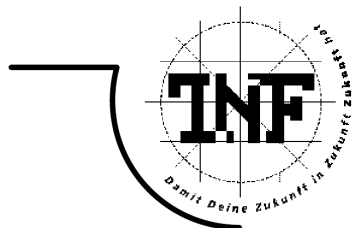




JOHANNES KEPLER  
UNIVERSITÄT LINZ

Netzwerk für Forschung, Lehre und Praxis



## E-Mail

Sicherheit in Applikationsprotokollen

LVA-Nummer: 353.016, WS 2011/12

Angefertigt am *Institut für Informationsverarbeitung und Mikroprozessortechnik*

Kursleiter:

*Dr. Peter René Dietmüller*

Eingereicht von:

*Ludwig Koller, 0655517*

Linz, November 2011

## **Inhaltsverzeichnis**

1	Einleitung.....	1
2	Geschichtliches.....	1
3	SMTP.....	1
3.1	Grundsätzliches.....	1
3.2	Ablauf.....	2
3.3	Folgerungen zur Sicherheit.....	4
4	POP3.....	5
4.1	Grundsätzliches.....	5
4.2	Ablauf.....	5
4.3	Folgerungen zur Sicherheit.....	7
5	Zusammenfassung.....	8
6	Quellen.....	9

## **1 Einleitung**

E-Mail ist mittlerweile wohl eines der meist genutzten Medien zur Kommunikation. Diese Behauptung scheint alleine durch die schiere Masse von E-Mails, die tagtäglich versendet werden, belegt zu sein - alleine 2010 wurden 107 Billionen E-Mails [1] versendet! Ob das sichtlich große Vertrauen der Menschheit in diese Technologie gerechtfertigt oder etwa sogar leichtsinnig ist soll in diesem Paper untersucht werden.

## **2 Geschichtliches**

Der Versand von E-Mails war eine der ersten Anwendungen des Advanced Research Projects Agency Networks - besser bekannt als ARPANET [2]. Es handelte sich dabei um ein Projekt verschiedener amerikanischer Hochschulen und dem amerikanischen Verteidigungsministerium. Das Ziel des Projekts war die Schaffung eines dezentralen Netzwerks für die US-Luftwaffe [3]. Der Versand von Textnachrichten war keinesfalls Ziel des Projekts, vielmehr etablierte sich diese Technologie durch das Verhalten der BenutzerInnen. Der Ursprung des heutigen E-Mails war damals ein Programm namens SNDMSG, mittels welchem Textnachrichten an eine bestehende Mailbox anderer BenutzerInnen am selben Computer angehängt werden konnten. Dieses Programm wurde von Ray Tomlinson mit CPYNET so verknüpft, dass diese Nachrichten über das Netzwerk auch an andere Computer versendet werden konnten. Zeitgleich wurden auch andere Mailbox-Systeme für andere Netzwerkformen entwickelt wie z.B. X.25, Novell oder BTX. Durch den Durchbruch des heutigen Internets konnten sich diese allerdings nicht durchsetzen. Die erste Internet-E-Mail nach Deutschland wurde am 2. August 1984 versendet und kam einen Tag später bei Michael Rotert an. Nur sieben Jahre später wurde die erste E-Mail aus dem All von einem Mac Portable versendet [4]. Mittlerweile hat sich der Versand bzw. der Empfang von E-Mails mittels SMTP und POP3 oder IMAP etabliert [2]. Dieses Paper beschränkt sich aber auf SMTP und POP3 - die beiden meistgenutzten Protokolle.

## **3 SMTP**

### **3.1 Grundsätzliches**

Das Simple Mail Transfer Protokoll dient zum Austausch von E-Mails in Computernetzen. Die Hauptanwendungen des Protokolls sind damit der Versand und die Weiterleitung von E-Mails im

Internet. SMTP wurde im RFC 821 [5] das erste Mal beschrieben. Der mittlerweile gültige RFC für SMTP oder extended SMTP ist der RFC 5321 [6]. SMTP basiert auf ASCII-Codierung und kann damit nur Text übertragen. Um dieses Problem zu umgehen und SMTP auch für andere Schriften oder Formate nutzbar zu machen wird der Kodierstandard MIME verwendet. Für SMTP sind die Ports 25, 465 und 587 reserviert [7]. Ein SMTP-Server ist keinesfalls nur das Endziel der Nachricht, sondern jeder Mailserver der auf dem Weg dorthin liegt. Abbildung 1 zeigt, wie mittels SMTP E-Mails in das Internet versendet werden.

