besteht aus einem E-Mail-Filter. Wir müssen ein Programm zwischen Mail-Client und Mail-Server schalten, das die Aufgaben des SMG übernimmt. Ein solcher Filter muß zum einen für das Senden und zum andern für das Empfangen von E-Mails existieren. Wir nennen diese Programme Secure E-Mail Proxy-Tools.

Diese Programme verhalten sich in Richtung Client genau wie die Server und aus Richtung der Server wie die Clients. Bei der E-Mail-Konfiguration wird als Mail-Server bzw. POP3-Server die Localhost-Adresse angegeben. In den Proxies sind dann die echten Adressen. Die Proxies selbst erhalten eine Schnittstelle zu den vom SMS verwendeten Verschlüsselungswerkzeugen. Beim Absenden oder Empfangen übernimmt das Proxy-Tool die Überprüfung, Verschlüsselung oder Entschlüsselung. Wichtig zu erwähnen ist die Tatsache, daß die Proxies selbstverständlich nur Client-Verbindungen vom lokalen Rechner aus annehmen.

Aus Sicht des SMS ist das Senden von einem Gateway und einem Stand-Alone PC mit den Proxy Tools nicht mehr zu unterscheiden. Anders ist dies jedoch beim Empfangen. Bei den Gateways sieht die Lösung vor, die verschlüsselten Mails an den Mailer der Gateways mit deren Public-Key verschlüsselt zu versenden. Im Falle eines Proxy Tools wird die Mail jedoch über POP3 gefordert. Aus diesem Grund müssen diese Mails auf dem SMS selbst verschlüsselt in einer Mailbox liegen, wo diese abgeholt werden können.

Liegen die Mails verschlüsselt auf dem SMS, kann kein Nutzen aus dem unverschlüsselten und unauthentifizierten Protokoll POP3 gezogen werden. Es ist einem Angreifer zwar möglich Mails abzurufen, ohne den Privaten Schlüssel des Empfängers sind sie jedoch nutzlos. Die bestehende Gefahr ist hier jedoch, relativ einfach Mails zu löschen, indem ein Angreifer das Password der POP3-Verbindung abhört und Löschbefehle sendet.

In unseren Prototypen wird gegen diese Gefahr nicht vorgegangen. Abhilfe könnte hier ein modifizierter POP3-Server oder evtl. eine IMAP-Implementierung [8] bringen.



4.4 Der Einsatz von Smartcards

Vor allem bei Einzelplätzen stellt sich die Frage nach der Sicherheit der privaten Schlüssel. Die SMGs kann man als relativ sicher ansehen. Aber auch hier kann ein höheres Sicherheitsniveau gefordert sein. Aus diesem Grund stellt die E-Mail-Umgebung auch die Unterstützung von Smartcards zur Verfügung.

Üblicherweise wird bei einer Textverschlüsselung über einen Session-Key verschlüsselt und dieser Session-Key dann über den Public-Key des Empfängers. Dieser letzte Schritt kann von der Smartcard ausgeführt werden.

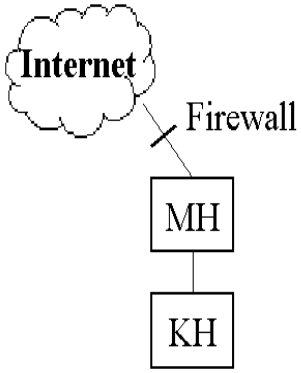
Die Schlüssel der Smartcards können nicht ausgelesen werden; aus diesem Grund bietet sich die Verwendung bei Einzelplatzlösungen an. Aber auch beim SMG kann eine Smartcard zur Ver- und Entschlüsselung eingesetzt werden. Auch wenn der Einsatz einer Smartcard im SMS denkbar wäre, wäre eine solche Lösung viel zu langsam und zu unflexibel.

