erschienen in: Datenschutz und Datensicherung DuD 20/5 (1996) 286-294

Maskerade-Angriffe im Internet

Eine Demonstration von Unsicherheit

Herbert Damker, Universität Freiburg, Institut für Informatik und Gesellschaft
Hannes Federrath, TU Dresden, Institut für Theoretische Informatik, 01062 Dresden
Michael J. Schneider, provet, GMD Darmstadt, Institut für Telekooperationstechnik

Zusammenfassung: *Das Kolleg "Sicherheit in der Kommunikationstechnik" der Gottlieb Daimler - und Karl Benz - Stiftung in Ladenburg hat sich zum Anliegen gemacht, die Sicherheit und Unsicherheit von Kommunikationsnetzen durch verschiedene Arten von Demonstratoren anschaulich zu machen. Die vorliegende Arbeit verfolgt dies für das Problem des Vortäuschens einer falschen Absenderidentität bei Email im Internet, hier Maskerade-Angriff genannt. Die Autoren möchten einen Eindruck vermitteln, wie leicht ein beliebiger Nutzer im Internet elektronische Nachrichten unter Vortäuschung einer falschen Identität verschicken kann.*

Dazu werden zunächst die technischen Hintergründe und einige mögliche Angriffsvarianten beschrieben. Anschließend wird auf Verletzlichkeitsfragen im Zusammenhang mit Maskerade-Angriffen eingegangen und eine kurze Übersicht über Schutz- und Gegenmaßnahmen gegeben. Einige kommentierende Bemerkungen schließen den Beitrag ab.

Ein wichtiger Hinweis vorab: Die Erklärungen zu den Angriffsweisen dürfen natürlich keinesfalls als Anleitungen zum Mißbrauch verstanden werden. Allerdings meinen die Autoren, daß nur informierte Internet-Benutzer die Gefahren des Mediums angemessen einschätzen können. Zudem ist die Erarbeitung von Sicherheitsmaßnahmen nur möglich, wenn die Sicherheitslücken genau bekannt sind. Insofern seien die Leser um verantwortungsvollen Umgang mit den hier präsentierten Informationen gebeten.

1. Vortäuschen falscher Absender bei Email

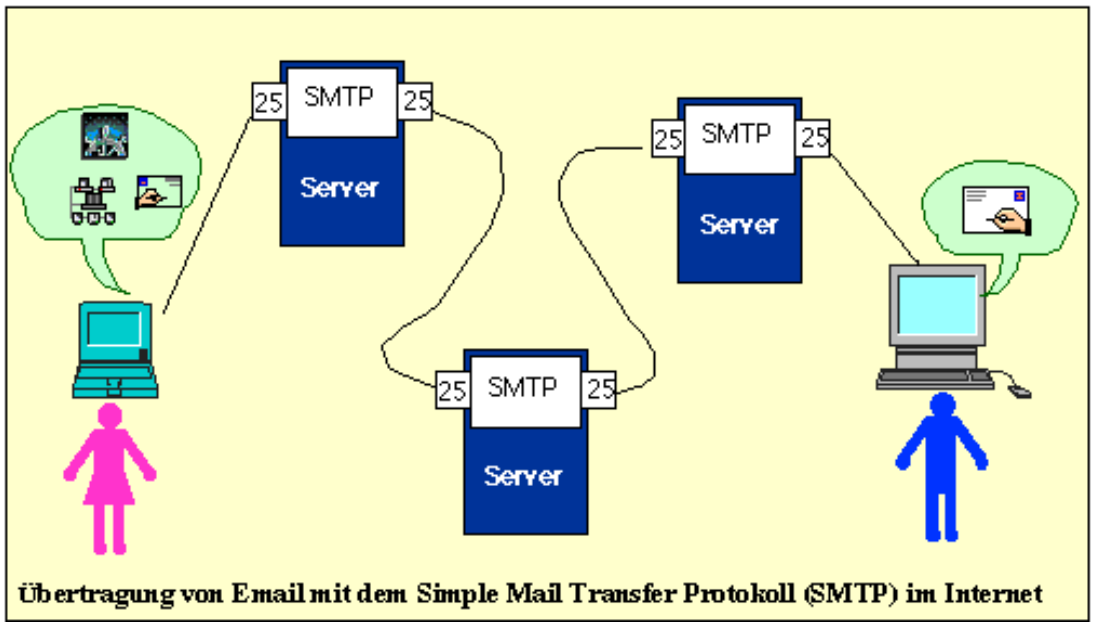
1.1 Technischer Hintergrund

Das weltweite Rechnernetz "Internet" wird gebildet durch den Zusammenschluß vieler Millionen Rechner. Zu Beginn waren dies größtenteils Rechner wissenschaftlicher und technischer Einrichtungen. Mehr und mehr kommen jedoch Rechner aus allen Bereichen des Lebens (Wirtschaft, öffentliche Einrichtungen, private Haushalte) hinzu. Als Folge dieser Integration werden über das Internet auch verstärkt "postalische" Kommunikationsformen gepflegt. Der bedeutendste Dienst dieser Art ist elektronische Post, kurz: Email.

Die verteilte Netzstruktur des Internet besteht aus Rechnern vieler verschiedener Hersteller mit sehr unterschiedlicher Hardware- und Softwareausstattung. Damit die daraus resultierende Vielfalt kein Hindernis bei der weltweiten Kommunikation ist, wurden technische und organisatorische Kommunikationsvereinbarungen getroffen, an die sich alle Rechner des Internet halten.