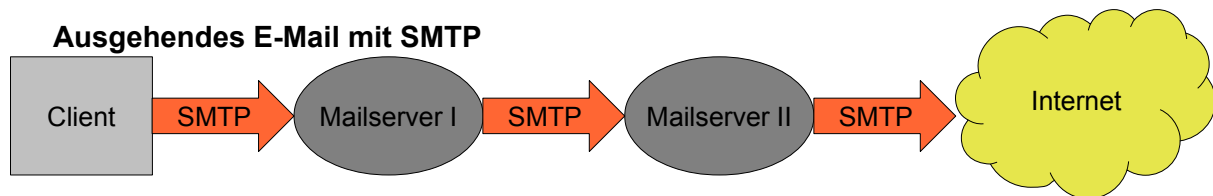


Abbildung 1: Einsatz von SMTP [8]

### 3.2 Ablauf

Der grobe Ablauf einer SMTP-Session im RFC 821 besteht aus vier Schritten: Der Server lauscht auf einem der o.g. Ports auf eingehende Verbindungen. Der Sender initiiert eine bidirektionale Verbindung zum Server. Sobald vom Server eine Erfolgsmeldung wie z.B. "220 Service ready" empfangen wird lautet der erste Befehl des Senders "MAIL <SP> FROM:<Pfad> [SP <Parameter>] <CRLF>" wobei der Pfad die Mailbox und der Server des Senders sind, SP ein Leerzeichen und das Ende jedes SMTP-Befehls mit einem Carriage Return und einem Linefeed abgeschlossen wird. Sollte der Server diesen Befehl akzeptieren antwortet er mit "250 OK". Andernfalls sendet er eine Antwort mit genauerer Beschreibung des Fehlers. Bei Erfolg setzt der Sender mit "RCPT <SP> TO:<Pfad> <CRLF>" fort - er gibt also den ersten Empfänger der Nachricht an. Pfad ist hier abermals eine Mailbox, allerdings ergänzt mit den nötigen Hosts auf dem Weg zum Empfänger. Der Server antwortet hier wieder entsprechend woraufhin der Sender für jeden anderen Empfänger diesen Befehl wiederholt. Danach werden die Daten nach Senden des Befehls "DATA" und Antwort des Servers übertragen. Die Daten werden mit einem einfachen Punkt in einer eigenen Zeile beendet. Dies bestätigt der Server wieder mit einer entsprechenden Antwort und beendet die Verbindung zum Sender. [5]

In den RFCs 5321, 2821, 1869 und 974 wurde das Protokoll erweitert und wird nun oft ESMTP, also erweitertes SMTP genannt. Die großen Änderungen sind die Einführung des HELO- bzw. EHLO- und eines QUIT-Befehls. Beim HELO Befehl teilt der Sender dem Server mit wer er ist, beim EHLO (extended HELO) erfragt er gleichzeitig vom Server eine Liste der erweiterten Funktionen des Servers. Falls vom Server EHLO nicht unterstützt wird von den meisten Clients automatisch HELO als Fallback verwendet. Weiters bestehen E-Mails nicht mehr nur aus Daten sondern werden getrennt in Envelope und Content. Der Envelope ist nur der Umschlag der Nachricht, also die Ursprungs- und die Empfängeradressen. Der Content besteht aus Header und Body, wobei letzterer meist mit MIME codiert ist. Außerdem wird die Sitzung nun nicht mehr einfach beendet nach Bestätigung des Erhalts der Daten vom Server sondern erst nach dem QUIT-Befehl und positiver Antwort vom Server [6].

Abbildung 2 zeigt den typischen Ablauf einer SMTP-Sitzung. Die erste Zeile ist die Ausführung des TELNET-Programms mit welchem Informationen zwischen Server und Client im Textformat übertragen werden können.

