Standards für informatische Bildung
E-Mail-Kompetenzen

Jochen Koubek
Humboldt-Universität zu Berlin
Informatik in Bildung und Gesellschaft

Als Ray Tomlinson 1971 die erste E-Mail verschickte, war er sich der historischen Bedeutung seiner Erfindung nicht bewußt, rollte mit allen zehn Fingern über die obere Buchstabenreihe seiner Tastatur und gab der ersten E-Mail damit den gänzlich unspektakulären Text „qwertyuiop". Tomlinson ahnte nicht, dass E-Mail sich zur erfolgreichsten Netzanwendung entwickeln würde, wie viele Internetpioniere wurde auch er vom Erfolg der neuen Protokolle überrascht. Anfang 2004 nutzten in Deutschland 47% der Bevölkerung den Dienst E-Mail, die Quote lag unter Schülern sogar bei 78% [SB05]. E-Mail ist als Medium so erfolgreich, dass es inzwischen zum Opfer seines eigenen Erfolgs wird. Teilt man E-Mails in gewünschte und ungewünschte Sendungen [BSI05] so gehören Schätzungen zufolge nur noch 10% aller E-Mails zur ersten Kategorie. Die unerwünschten Mails teilen sich wiederum auf in kommerziellen und nicht-kommerziellen Spam, Malware, d.h. Viren und Würmer, die sich automatisch über die Adressbücher verschicken, Rufschädigungen und Verleumdungen, Phishing-Mails, die Passwörter, PINs und TANs zu erschleichen suchen, Hoaxes, Scherz- und Kettenbriefe, leere Mails sowie Collateral Spam, der entsteht, wenn E-Mails mit unbekannter Adresse an den gefälschten Absender zurückgeschickt werden.

Hauptgrund für diese Entwicklung ist der Umstand, dass der empfangende Server die Absenderadresse nicht kontrollieren kann und Fälschungen somit folgenlos bleiben. Lediglich die IP-Adressen des Senders sind identifizierbar, aber fehlende internationale Regelungen verhindern die Rückverfolgung diese Adressen. Tomlinson rechnete weder mit der großen Nutzerzahl noch damit, dass einige sich nicht an die Regeln der Online-Community halten würden und dies im großen Stil.

Angesichts dieser Entwicklung umfasst der Umgang mit dem Medium E-Mail mehr als Verfassen und Lesen von Nachrichten. Systematisch muss die Kompetenz aufgebaut werden, E-Mails auf ihre Absichten zu befragen und kritisch mit den erhaltenen Sendungen umzugehen.

Eine für diese Zwecke günstigere Unterscheidung der Mails als die erwähnte in *erwünscht/unerwünscht* ist die in *vertrauenswürdig* und *nicht vertrauenswürdig*. *Vertrauen* heißt hier, dass der Empfänger dem Absender redliche Kommunikationsabsichten unterstellt.

Das bedeutet nicht, dass er dem Inhalt in jedem Fall Glauben schenkt – auch ein Freund kann lügen oder sich irren – er geht aber davon aus, die Absichten des Senders einschätzen zu können.

Beide Kategorien sind im Wesentlichen deckungsgleich. Nutzer vertrauen den E-Mails, deren Empfang gewünscht ist. Gegen E-Mails, die unerwünscht sind, haben sie einen Vertrauensvorbehalt. Der Trick der Absender unerwünschter E-Mails besteht nun darin, ihre Sendungen als vertrausenwürdige zu tarnen. Zur näheren Erläuterung ist es notwendig, die Bestandteil einer E-Mail zu kennen, anhand derer sich Vertrauen oder Misstrauen bemessen lassen. Die folgende Liste erklärt nicht die Bestandteile, die ich als bekannt voraussetze, sondern sie führt Gründe auf, wann einer dieser Bestandteile den Verdacht bestärkt, eine nicht-vertrauenswürdige E-Mail erhalten zu haben.