Für Email hat diese Vereinbarung den Namen *Simple Mail Transfer Protocol* (SMTP). Es arbeitet nach dem *store&forward*-Prinzip. Das bedeutet, der Rechner, von dem die Email abgesetzt wird, schickt sie nicht direkt an den Zielrechner, sondern an einen günstig gelegenen Rechner auf dem Weg zum Zielrechner. Erhält ein günstig gelegener Rechner die Email, so speichert er sie lokal (*store*), sucht einen weiteren günstig gelegenen Rechner und schickt die Email dort hin weiter (*forward*). Dieses *store&forward* wiederholt sich, bis der Zielrechner erreicht ist.

Da nicht alle Teilnehmer auf jedem SMTP-Server im Internet eine Nutzerberechtigung haben können, sind diese Server meist über einen speziellen Zugang (TCP port 25) für den SMTP-Dialog *ohne Account* zugänglich. Ein Angreifer kann also mittels eines für ihn zugänglichen Rechners und einer "irgendwie" gearteten Netzverbindung mit irgendeinem beliebigen SMTP-Server ohne Account kommunizieren. Der Zugangsrechner kann ebenfalls ohne Account nutzbar sein, beispielsweise PCs oder Macintosh-Rechner. Lediglich Rechner mit Zugangskontrolle, z.B. UNIX-Workstations, verhindern den Zugriff durch Unbefugte ohne Account. Als Netzverbindung kann ein organisationsinternes LAN oder eine Telefon/Modem-Verbindung benutzt werden. In diesem Fall muß eine Rufnummer zum Einwählen verfügbar sein.



Übertragung von Email mit dem Simple Mail Transfer Protokoll (SMTP) im Internet

Das *Angriffsziel* soll sein, unter Vortäuschen einer falschen Absenderidentität eine Email an eine beliebige existierende Internet-Mailadresse abzusetzen. Die Absenderidentität kann dabei frei erfunden sein. Es kann aber auch eine beliebige existierende Email-Adresse als Absenderidentität angegeben werden.

1.2 Angriff per Terminal

Für den folgenden Angriff genügt ein Terminalprogramm auf irgendeinem Rechner, der mit einem Internetserver verbunden ist. Der Nutzer

1. hat sich mit seinem Login angemeldet und ein Terminal geöffnet.
2. denkt sich eine falsche Identität aus oder wählt die Identität eines Nutzers, in dessen Namen er eine Email versenden will. Wir wählen: `attacker@nirgends.de`

3. wählt die Email-Adresse des Nutzers (bzw. der Nutzer), die die gefälschte Nachricht erhalten sollen. Es wird als Zieladresse gewählt:
   `federrath@inf.tu-dresden.de`
4. wählt den zu übermittelnden Text:
   `Das ist eine gefaelschte email.`
   `Mr Nobody`
5. wählt einen beliebigen Rechner des Internet, der einen SMTP-Port – gewöhnlich die Nummer 25 – besitzt, den sog. SMTP-Server. Der Angreifer muß auf diesem Rechner *keinen* Account besitzen! Wir wählen: `tcs.inf.tu-dresden.de`

Der Dialog mit SMTP läuft etwa in folgender Weise ab: (">>>"=Benutzereingabe)

```
>>>telnet tcs.inf.tu-dresden.de 25
Trying 141.76.75.101...
Connected to tcs.inf.tu-dresden.de.
Escape character is '^]'.
220 tcs.inf.tu-dresden.de Sendmail 4.1/SMI-4.1 ready at Tue, 30 Jan 96
11:18:45  +0100
>>>MAIL FROM: attacker@nirgends.de
250 attacker@nirgends.de... Sender ok
>>>RCPT TO: federrath@inf.tu-dresden.de
250 federrath@inf.tu-dresden.de... Recipient ok
>>>DATA
354 Enter mail, end with "." on a line by itself
>>>Das ist eine gefaelschte email.
>>>Mr Nobody
>>>.
250 Mail accepted
>>>QUIT
221 tcs.inf.tu-dresden.de delivering mail
Connection closed by foreign host.
```

Damit ist die Email abgeschickt.

Der Nutzer `federrath@inf.tu-dresden.de` erhält nun folgende Nachricht:

```
X-POP3-Rcpt: hf2@irz301.inf.tu-dresden.de
Received: by irz301.inf.tu-dresden.de (8.6.12/8.6.12-s1) id LAA17026 for
hf2@irz.inf.tu-dresden.de; Tue, 30 Jan 1996 11:14:59 +0100
From: attacker@nirgends.de
Received: from tcs.inf.tu-dresden.de by irz301.inf.tu-dresden.de
(8.6.12/8.6.12-s1) with SMTP id LAA16965 for <federrath@inf.tu-dresden.de>;
Tue, 30 Jan 1996 11:13:58 +0100
X-PH: V4.2@irz301.inf.tu-dresden.de
Received: from  (irz101.inf.tu-dresden.de) by tcs.inf.tu-dresden.de (4.1/SMI-
4.1)
        id AA20259; Tue, 30 Jan 96 11:15:50 +0100
Date: Tue, 30 Jan 96 11:15:04 +0100
Message-Id: <9601301015.AA20259@tcs.inf.tu-dresden.de>
Apparently-To: federrath@inf.tu-dresden.de

Das ist eine gefaelschte email.
Mr Nobody
```