Wie man sieht erfolgt keine Authentifizierung beim Versand der Nachricht - wie soll hier also der Sender nachvollzogen werden? Außerdem können in Header und MAIL FROM meist unterschiedliche und beliebige Mailadressen angegeben werden.

Client	Server
telnet mail.example.com 25	
	220 service ready
HELO foobar.example.net	
	250 OK
MAIL FROM:<info@example.org>	
	250 OK
RCPT TO:<info@example.com>	
	250 OK
DATA	
	354 start mail input
From: <info@example.org> To: <info@example.com> Subject: Testmail Date: Thu, 26 Oct 2006 13:10:50 +0200  Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed eiusmod tempor incididunt ut labore et dolore magna aliqua. .	
	250 OK
QUIT	
	221 closing channel

Abbildung 2: Beispiel einer SMTP-Sitzung [7]

### **3.3 Folgerungen zur Sicherheit**

In Hinblick auf Integrität sei nochmals erwähnt, dass bei SMTP keinerlei Authentifizierung nötig ist und die Absenderadresse meist völlig beliebig gewählt werden kann. Dies kann höchstens durch entsprechende Konfiguration des Mailservers, also Verwendung der Erweiterungen AUTH oder STARTTLS, umgangen werden. Dies garantiert aber nicht, dass auch andere Server, von denen man im Normalfall ebenso Nachrichten empfangen möchte, derartig konfiguriert sind. So kann auch ein fremder Server E-Mail mit Absenderadressen des eigenen Servers versenden. Spoofing ist also bei E-Mails sehr einfach. Dazu kommt, dass die Nachrichten und Daten im Klartext übertragen werden. Es kann also jeder Host auf dem Weg zum Empfänger die Daten beliebig verändern oder zumindest mitlesen, wodurch nicht nur die Integrität sondern auch die Vertraulichkeit verletzt ist. Verschlüsselung der Verbindung zwischen Sender und Server scheint die Vertraulichkeit zu garantieren, was aber nicht zwingend der Fall ist, da die Nachrichten auf dem Server trotzdem im Klartext gespeichert und verarbeitet werden. Außerdem bedeutet die Verschlüsselung zwischen Client und Server nicht, dass auch die Verbindungen zwischen den folgenden Servern sicher sind. Die einzige Möglichkeit Integrität und Vertraulichkeit sicherzustellen ist damit der Einsatz anderer Methoden wie zum Beispiel asymmetrische Verschlüsselung mit Pretty Good Privacy (PGP) oder S/MIME.

SMTP wurde zu einer Zeit entwickelt, in der Sicherheit im Internet noch keine Rolle spielte, da es nur sehr wenige Hosts gab und kein so großes Interesse wie heute an einer Vermarktung von Daten bestand. Außerdem wurde E-Mail anfangs nur zum Austausch kleiner Textnachrichten zwischen bekannten Personen verwendet, ganz im Gegensatz zur heutigen Zeit, wo selbst förmliche Briefe und Bewerbungen per E-Mail versendet werden. Der damalige Grundgedanke war - wie im ersten Absatz der Einleitung des RFC 5321 steht: "The objective of the Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently" - Nachrichten zuverlässig und effektiv zu übertragen und nicht durch aufwändige Verschlüsselung oder Authentifizierungsmechanismen den Versand von Nachrichten unnötig zu verkomplizieren.

## 4 POP3

### 4.1 Grundsätzliches

Das Post Office Protokoll (POP) wurde 1984 entwickelt. Das aktuell gültige POP3 ist die dritte Version dieses Protokolls und ist im RFC 1939 definiert. Grundsätzlich macht POP nichts anderes, als Nachrichten von der Mailbox auf dem Server in die Mailbox am Client zu übertragen und ist damit das Gegenstück zu SMTP wie sich in Abbildung 3 gut erkennen lässt. Die Nachrichten werden mit SMTP vom Email Client X zum Mail Server X übertragen. Jener sendet die Nachrichten über das Internet zum Mail Server Y, von wo sie der Email Client Y mit POP3 abholt. Um die Nachrichten dem Client zuordnen zu können ist es nötig, sich vor Erhalt der Nachrichten zu authentifizieren. Für POP3 sind die Ports 110 und 995 reserviert [11].