5.0 Vermeidung von Klartext

Es ist durchaus möglich, E-Mails im SMS umzuverschlüsseln, ohne dabei Klartext auf dem Weg zu erzeugen, es also unmöglich zu machen, die E-Mail selbst bei der Umverschlüsselung zu lesen. Dieses Konzept wurde von Michael Herfert [1] im Rahmen des E2S-Projektes entwickelt. Dieses Prinzip nutzt die Tatsache aus, daß bei der verschlüsselten Mail nicht alles mit dem Public-Key des Empfängers verschlüsselt wird, sondern nur ein Session-Key, über den die eigentliche Verschlüsselung stattfindet. Also ist es durchaus möglich, den verschlüsselten Session-Key, von der E-Mail zu entfernen und an einer anderen Stelle nur den Session-Key zu entschlüsseln und mit einem neuen Public-Key zu verschlüsseln.

5.1 Key-Handler

Architektonisch wurde deshalb im SMS die Trennung zwischen Message-Handler und Key-Handler gemacht. Der Message-Handler stellt die eigentliche Schnittstelle zwischen der Außenwelt und der Software im SMS da. Der Key-Handler wird vom Message-Handler benutzt, um die Mails umzuverschlüsseln und um z.B. Signaturen zu prüfen. Der Message-Handler kennt also nicht den Privat-Key der Organisation. Dieser ist nur dem Key-Handler bekannt. Die verschlüsselte E-Mail verläßt den Message-Handler nicht. Läuft der Key-Handler nun auf einem anderen Rechner als der Message-Handler, ist es organisatorisch machbar, ein Lesen der E-Mail zu verhindern. Gibt es nämlich unterschiedliche Administratoren auf beiden Maschinen, müßten diese schon eine kriminelle Vereinigung schließen, um gemeinsam an den Klartext der E-Mail zu kommen, da jede Maschine ja nur einen unbrauchbaren Teil davon hat.



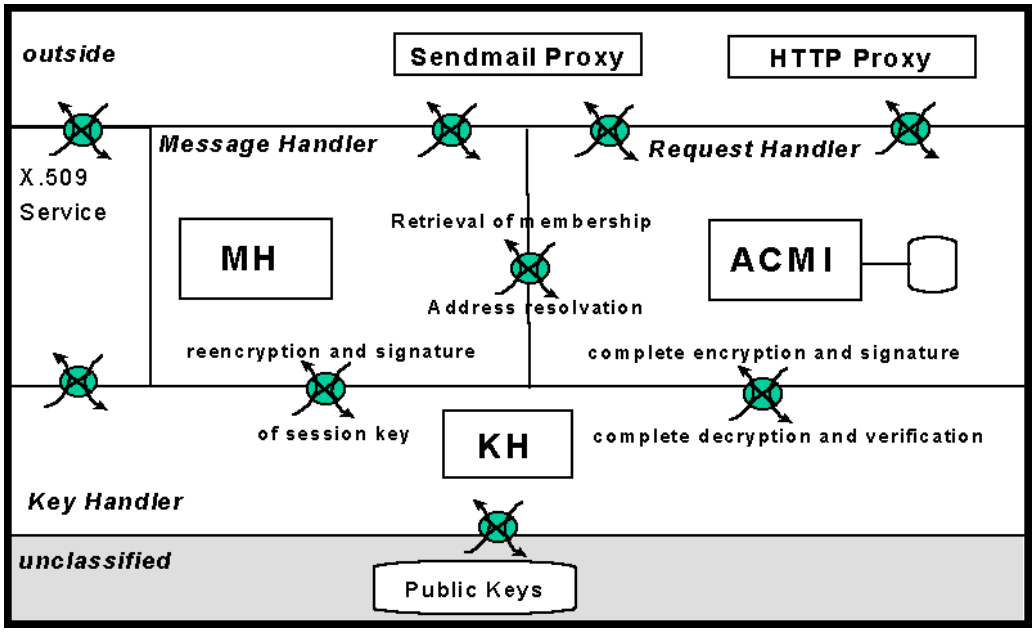
Dem Administrator des Key-Handler wäre ein Entschlüsseln der Mails selbstverständlich möglich, wenn er die eingehenden E-Mails auf dem Weg zum Message-Handler abfängt und selbst entschlüsselt (er selbst ist im Besitz des Firmen-Private-Keys).