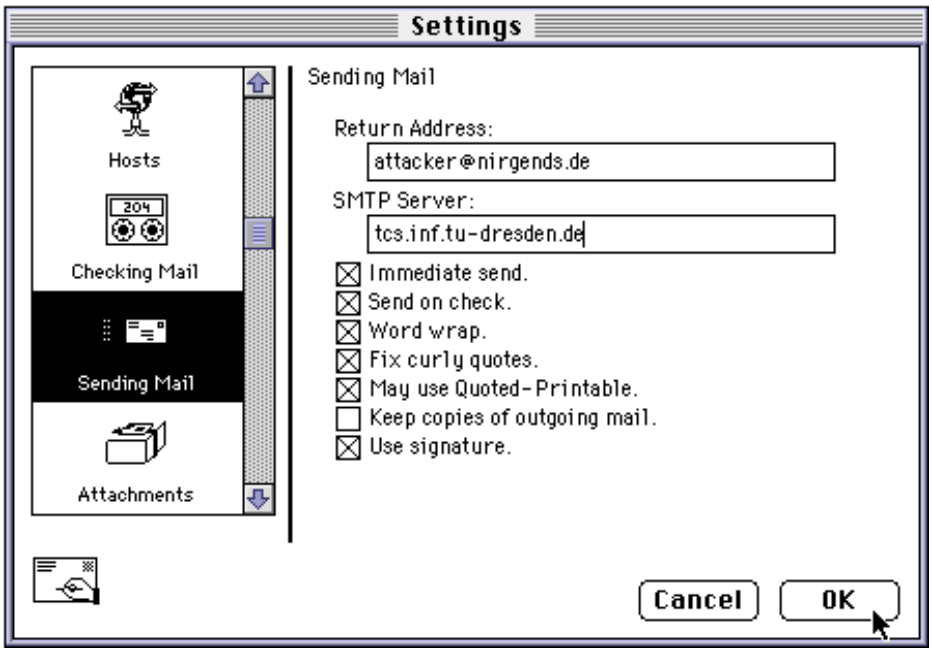
Anhand der Zusatzinformationen im Header der Email kann er nur erkennen, daß die Email

- vom Server `irz101.inf.tu-dresden.de` abgeschickt wurde und
- die Rechner `tcs.inf.tu-dresden.de` und `irz301.inf.tu-dresden.de` auf ihrem Weg zum Zielrechner durchlaufen hat.

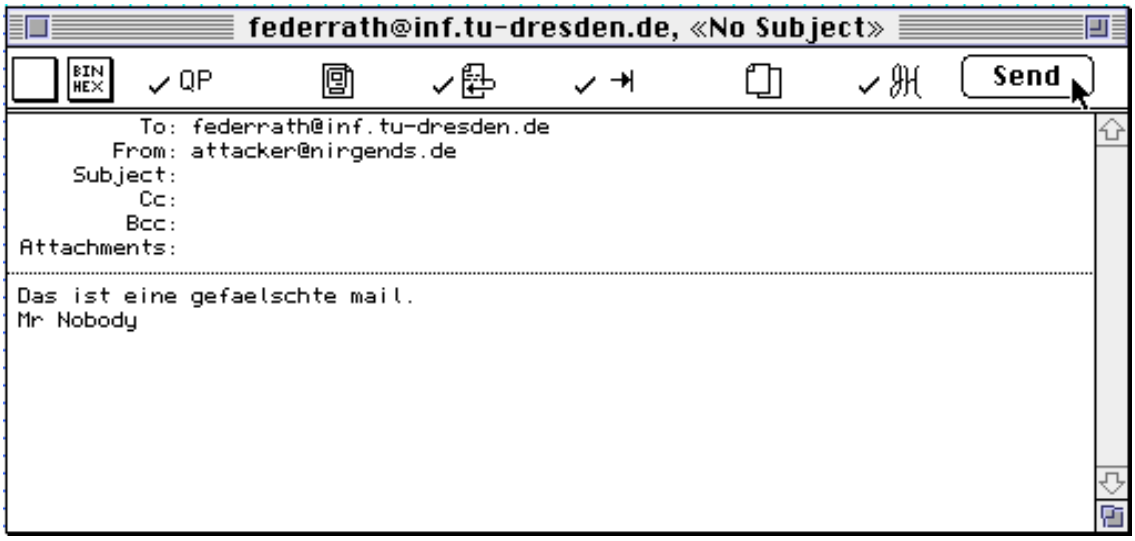
1.3 Angriff mittels eines Mailprogramms

Der hier beschriebene Angriff wird auf einem Apple Macintosh Rechner durchgeführt und findet über eine bestehende MacTCP-Verbindung zu einem Internet-Server statt. Auf dem Rechner muß ein Mail-Programm installiert sein oder durch den Angreifer installiert werden. Im hier beschriebenen Beispiel wird das Programm Eudora verwendet.

Der Angreifer wählt wie oben beschrieben die gewünschten Daten und trägt sie in die Konfiguration des Mail-Programms ein:



Jetzt setzt der Angreifer folgende Email ab:



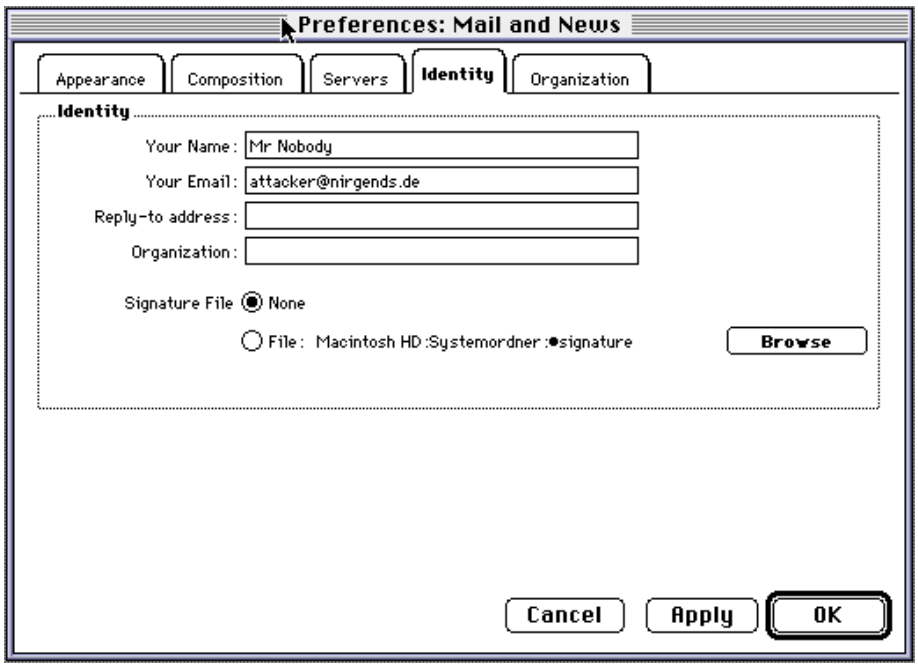
Der Eintrag der Zeile "From:" erfolgt vom Mail-Programm automatisch – entsprechend der Einstellung der Konfiguration.

Der Empfänger erhält die folgende Email:

1.4 Angriff mittels WWW-Browser

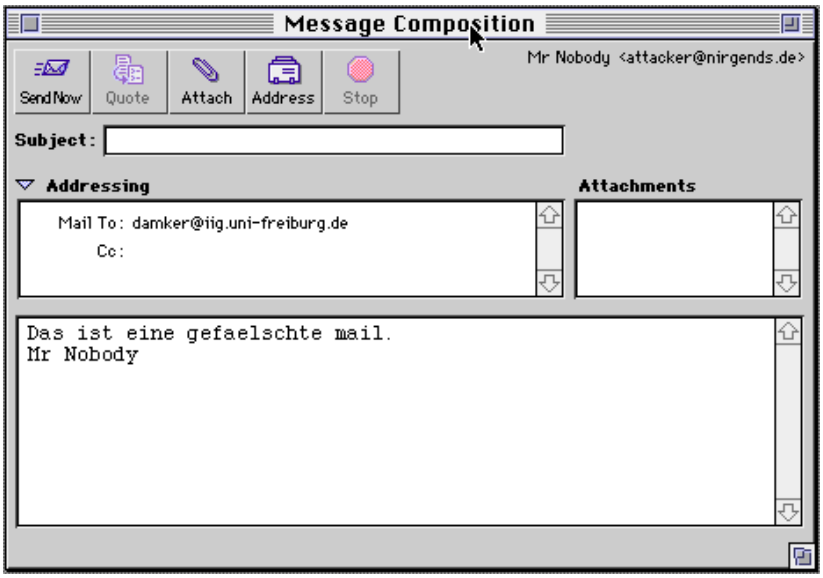
Die meisten der populären Browser (Netscape, Mosaic) für das World-Wide-Web (WWW) haben eine Funktion integriert, die es erlaubt, Emails zu versenden. Diese Programme sind häufig auf Rechnern installiert, die weitgehend frei zugänglich in Pool- oder Arbeitsräumen stehen. Durch einfache Änderungen an der Voreinstellungen der Programme hat ein Angreifer hier die Möglichkeit, eine Email unter falscher Identität abzusenden, ohne daß Rückschlüsse auf seine Person möglich sind. Das folgende Beispiel zeigt das Vorgehen mit der aktuellen Version 2.0 des "Netscape Navigators".

Der Angreifer wählt wie oben beschrieben eine "Identität" und trägt sie in den Abschnitt "Identity" der Voreinstellungen des Programms ein.

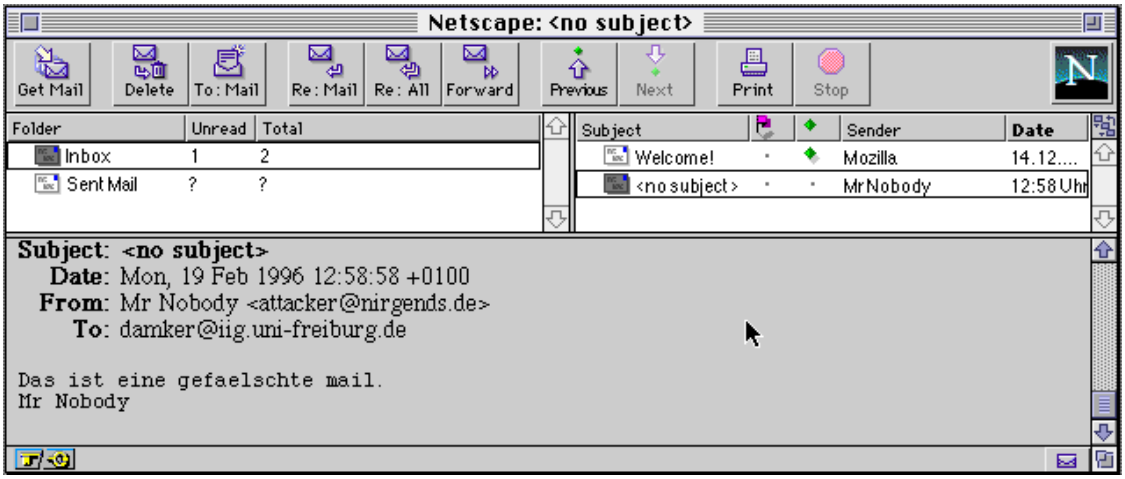


Im Abschnitt "Servers" trägt er den SMTP-Server ein, der für den Angriff verwendet werden soll:

Nun erstellt er eine Nachricht (hier an die Adresse "damker@iig.uni-freiburg.de") und schickt diese ab:



Verwendet der Empfänger den Netscape Navigator zum Lesen von Email, so erscheint die empfangene Nachricht bei ihm so:



Ein Menüpunkt ermöglicht auf einfache Weise, alle Header-Zeilen (incl. der Receive-Zeilen) anzeigen zu lassen, in der Grundkonfiguration werden diese jedoch nicht angezeigt.