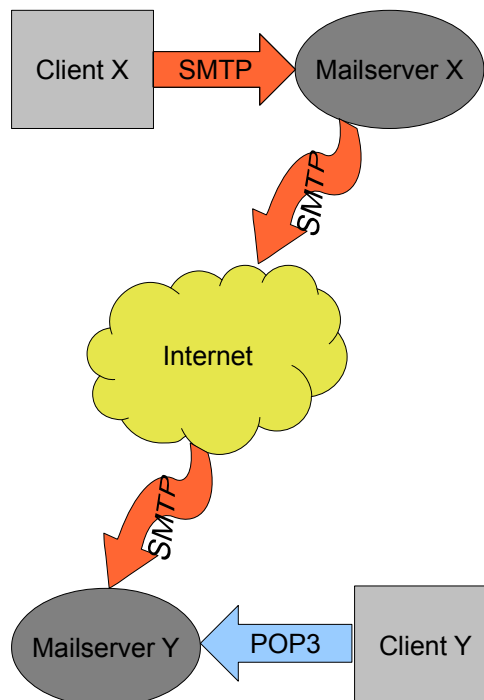


Abbildung 3: Zusammenspiel von SMTP und POP3 [9]

### 4.2 Ablauf

Abermals wartet der Server auf eingehende Verbindungen auf den Ports für POP3. Der Client initiiert eine TCP-Verbindung zum Server woraufhin der Server eine Begrüßung sendet. Anschließend werden Befehle und Nachrichten ausgetauscht, bis die Verbindung mit QUIT vom

Client beendet wird. Der Client authentifiziert sich nach der Begrüßung mit den Befehlen USER und PASS bzw. mit APOP. Die ersten beiden Befehle übertragen Benutzername und Passwort im Klartext zum Server, bei APOP wird nur der Name im Klartext gesendet, das Passwort wird gemeinsam mit einem Zeitstempel, den der Server bei der Begrüßung mitgesendet hat, gehasht um zumindest dieses nicht im Klartext übermitteln zu müssen. Nach einer erfolgreichen Authentifizierung sperrt der Server die Mailbox des Clients, im Falle eines Mailfiles wird dieses in einzelne Nachrichten zerlegt, indiziert die Nachrichten, berechnet deren Größe und setzt den lastRetrieved-Index auf den Index der Nachricht, die als letztes vom Client abgeholt wurde. Nun startet der Transaktions-Modus. Hier sind folgende grundsätzlichen Befehle verfügbar:

- STAT: Info über die Anzahl von Nachrichten und die gesamte Größe
- LIST: Anzeigen der Größe der einzelnen Nachrichten
- LAST: Index der zuletzt abgeholten Nachricht
- RETR x: Abruf der Nachricht mit dem Index x
- DELE x: Markieren der Nachricht x als gelöscht
- RSET: Zurücksetzen des lastRetrieved-Index und der gelöscht-Markierungen

Als letzter Teil der Sitzung bleibt der Update-Modus. Dieser enthält nur den Befehl QUIT welcher den Server veranlasst die als gelöscht markierten Nachrichten tatsächlich zu löschen und die Sperrung der Mailbox aufzuheben. Abschließend antwortet der Server auf den Befehl mit "-ERR" oder "+OK", wobei eine erstere Meldung vom Client getrennt behandelt werden sollte.

Es gibt außerdem für POP3 noch weitere optionale Befehle, die keinen Einfluss auf die Sicherheit haben und deshalb hier nicht behandelt werden [10, 11].

Ein Beispielablauf einer POP3-Sitzung ist in Abbildung 4 zu sehen. Die Authentifizierung erfolgt hier mit den Befehlen USER und PASS, da der Server bei der Begrüßung keinen Zeitstempel mitgesendet hat. Nach der erfolgreichen Authentifizierung wird mit STAT eine Übersicht über die Mailbox abgerufen, anschließend mit LIST die Auflistung der Nachrichten und deren Größe. Testweise wird daraufhin Nachricht 2 gelöscht. Ein neuerliches LIST zeigt, dass diese nicht mehr verfügbar ist. Ein RSET gefolgt von einem weiteren LIST führt dazu, dass die Nachricht wieder zum Abruf bereit ist. Die Sitzung wird zuletzt mit QUIT beendet.

```
+OK POP server ready H migmx101
user [REDACTED]
+OK password required for user [REDACTED]
pass [REDACTED]
+OK mailbox [REDACTED] has 2 messages (170454 octets) H migmx101
stat
+OK 2 170454
list
+OK
1 87294
2 83160
.
dele 2
+OK
list
+OK
1 87294
.
rset
+OK maildrop has 2 messages (170454 octets)
list
+OK
1 87294
2 83160
.
quit
+OK POP server signing off
```