- **Adresse:** Wer Wegwerf- oder Einmaladressen einrichtet, erwartet über diese Adresse keine weiteren Mails als für den Zweck, für den sie eingerichtet wurde. Gleiches gilt für alte Adressen, die zwar noch weitergeleitet werden, aber nicht mehr in Benutzung sind. Beispiel: Meine Studenten-Adresse ist zwar noch heute gültig und nicht kündbar, sie wird aber nur noch von Spammern genutzt.
- **Absender:** Während die Adresse gültig sein muss, kann ein beliebiger Absender in der Mail stehen. Insbesondere unbekannte oder kryptische Adressen sind hier verdächtig. Aber auch bekannten Absenderangaben ist nicht zu trauen, Viren kommen meistens aus dem Bekanntenkreis. Der Angabe des Absenders ist alleine grundsätzlich nicht zu trauen.
- **Betreff:** Anhand der Betreff-Zeile können viele Mails als verdächtig eingestuft werden, allen voran WerbE-Mails.
- **Sprache:** Wer eine Mail in einer unerwarteten Sprache erhält, sollte vorsichtig sein. Nur wenige Schüler dürften englischsprachige Mails erwarten.
- **Schlüsselwörter:** Manche Begriffe deuten klar auf unerwünschte Mails.
- **Inhalt:** Entspricht der Inhalt den Erwartungen? Ganz wichtig: Ist der Inhalt persönlich formuliert, oder wäre es möglich, die Mail an einen beliebigen Adressaten zu verschicken?
- **Anhang :** E-Mails mit Anhängen sollten zunächst immer als verdächtig eingestuft und in jedem Fall genauer geprüft werden.**Return-Path:** Über den Return-Path läßt sich die E-Mail bis zur sendenden IP-Adresse zurückverfolgen. Der Return-Path ist der sicherste Weg, um die Gültigkeit einer Absende-Adresse zu prüfen. Bei Virenmails ist der Return-Path allerdings trügerisch und verweist auf einen befreundeten Absender.
- **URLs:** Sind URLs in der Mail angegeben? Phishing-Mails bedienen sich dieser Technik, wobei die angezeigte Adresse keineswegs mit der tatsächlichen URL übereinstimmen muss. Hier hilft nur ein Blick in den
- **Quelltext:** In HTML-Mails lassen sich bei URLs vor Gebrauch prüfen, ob die Angaben im href-Attribut mit der in der Mail gedruckten übereinstimmt.

Autoren, die für die Sendung unerwünschter Mails verantwortlich sind, bemühen sich, ihre Sendungen als vertrauenswürdige erscheinen zu lassen, um entsprechende Reaktionen beim Empfänger zu provozieren, bei Spams eine Geschäftsbeziehung, bei Malware eine Installation, bei Kettenbriefen Weitersendung etc. Zu diesem Zweck versuchen sie sich, möglichst viele Bestandteile als vertauenswürdig erscheinen zu lassen. Da unerwünschte Mails i.d.R. an einen unbestimmten Empfängerkreis gerichtet sind entsteht dabei das Problem, Massenmails individuell erscheinen zu lassen. Dieses Problem ist zum Glück noch nicht gelöst, so dass Muster entstehen, anhand derer sie automatisch gefiltert werden können. Da bei diesen Filtern Falschpositivmeldungen vermieden werden müssen, schaffen es immer einige Mails durch das Netz, sie können aber von Hand relativ einfach aussortiert werden.

Bei vertrauenswürdigen Mails entsprechen alle Kriterien der Erwartung. Umgekehrt verdient eine Mail das Attribut *nicht vetrauenswürdig*, wenn nur eines der Bestandteile verdächtig ist. Solche Mails erfordern eine besondere Prüfung, sollten in jedem Fall vorsichtig behandelt und im Zweifelsfall gelöscht werden.

Das Vorgehen ist Folgendes:

Entsprechen alle Kriterien der Mail der Erwartung?
Falls ja: Mailstatus *vertrauenswürdig*
Falls nein. Ist die Mail eine klare unerwünschte Sendung?
Falls ja: löschen
Falls nein: Gibt es erkennbare Gründe, warum die Mail anders als erwartet geschrieben wurde?
Falls nein: löschen
Falls ja: Status vertrauenswürdig

Zur Prüfung der Bestandteile sind technische Kenntnisse über Struktur und Funktionsweise von E-Mails in unterschiedlicher Detaillierungsstufe bis hin zum Verständnis der Grundlagen des SMTP-Protokolls, die im Folgenden in aufsteigender Reihenfolge beschrieben werden. Zu jeder Kompetenzstufe wird zumindest eine Aufgabe angegeben, anhand derer die Zielerreichung geprüft werden kann. Jede Kompetenzbeschreibung ist damit von der Form

- Klassenstufe
- Merkmale die mindestens bei der Prüfung von E-Mails berücksichtigt werden sollten
- Beschreibung der Kompetenz, die in der jeweiligen Klassenstufe mindestens erfüllt sein sollte
- Aufgabe
- Kommentar