2. Bemerkungen zur Verletzlichkeit durch Maskerade

Zur Beurteilung von Verletzlichkeitsaspekten werden üblicherweise Fragen der Schadenswahrscheinlichkeit und des Schadenspotentials betrachtet (vgl. Roßnagel/Wedde/Hammer/Pordesch 1990).

2.1 Erfolgs- und Schadenswahrscheinlichkeiten

Ob und wie wahrscheinlich Maskerade-Angriffe erfolgreich sind, hängt davon ab,

- welche Tools der Angreifer verwenden kann,
- welche Anzeigeoptionen der Empfänger wählen kann und
- wie die Empfänger sich als Nutzer allgemein verhalten.

Zur technischen Fälschbarkeit

Normalerweise protokollieren die SMTP-Server die Rechneradresse des tatsächlichen Senders und schicken diese mit. So sieht zwar der Empfänger eine falsche "Return-Adresse", kann aber im Prinzip am Wege-Protokoll der Mail erkennen, woher sie wirklich stammt.

So ist es beispielsweise unwahrscheinlich, daß eine Email von Herbert Damker an Hannes Federrath von einem Rechner der Universität Freiburg aus über einen SMTP-Server in Italien versendet wird. Ein solcher Umstand müßte also Verdacht erregen, wenngleich damit auch der Angreifer noch nicht ausgemacht werden kann.

Es gibt jedoch auch SMTP-Server, die die Rechneradresse des Absenders (aus welchen Gründen auch immer) nicht mitschicken. Die Autoren haben einen solchen in Deutschland gefunden. (Die Administratoren sind auf das Problem hingewiesen, sagten aber, es ließe sich nicht ändern.) Wer eine gefälschte Mail durch einen solchen SMTP-Server erhält, erfährt also nichts über die mögliche Lokalisierung des Senders.

Zu den Angreifertools

Die Telnet-Variante des Versuchs macht die Durchführung des Angriffs gerade dadurch leicht, daß sie "unkomfortabel" ist. So wird an Informationen nur das nötigste versendet und der Angreifer hat darüber volle Kontrolle, da er die Daten per Hand eingeben muß.

Bei Verwendung komfortablerer Programme sind eine Reihe von Einstellungen vorzunehmen. Dabei ist auf Vollständigkeit und Konsistenz zu achten, damit nicht automatisch erzeugte inkonsistente Informationen mit der falschen Email versendet werden.

Zu den Anzeigeoptionen beim Empfänger

Werden vom Mailprogramm des Empfängers die vollen Header angezeigt, so kann er den Weg der Nachricht verfolgen. Leider blenden jedoch viele Mail-Programme die "unwichtigen" Header aus, so daß selbst ein Nutzer, der gewillt ist, sich durch die unübersichtlichen Received-Informationen zu arbeiten, keine Möglichkeit der Kontrolle des Absenders hat.

Die meisten Mailprogramme bieten dem Empfänger die Möglichkeit, einen verkürzten Header anzuzeigen, in dem beispielsweise nur das "From"-, "To"- und "Subject"-Feld aufgeführt werden. In dieser Anzeigeweise kann der Empfänger zumindest aufgrund der Headerangaben keinen Verdacht schöpfen. Bei einigen Mailtools ist es sogar mit Aufwand verbunden, den vollständigen Header anzeigen zu lassen. Bei der

Standardkonfiguration von Eudora werden jene Header ebenfalls ausgeblendet, um die Übersichtlichkeit zu erhöhen. Im Konfigurationsmenü oder mit einem Button des Nachrichtenfensters (mit "blah, blah" etwas unglücklich bezeichnet) kann man sie jedoch einschalten.

Zum Nutzerverhalten

Eine entscheidende Größe für den Erfolg oder Mißerfolg eines Angriffs ist das Verhalten der Empfänger, insbesondere ihre Skepsis oder nicht-Skepsis beim Lesen von Email. Ein Hinweis auf eine gefälschte Email könnte es sein, wenn auf dem Weg ein SMTP-Server durchlaufen wird, den bisherige Emails dieses Absenders noch nie durchlaufen haben.

Natürlich werden im Normalfall die verkürzten Header angezeigt, da sich die Nutzer nicht für die "technischen" Angaben interessieren. Verdacht kann also nur geschöpft werden, wenn der Inhalt einer Nachricht wirklich sehr ungewöhnlich ist.

2.2 Schadensszenarien

Erfolg und Schadensausmaße von Angriffen hängen auch von Angriffskonstellationen ab. Gewöhnlich gehört dazu eine Betrachtung der möglichen Angriffsmotive und der Angreifertypen.

Während bei Fragen der Verletzlichkeit von Informations- und Kommunikationstechnik herkömmlich zwischen internen und externen Angreifern unterschieden wird, fällt dies im Falle der Email-Nutzung schwer, da die Grenze zwischen intern und extern nicht einfach an den Grenzen einer Organisation orientiert werden kann. In Bezug auf die Internet-Nutzung kommt jeder Internet-Teilnehmer als interner Angreifer in Frage.