Abbildung 4: Beispiel einer POP3-Sitzung

### 4.3 Folgerungen zur Sicherheit

Da POP3 im Gegensatz zu SMTP nur Nachrichten vom Server zum Client überträgt aber keine neuen Nachrichten erzeugt ist hier der Gedanke der Integrität zu vernachlässigen. Die Vertraulichkeit ist aber natürlich auch Sache von POP, da die E-Mails nur an den tatsächlich gewollten Empfänger zugestellt werden sollen. Aus diesem Grund ist für POP3 Authentifizierung nötig. Die traditionelle Art der Verifikation des Clients mittels Benutzername und Passwort welche im Klartext übertragen werden, ist für die Vertraulichkeit eventuell ausreichend, allerdings nur solange niemand diese beiden Komponenten erfährt - dies ist ein Problem bei allen Authentifizierungsmechanismen. POP3 bemüht sich die Sicherheit des Passworts zu erhöhen indem der Befehl APOP verwendet wird. All diese Verfahren garantieren aber keine Vertraulichkeit, da die Nachrichten selbst im Klartext übermittelt werden, solange keine sichere Verbindung verwendet wird. POP3 über eine sichere Verbindung zu verwenden ist hingegen durchaus eine Möglichkeit die Vertraulichkeit zwischen Server und Client zu gewährleisten.

## **5 Zusammenfassung**

Bei einer genaueren Betrachtung von SMTP und POP3 wird klar, dass E-Mail an sich kein sicheres Medium ist. Es eignet sich hervorragend schnell und unkompliziert Nachrichten und, bis zu einer gewissen Menge, Daten auszutauschen. Es sollte sich aber jedeR BenutzerIn bewusst sein, dass es keine Gewissheit gibt, dass die gesendeten E-Mails unverändert ausschließlich bei den gewünschten Empfängern ankommen oder die empfangenen E-Mails tatsächlich so von der angegebenen Person versendet wurden und unterwegs von niemand mitgelesen werden konnten.

Da E-Mails immer mit SMTP versendet oder übertragen werden und auf den Servern selbst im Klartext verarbeitet und gespeichert werden kann selbst ein noch so sicheres POP oder IMAP keine vollständige Sicherheit vom Sender bis zum Empfänger bieten. Die einzige Möglichkeit diese derzeit zu gewährleisten ist die Verwendung anderer End-To-End Methoden wie beispielsweise PGP oder S/MIME.

## 6 Quellen

- [1] Internet 2010 in numbers: <http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/>
- [2] Wikipedia: E-Mail: <http://de.wikipedia.org/wiki/E-Mail>
- [3] Wikipedia: Arpanet: <http://de.wikipedia.org/wiki/Arpanet>
- [4] erstes E-Mail aus dem All: <http://www.computinghistory.org.uk/det/6115/First%20E-mail%20From%20Space%20Is%20Sent%20from%20a%20Mac%20Portable>
- [5] SMTP - Request for comments: <http://tools.ietf.org/html/rfc821>
- [6] ESMTP - Request for comments: <http://tools.ietf.org/html/rfc5321>
- [7] Wikipedia SMTP: <http://de.wikipedia.org/wiki/SMTP>
- [8] Grafik - SMTP: Zeichnung von L. Koller
- [9] Grafik - SMTP und POP3: Zeichnung von L. Koller
- [10] POP3 - Request for comments: <http://tools.ietf.org/html/rfc1939>
- [11] Guidelines on Electronic Mail Security von M. Tracy, W. Jansen, K. Scarfone und J. Butterfield: <http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf>
- [12] E-Mail im Rahmen der LVA Sicherheit in Applikationsprotokollen im SS2010:  
<http://www.dietmueller.at/download/E-Mail.pdf>