Eine Lösung wäre hier nur mit organisatoren Mitteln möglich. Sitzt der Key-Handler in einem gesonderten privatem Netz hinter dem Message-Handler und wird dem Administrator jeder Datenaustausch mit der Internetwelt von diesem Platz aus gesperrt und sind ferner das mitnehmen von Datenträgern verboten. Kann selbst der Administrator des Key-Handlers eine Mail nie mit den Schlüsseln in Verbindung bringen.

5.2 Einsatz compartment-basierter Betriebssysteme

Einfacher wird hier der Einsatz compartment-basierter Betriebssysteme. Im E2S-Projekt wurde hier mit HPs CMW [...] experimentiert. So ist es hier möglich, die Trennung auf einer Maschine zu realisieren; denn unter CMW läßt sich der Superuser löschen und ein Administrator für lediglich ein Compartment der Maschine definieren. So reicht es hier aus, ein Compartment für den Key-Handler und ein Compartment für den Message-Handler zu definieren.

Man kann aber auch noch weitergehen und den Sendmail-Prozeß als einzigen im sogenannten Outer-Compartment starten. Das Outer-Compartment stellt die Schnittstelle zur Netzwelt zur Verfügung. Gibt es noch irgendwelche Sicherheitslücken, die irgendwann im Sendmail aufgedeckt werden, so wäre es theoretisch nur möglich, in das Outer-Compartment einzubrechen. Die Schnittstellen zu den anderen Compartments sind winzige, überschaubare Programme, die ein weiteres Einbrechen in andere Compartments fast unmöglich machen sollten.

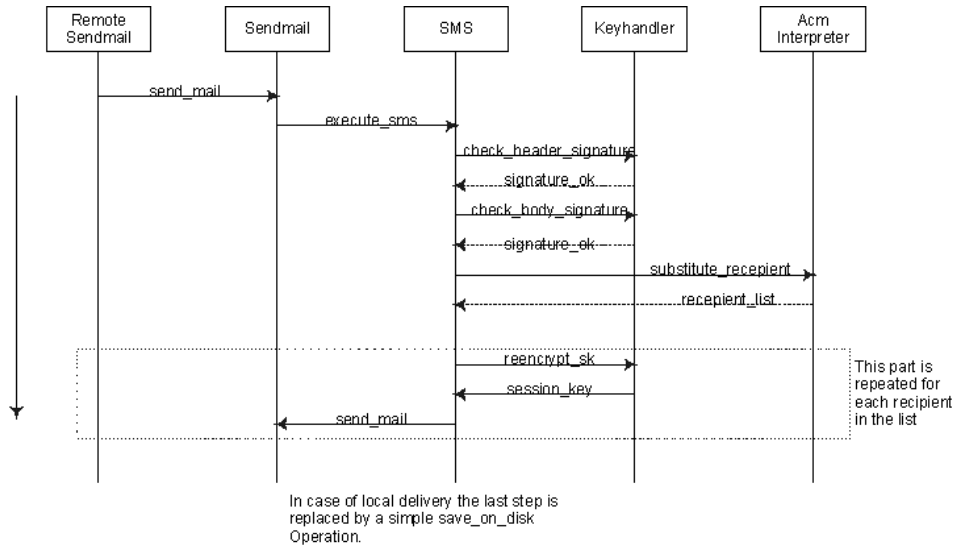


5.3 Erst verschlüsselt, dann signiert

Mit der Signatur einer Mail wird in diesem Konzept folgendermaßen umgegangen:

Eine abzusendende E-Mail wird entweder im SMG oder den Proxy-Programmen zunächst mit dem Organisations-Schlüssel verschlüsselt und dann mit dem eigenem Schlüssel unterschrieben.