Die Voraussetzungen eines Angreifers wurden oben bereits genannt. Sie können sowohl mit als auch ohne Account handeln. Es gibt allerdings bestimmte Konstellationen, die hinsichtlich des Empfängerverdachts einen Angriff begünstigen:

So fällt die Fälschung nicht auf, wenn der Angreifer einen Account am SMTP-Server selbst hat und sowohl der falsche Absender als auch der Empfänger von diesem Mailserver bedient werden, weil sie in der gleichen Organisation beschäftigt sind. Der Empfänger erhält dann vermeintlich eine Mail von einem Kollegen (der Firma, der Universität, etc.) mittels des eigenen Mailservers, was ganz gewöhnlich aussieht. Für diesen Angriff genügt es bereits, daß der echte und falsche Abesender den gleichen SMTP-Server benutzen.

Angriffsmotive dürften im Wesentlichen darin bestehen, die Empfängerperson zu Handlungen zu bewegen, die dem Angreifer in irgendeiner Weise nützen. Das könnte beispielsweise die Bitte um Informationsherausgabe sein, das Weglocken des Empfängers von seinem Arbeitsplatz, um dort unbemerkt etwas zu tun oder das Auslösen von Handlungen, die in der Kompetenz des Empfängers, nicht aber des Angreifers liegen. Hier wäre etwa an die Bitte um Einrichtung bestimmter Accounts an einen Systemverwalter zu denken oder ähnliches. Ferner sind Sabotage- oder Störmotive zu berücksichtigen.

Einige Beispiele für organisationsinterne Angriffe dieser Art sind:

- Abteilungsleiter ernennt Gruppenleiter zu seinem neuen Stellvertreter
- Kollegin A. bittet Kollege B., für sie ein teures Mittagessen mitzubestellen
- Kollege C. läßt vom Einkauf einen neuen Rechner ordern

- Die Verwaltung informiert Mitarbeiterin D. über ihre bevorstehende Kündigung
- Die Verwaltung informiert über neue interne Stellenausschreibungen

Erleichtert werden solche Angriffe noch, wenn die vermeintlichen Absender gerade auf Dienstreise sind und daher einerseits auf Rückfragen nicht sofort reagieren können bzw. andererseits es den Empfängern plausibel erscheinen kann, daß die Email von fremden SMTP-Servern kommt.

2.3 Mögliche Schadensausmaße

Über die Schadensausmaße kann hier in aller Kürze festgehalten werden, daß bei entsprechend intelligenten Fallkonstellationen sicher hohe Einzelschäden möglich sind. Ob diese reversibel sind, hängt vom Gegenstand des Angriffs ab und vor allem davon, welche sozialen Auffangmechanismen einsetzen können. Wird beispielsweise eine falsche elektronische Bestellung ausgeliefert und in Rechnung gestellt, so kann im Prinzip nach der Klärung, daß die Bestellung falsch war, die Ware zurückgegeben werden.

Schwieriger könnte der Umgang mit einer großen Menge vergleichsweise einfacher Angriffe werden. Wenn etwa jeder Internet-Nutzer täglich mit 50% gefälschten Mails konfrontiert wird, wird die Nutzbarkeit des Mediums stark in Frage gestellt.

Insgesamt wird das Schadenspotential um so höher, je abhängiger die mittlerweile schon vielen Internet-Nutzer von dieser Kommunikationsart werden. Dann nämlich, wenn für immer mehr Nutzer das Medium Email das hauptsächliche oder sogar alleinige Kommunikationsmittel mit bestimmten Personen geworden ist, kann eine große Anzahl von Maskerade-Angriffen indirekt zum Angriff auf die Verfügbarkeit werden.

3. Schutz- und Gegenmaßnahmen

3.1 Pretty Good Privacy

Das Programm *Pretty Good Privacy* (PGP) des Amerikaners Phil Zimmermann bietet dem Nutzer von Email eine leichte Möglichkeit, die Integrität einer Email, d.h. die Unverfälschtheit des Nachrichteninhaltes und Authentizität des Absenders zu testen (vgl. Garfinkel 1995). Weiterhin unterstützt es die Vertraulichkeit der Nachrichteninhalte, da eine Verschlüsselung der Nachrichten ebenfalls möglich ist.

Die Sicherheit der implementierten Funktionen beruht auf kryptographischen Verfahren:

Die Nachrichtenintegrität und Authentizität werden mit *public key*-Verfahren erreicht. Es wird an die Nachricht eine digitale Signatur angehängt.

Die Vertraulichkeit der Nachrichteninhalte wird mit hybriden Kryptoverfahren, d.h. einer Kombination von *public key*- und *secret key*-Verfahren, erreicht

Das Schlüsselmanagement von PGP ist dezentral organisiert. Die Zertifizierung der eigenen öffentlichen Schlüssel erfolgt durch die anderen Nutzer des Systems, wenn sie der Authentizität eines Schlüssels trauen.

Eine Email, die digital signiert ist, hat etwa folgende Gestalt:

```
Date: Thu, 22 Jun 1995 10:15:49 +0100
To: federrath@inf.tu-dresden.de
From: test@tcs.inf.tu-dresden.de

-----BEGIN PGP SIGNED MESSAGE-----

Hallo Hannes,
das ist eine signierte Nachricht.

-----BEGIN PGP SIGNATURE-----
Version: 2.6ui

iQCVAgUBL+k0s9YZ8Y2Or0HBAQFfBQP8CDqPcMeNcamBcVS5IQFESsvSoMsKcucy
AKp6bJnsDzbbMbAFIlke+N/1HsagcUtwS1NXFNh7WH9mRbZfk61DKUp9akPWciPh
kQuCh9vX50mNPBjqdZeSAaY08qPqOR3BLxXKt3KiHo/FE2CA3wh874QCNWWoMebO
D1fMoPKDJes=
=aRrI
-----END PGP SIGNATURE-----
```