SuS ist die Kurzform für *Schülerinnen und Schüler.*

Kompetenzen Klassen 5-7

Merkmale: Absender, Betreff, Inhalt, Anhang
Kompetenz: SuS beschreiben Auffälligkeiten an E-Mails.
Aufgabe: Was fällt Dir an folgender E-Mail auf:

```
Von: smuzender01@netscape.net
Betreff: Geschäftliches Angebot
Datum: 20. Mai 2005 18:54:53 MEZ
Antwort an: smuzender01@netscape.net
Sie mögen überrascht sein, diesen Brief von mir zu erhalten, da
Sie mich nicht persönlich kennen. Der Grund meiner Vorstellung
ist, dass ich Simon Muzenda der älteste Sohn von Paul Muzenda
bin, einem Farmer in Simbabwe, der kürzlich im Landstreit in
meinem Land ermordet wurde.
Ich bekam den Kontakt zu Ihnen über das Internet, daher
beschloss ich Ihnen zu schreiben...
```

Komentar:
Auf dieser Kompetenzstufe können E-Mails in der normalen Ansicht überprüft werden. Die genannten Merkmale sind die offensichtlichsten und einfach zu fälschen. So wichtig wie die Frage, ob die Mail anhand dieser Merkmale vertrauenswürdig erscheint ist die, wie plausibel es ist, dass eine solche Mail an 13-jährige SuS verschickt wird.
Die Mails der Aufgabe sollten wennmöglich aus dem aktuellen Tagesgeschehen, d.h. dem eigenen Spam-Ordner, entnommen werden. Bei obiger Mail handelt es sich um eine Variante der Nigeria-Connection. Der volle Text steht unter [Ka05], Hintergründe gibt es unter [Zi02] sowie unter http://www.419eater.com/

Kompetenzen Klassen 8-10

Merkmale: Return-Path
Kompetenzen:
1. SuS geben Verfahren an, mit denen sie überprüfen können, ob eine E-Mail wirklich von dem angegebenen Absender verschickt wurde.
2. SuS recherchieren Hintergründe zu Absenderangaben.
Aufgabe: Von wo wurde die folgende Mail verschickt:

```
Von: news@heise.de
Betreff: News
Datum: 29. April 2005 09:53:40 MESZ
An: jochen.koubek@rz.hu-berlin.de
Return-Path: <news@heise.de>
Received: from localhost (nsuncom.rz.hu-berlin.de [141.20.1.7])
                  by nsuncom2.rz.hu-berlin.de (8.12.11/8.12.11)
                  with ESMTP id j3T7xYJ3018340 for
                  <jochen.koubek@rz.hu-berlin.de>; Fri, 29 Apr
                  2005 09:59:34 +0200 (MEST)
Received: from nsuncom.rz.hu-berlin.de ([127.0.0.1]) by
                  localhost (nsuncom [127.0.0.1]) (amavisd-new,
                  port 10024) with ESMTP id 20830-170 for
                  <jochen.koubek@rz.hu-berlin.de>; Fri, 29 Apr
```

```
                  2005 09:59:32 +0200 (MEST)
Received: from 211.208.147.33 ([211.208.147.33]) by
                  nsuncom.rz.hu-berlin.de (8.12.10/8.12.10)
                  with SMTP id j3T7crkF024846 for
                  <jochen.koubek@rz.hu-berlin.de>; Fri, 29 Apr
                  2005 09:59:24 +0200 (MEST)
Message-Id: <200504290759.j3T7crkF024846@nsuncom.rz.hu-
                  berlin.de>
Mime-Version: 1.0
Content-Type: multipart/alternative; boundary="ejyKFsz7kdNYbjXf"
X-Virus-Scanned: by amavisd-new at cms.hu-berlin.de
X-Spam-Status: No, hits=0.698 tagged_above=-9999.9 required=6
                  tests=BAYES_00, HTML_30_40, HTML_MESSAGE,
                  HTML_TAG_BALANCE_BODY, MIME_HTML_MOSTLY,
                  MSGID_FROM_MTA_SHORT
X-Spam-Level:
Content-Length:10653
Status:

Meldungen des Tages 29.04.2005
c't magazin.tv: Vorsicht Falle -- Flugreisen im Internet
Die Suche nach dem richtigen Internet-Angebot für Flugreisen ist
zwar mühsam, kann sich aber rechnen. Die Möglichkeiten zur
Online-Buchung ist neben günstigen Dia-Scannern und Abmahnungen
der Musikindustrie wegen Links Thema im Fernsehmagazin der c't.
mehr…
Ricoh tritt mit Gel-Printern im Office-Markt an
Mit zwei neuen Geräten, die auf einer selbst entwickelten
Farbdruck-Technik mit gelierenden Tinten basieren, geht der
japanische Hersteller ab Juni an den Start. mehr…
Microsoft blickt optimistisch in die Zukunft
Microsoft kann den Gewinn nahezu verdoppeln, erfüllt aber nicht
ganz die eigenen Prognosen und profitiert unter anderem von
niedrigeren Ausgaben für juristische Streitigkeiten. Für den
weiteren Geschäftsverlauf erwartet man wieder stärkeres
Wachstum. mehr…
```