Diese Unterschrift wird im SMS geprüft; anschließend findet die Umverschlüsselung der Mail statt. Durch diese Umverschlüsselung geht die digitale Unterschrift des Absenders verloren, stattdessen wird die umverschlüsselte Mail erneut unterschrieben, diesmal mit dem Private-Key des SMS.



Auf gleiche Art und Weise wird auch mit den E-Mails von außen verfahren. Da die SMGs und Stand-Alone Arbeitsplätze keine Schlüssel zum Vergleich besitzen, muß eine Überprüfung vom SMS durchgeführt werden. Nach erfolgreicher Überprüfung entfernt der SMS die Unterschrift und unterschreibt selbst. Die Sicherheitseinstufungen muß der Experte des Key-Handlers vornehmen.

6.0 Einbindung in bestehende sichere E-Mail-Netze

Wie beschrieben, muß es irgendeine Lösung geben, die sichere E-Mail-Umgebung auch in bestehende Systeme einzugliedern. Im Fall von PGP und PEM ist dies einfach. Anstelle des privaten Schlüssels eines Mitarbeiters wird der Schlüssel der Organisation bekanntgegeben und verteilt. Der Security-Experte der Firma kann selbst die Verwaltung der Public-Keys Dritter verwalten. Im Modell des SMS wird ein externer Mail-Empfänger genau wie ein interner behandelt. Dieses gilt das nur insoweit, wie es um Standardverschlüsselung geht. So wird z.B. ein externer Mailer wird sicherlich keine Signatur über den Header machen. Aus diesem Grund werden externe Mails mit einem gewissen Vorbehalten weitergeleitet. Dies macht sich durch eine Meldung an den Mail-Empfänger bemerkbar.

Schwierig wird die Einbindung in eine komplexere Public-Key-Infrastruktur in der auch andere Zertifizierungsstellen agieren. Technisch gesehen bräuchte die Organisation nur einen Schlüssel, der z.B. von der höchsten Stelle der Organisation beantragt wird.

Wie bereits beschrieben könnten dann alle Empfänger, die bei dieser Zertifizierungsstelle ihren Schlüssel besitzen über das SMS aufgenommen werden, in dem beispielsweise ihr Schlüssel bei der Zertifizierungsstelle angefordert und wie ein lokaler Public-Key behandelt wird. Es können dann jedoch nur Personen angeschrieben werden, die im AC-Modell verzeichnet sind. Von der Zertifizierungsstelle müßten dann jeweils nur die höchste Stelle der Organisation verwaltet werden. Die Frage ist doch, wie einzelne Personen der Organisation so adressiert werden können, da aus sicht der Zertifizierungsstelle nur eine E-Mail Adresse sichtbar ist.

Rechtlich gesehen ist ein solches Vorgehen jedoch nicht zulässig oder müßte zumindest mit den Zertifizierungsstellen abgesprochen werden. Zumindest ist jedoch sichergestellt, daß der SMS auf solche Einbindungen vorbereitet ist. Mit zusätzlichen, externen Modulen ließen sich Gateways zu praktisch beliebigen Zertifizierungen und Verschlüsselungen erstellen. Da nur der SMS dazu in der Lage sein muß, bleibt der Umstellungs und Wartungsaufwand sehr gering.

7.0 Hierarchien von sicheren Mail-Umgebungen

Zentralistische Systeme haben immer klassische, durch den zentralen Server gesetzte Limits und Probleme. Dazu gehört die Ausfallsicherheit, Geschwindigkeitsprobleme und evtl. auch der Flaschenhals des zuleitenden Netzwerkes.

Diese Probleme relativieren sich beim SMS ein wenig. Denn beim E-Mail Dienst handelt es sich um einen asynchronen, also nicht zeitkritischen Dienst. Aber auch hier gibt

es Grenzen von Antwortzeiten. Ab einer gewissen Anzahl gleichzeitig zu bearbeitender Mails bekommen die Mail-Clients Timeouts.