Eine Email, die verschlüsselt (und evtl. signiert ist), stellt sich folgendermaßen dar:

```
Date: Thu, 22 Jun 1995 10:14:52 +0100
To: federrath@inf.tu-dresden.de
From: test@tcs.inf.tu-dresden.de

-----BEGIN PGP MESSAGE-----
Version: 2.6ui

hIwCAP2OoXUGJkEBA/9jj79NxKhbsb+1+1ujSTWP40EYSPXKvhtRK9vJ2I3Lj2kk
M/vralTGN0l+RSbkpHet7GEGrlZbfc5pOqdDlDgjPddpMdrBQpfojH/MT/87/vEq
N3N8Geh2MsNjXqGDGx8kJlqhQ2s7Vcy0W99HRmo82mLohc5Vn1oY+49ZGIfWJKYA
AAD5XPGjb00jexwviwh91mao/dGL9bTc/zhnhfBCqY4ILJtYxM6ewC4ZeFHP1xlM
xdUXZuRqYInFckgUO/yrty9bAszwEehHUtgNxJ4DTYDWsQw+Xy9zFLKExuOux1Ex
rW/zo7I72qBBpnc71CU1kGxO+H/dq2fx52kF+uYh8+pvHORNOp7z1JIijyiDay+u
VW95szEpWPWujDXBSXYABOpIWbpTmFxF9ZImFkQHYVew5EsUB37Gebpz4/aAezfG
xuR07VeLyo1W+ZuYjMtv5s+lDyHputqxuhmPH+Fj6ut1s0qfE8l8qgEB2ywRcYiW
20oiwaJuXgXWWCuE
=4XoS
-----END PGP MESSAGE-----
```

Es existieren inzwischen einige Anbindungen von PGP und Mail-Programmen. Viele davon zeichnen sich bereits durch gute Handhabbarkeit aus.

3.2 Privacy Enhanced Mail (PEM)

Es existiert derzeit für Email noch eine weitere Initiative unter dem Namen *Privacy Enhanced Mail* (PEM). Im Gegensatz zu PGP ist die Zertifizierung der öffentlichen Schlüssel gemäß dem Standard X.509 hierarchisch organisiert (vgl. CCITT X.509, 1988 sowie die RFCs 1421-1424). Das Verfahren ist also erst einsetzbar, wenn es eine funktionierende Infrastruktur von Zertifizierungsservern gibt. Diese aufzubauen lohnt sich jedoch erst, wenn das Verfahren in gängige Mail-Programme integriert ist. Die Lösung dieses klassischen Henne-Ei-Problems hat sich auf europäischer Ebene das Projekt ICE zum Ziel gesetzt (vgl. W. Schneider, 1995).

4. Kommentar

4.1 Weitere Sicherheitsprobleme

Neben der Fälschbarkeit von Email existieren noch weitere Probleme, die insbesondere die Vertraulichkeit von Nachrichteninhalten betreffen. So können die Systemadministratoren aller Rechner, die eine Email auf dem Weg zum Zielrechner durchläuft über Manipulation ihres lokalen SMTP-Servers erreichen, daß die (gemäß der *store*-Funktion von *store&forward*) zwischengespeicherten Emails nicht gelöscht werden. Somit kommen der Systemadministrator und alle weiteren Personen, die Zugriff auf diese gespeicherten Nachrichten haben, in Kenntnis der Nachrichteninhalte.

Ein weiteres Problem sind sogenannte log-Dateien, die Informationen über die Aktivitäten eines Systems enthalten und im Fehlerfall die Fehlersuche erleichtern sollen. So speichert z.B. das Programm `sendmail` Informationen über Absender, Adressat, Datum und Urzeit des Absendens und Empfangens von Email. Häufig sind die Dateien für jeden Nutzer lesbar. Als Folge davon lassen sich Kommmunikationsprofile der Nutzer sehr leicht erstellen.

Die gespeicherten Informationen einer an die Nutzer `test@tcs.inf.tu-dresden.de` und `federrath@inf.tu-dresden.de` gesendeten Email (Sender: `feder@tcs.inf.tu-dresden.de`) sehen etwa so aus:

```
tcs>tail /var/log/syslog
Jan 15 16:32:06 tcs sendmail: from=<feder@tcs.inf.tu-dresden.de>, size=1150,
class=0
Jan 15 16:32:06 tcs sendmail: to=<test@tcs.inf.tu-dresden.de>, delay=00:00:01,
stat=Sent
Jan 15 16:32:07 tcs sendmail: to=<federrath@inf.tu-dresden.de >,
delay=00:00:03, stat=Sent
Jan 15 16:39:29 tcs sendmail: message-id=<9601151539.AA29075@tcs.inf.tu-
dresden.de>
```

4.2 Warnung vor Nachahmung

Mit einem ähnlichen Artikel (Fox, 1995) wurde bereits in Fachkreisen Aufsehen erregt, weil der Autor in seinem Beispiel die Adresse des Mailservers des Weißen Hauses angegeben hatte.