Aus diesem Grund kann es durchaus sinnvoll sein, den SMS selbst im Netz zu betreiben, dabei wird jeweils ein Teil der Organisation von einem SMS übernommen. Zu diesem Zweck muß dann bei der jetzigen Implementierung jeder SMS ein eigenes Teilmodell (AC-Modell) der Firma halten. Jede Teilorganisation wird dann als eigene sichere E-Mail-Umgebung angesehen.

8.0 Aussichten

Ein problematisierter, aber in unserer prototypischen Entwicklung noch nicht berücksichtigter Faktor ist die Unabstreitbarkeit des Empfangs einer E-Mail. Hier sieht die geplante Lösung vor, weitere X-Header-Zeilen dazu zu benutzen, um Anfragen nach Rückscheinen zu übertragen. Die Proxy Tools oder Gateways können dann den Empfang bestätigen, wobei eine Bestätigung lediglich den Empfang durch den Client-Rechner bestätigen kann. Ob es einem Benutzer dann möglich ist, die Mail auch zu lesen, kann nicht sichergestellt werden.

Ein weiterer ausstehender Punkt in der Forschungsarbeit ist die Integration von Workflowprozessen in die sichere E-Mail-Umgebung. Zum einen werden heute schon in vielen Organisationen E-Mails zur Aufgabenverwaltung benutzt, zum anderen besteht die Notwendigkeit, so etwas wie ein Mehraugenprinzip einzuführen. Damit meint man Vorgänge, bei denen Dokumente zunächst von verschiedenen Personen eingesehen und bearbeitet werden müssen, bevor eine Aktion ausgeführt werden kann. Meist muß dann sichergestellt werden (i.d.R. durch Unterschriften), daß jeder Teilschritt von einer autorisierten Person erledigt wurde.

9.0 Zusammenfassung

Im E2S-Projekt ist es gelungen, den Prototypen eines Mail-Systems zu entwerfen, das

- für die Benutzer völlig transparent sichere Mail zur Verfügung stellt,
- sich in bestehende sichere Mail-Systeme einbinden läßt,
- dynamische und von Benutzern selbst änderbare Mailinglisten beinhaltet,
- völlig unabhängig von Herstellern der Rechner und Mail-Programmen ist,
- eine eigene Key-Verwaltung zuläßt, die jedoch nicht von den Endnutzern verwaltet werden muß,
- Smartcards integriert
- und das bereits als sicheres Gesamtkonzept mit mehreren Alternativen entworfen ist.

Dabei reichen die Komponenten von Einzelplätzen mit E-Mail Proxy Tools über einen Secure Mail Gateway, der LANs ans Internet anschließt und dabei absichert, bis hin zum Secure Mail-Server, der als einfacher Server, aber auch als Cluster von Servern oder einer CMW-Maschine denkbar ist.

10.0 Literaturangabe

[1] M. Herfert: Security Enhanced Mailing Lists, IEEE Network and Internet Security Vol. 11 No 3, p. 30-33, May/June 1997

[2] N. Freed und N. Borenstain, Multipurpose Internet Mail Extensions (MIME), RFC 2045 - 2049, 1996

[3] P. Zimmermann, PGP Pretty Good Privace, Deutsche Übersetzung Abel Deuring und Christopher Creuzig, FoeBud e.V. Bielefeld, 1990-1994

[4] J. Bartholdt und K. Nagel, Smart Card gesicherte Web-Umgebung und rollenbasierte Zugriffskontrolle im administrativen Bereich, Proposal 5. Workshop DFN-Cert, 1998

[5] J. Linn et. al, Privacy Enhancment for Internet Electronic Mail, RFC 1421-1424, 1993

[6] J. Myers und M. Rose, Post Office Protocol - Version 3, RFC 1939, 1996

[7] D. Crocher, Standard for the format ARPA Internet text messages, RFC 822, 1982

[8] M. Crispin, Internet Message Access Protocoll - Version 4rev1, RFC 2060, University of Washington, 1996