Die Sicherheitsgruppe CERT (*Computer Emergency Response Team*) des Deutschen Forschungsnetzes (DFN) äußerte sich darauf wie folgt:

> *"... in der c`t 9/95 Seite 185 sollte demonstriert werden, wie einfach der Absender von Mails gefälscht werden kann. Bei dem abgedruckten Beispiel wird dieser Angriff auf den Rechner {...} des Weißen Hauses dokumentiert. Dieses Beispiel hat offensichtlich viele Leser dazu veranlaßt, diesen Angriff selbst auszuprobieren. Der ahnungslose Administrator des Rechners {...} stellt seitdem eine Vielzahl von Login-Versuchen auf seinem Rechner fest. Der Adminstrator hat daraufhin CERT/CC informiert, die wiederum uns (das DFN-CERT) gebeten haben, der Sache nachzugehen.*
>
> *Von uns ein paar Anmerkungen zu diesem Vorfall:*
>
> ** Angriffe auszuprobieren, nur weil sie irgendwo veröffentlicht sind, ist keine akzeptable Benutzung des Netzes und wird von dem Betroffenen als Angriff gewertet.*

** Völlig indiskutabel ist es, Adressen von möglichen Opfern zu veröffentlichen. Wenn die c`t eine Beispiel-Adresse benötigt, soll sie ihre eigene dafür verwenden!*

Bitte halten Sie Ihre Benutzer zu einem verantwortungsvollen Umgang mit dem Internet an.

Mit freundlichen Grüßen

Uwe Ellermann, DFN-CERT, University of Hamburg"

Es muß deshalb noch einmal deutlich vor der Nachahmung gewarnt werden bzw. zu einem verantwortungsvollen Umgang mit dem Netz aufgefordert werden! Das Internet funktioniert zur Zeit nur auf der Basis gegenseitigen Vertrauens!

5. Weiterführende Materialien

5.1 Literatur

Fox, D. (1995): Schlüsseldienst - Private Kommunikation mit PEM und PGP, c`t 9/95.

Garfinkel, S. (1995): PGP: Pretty Good Privacy, O'Reilly & Associates, Inc., Sebastopol/CA, January 1995.

Roßnagel, A.; Wedde, P.; Hammer, V.; Pordesch, U. (1990): Die Verletzlichkeit der 'Informationsgesellschaft', Westdeutscher Verlag, Opladen 1989, 2. Auflage 1990.

Schallbruch, M. (1995): Electronic Mail im Internet; Wie steht es mit dem Datenschutz? Datenschutz-Nachrichten 5/95. (auch im WWW, siehe unten)

Schneider, W. (1995): Interworking Certification Infrastructure for Europe (ICE); In: Horster, P.: Proceedings der gemeinsamen Arbeitstagung Trust Center '95 der GI-Fachgruppe 2.5.3 Verläßliche IT-Systeme und dem TeleTrust Deutschland e.V., Vieweg Verlag, Braunschweig/Wiesbaden 1995.

5.2 Internet-RFCs

(auch im WWW bzw. per FTP erhältlich, siehe unten)

- Internet Requests for Comments (RFC) No. 821 und No. 822:
  - Postel, J. B.: "Simple Mail Transter Protocol", August 1982. (RFC 821)
  - Crocker, D., "Standard for the Format of ARPA Internet Text Messages," August 1982. (RFC 822)
- Internet Requests for Comments (RFC) No. 1421-1424 (1993):
  - Linn, J.: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", 02/10/1993. (RFC 1421)
  - Kent, S.: "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", 02/10/1993. (RFC 1422)
  - Balenson, D.: "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", 02/10/1993. (RFC 1423)
  - Kaliski, B.: "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services", 02/10/1993. (RFC 1424)

5.3 Internet/WWW-Adressen

- Datenschutz-Informationen (German Privacy Informations), von Martin Schallbruch
  - http://respa.rewi.hu-berlin.de:80/Datenschutz/
- German Cert:
  - http://www.cert.dfn.de/
- GMD-SIT (Security Technology), Aktivitäten
  - http://www.darmstadt.gmd.de/TKT/security/
  - speziell: Privacy Enhanced Mail: http://www.darmstadt.gmd.de/TKT/security/www95-PEM/PEM4WWW.html
- IDENTITY, PRIVACY, and ANONYMITY on the INTERNET (c) Copyright 1993 L. Detweiler,
  - http://www.rewi.hu-berlin.de/Datenschutz/Netze/privint.html
- Internet-RFC-Index:
  - http://www.internic.net/ds/rfc-index.html
- Pretty Good Privacy (PGP):
  - http://www.ifi.uio.no/pgp
  - news:comp.security.misc,
  - news:alt.security.pgp
- Schallbruch, M. (1995): Electronic Mail im Internet; Wie steht es mit dem Datenschutz? Datenschutz-Nachrichten 5/95,
  - http://www.rewi.hu-berlin.de/~mascha/mailds.html

Dank: Wir danken Andreas Pfitzmann, Kai Rannenberg, Gritta Wolf und Jan Zöllner für Hinweise und Kommentare.

Stichwörter: Electronic Mail, E-Mail, Internet, Maskerade, SMTP

Herbert Damker: Diplom-Informatiker, seit 1994 wissenschaftlicher Mitarbeiter am Institut für Informatik und Gesellschaft der Universität Freiburg. Arbeitsgebiete: Software-Ergonomie, verteilte Informationssysteme, Sicherheit in der Kommunikationstechnik.

Hannes Federrath: Diplom-Informatiker, seit 1994 wissenschaftlicher Mitarbeiter an der TU Dresden, Institut für Theoretische Informatik, Arbeitsgebiete: Sicherheit in verteilten Systemen, Technischer Datenschutz in Mobilkommunikationssystemen.

Michael J. Schneider: Diplom-Informatiker, seit 1990 Mitarbeiter der Projektgruppe Verfassungsverträgliche Technikgestaltung (provet) e.V. in Darmstadt. Ausserdem seit 1994 Doktorand in der GMD in Darmstadt. Arbeitsgebiete: Technikfolgenforschung, Sicherheit in der Kommunikationstechnik, Mobilfunkanwendungen und Erreichbarkeitsmanagement.