Kommentar: Die Lösung der Aufgabe fordert das Verständnis der E-Mail-Header, insbesondere des *Return-Path* und der *Received*-Felder. Bei dieser Aufgabe bietet sich der Einsatz eines Tracer-Programms an. In obiger Aufgabe wird schnell deutlich, dass der Rechner mit der Adresse **211.208.147.33** in Australien steht und nicht etwa bei **heise.de**. Ein kurzer Blick auf das Impressum dieser Website gibt als Adresse nämlich Hannover an. Der Server steht laut *WhatRoute* in Karlsruhe.

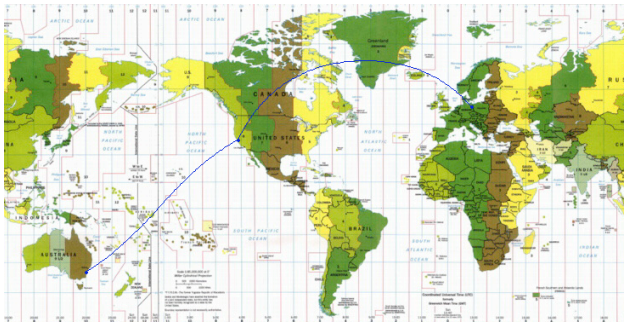

Abbildung 1: Der Weg von der HU-Berlin
zu 211.208.147.33 mit *WhatRoute*

Zu beachten ist auch, dass der Bayes-Spam-Filter nicht gegriffen hat, das Feld *X-Spam-Status* hat den Wert *No*. Automatischen Filtern ist somit nicht in jedem Fall zu trauen.

Bei der Mail handelt es sich um einen weiteren Versuch, Malware zu installieren. Der Heise-Verlag beschreibt den Vorfall unter [He04].

Kompetenzen Klassen 11-13 (Grundkurs)

Merkmale: Quelltext
Kompetenz: SuS überprüfen die Echtheit einer Mail anhand des Quelltextes
Aufgabe: Geeignete Untersuchungsgegenstände sind Phishing-Mails, da deren Autoren darauf angewiesen sind, mit gefälschten Hyperlinks oder Formularen vorzugehen. Der Abdruck eines E-Mail-Quelltextes kann jedoch schnell sehr umfangreich wird, so dass an dieser Stelle darauf verzichtet werden soll. Informaionten und Material gibt es u.a. unter [BSI05a], [Eb05], [Hu05] und [Zi04].
Kommentar: Da die Bedrohung durch Phishing-Mails in den kommenden Jahren vermutlich zunehemen wird, sollte die Analyse von E-Mail-Quelltext zum Grundwissen eines mündigen Internet-Nutzers gehören. Zwar kann diese Thema aufgrund seiner Zusammenhänge mit HTML erst in der Oberstufe behandelt werden, allerdings ist erst die Altergruppe für Phiser interessant, in der Menschen ein eigenes Bankkonto haben. Mit steigendem Alter nehmen die Bedrohungen zu. Die Kompetenzen, diese Bedrohungen zu durchschauen sollten es ebenso.

Kompetenzen Klassen 11-13 (Leistungskurs)

Kompetenz: SuS führen eine Client-Server-Kommunikation auf Grundlage des SMTP-Protokolls durch.

Aufgabe: Verschicken Sie an Ihren Lehrer über den Schulmailserver eine Mail mit ihrer Absendeadresse. Benutzen Sie dazu eine telnet-Verbindung über Port 23.
Kommentar: Das SMTP-Protokoll wird in RFC 821 beschrieben, einzusehen bei [Po82]. Das folgende Beispiel ist entnommen aus [BSI05b] und muss an die entsprechende Server-Umgebung angepasst werden.

220 mail.example.com ESMTP

EHLO mail.example.org

250-mail.example.com Hello **mail.example.org**

[192.0.2.17] 250-SIZE 250 PIPELINING

MAIL FROM:<absender@example.org>

250 OK

RCPT TO:<empfaenger@example.com>

250 Accepted

RCPT TO:<person@example.com>

250 Accepted

DATA

354 Enter message, ending with „.“ on a line by itself...*header* und *body*....**220 OK**

QUIT

221 mail.example.com closing connection

Kommentar: Mit dieser Aufgabe wird auf eine Analyse konkreter E-Mails verzichtet und auf die allgemeine Struktur des E-Mail-Verkehrs eingegangen. Die Fragen, wie es möglich ist, E-Mails zu fälschen, lässt sich aus dem SMTP-Protokoll ableiten, wobei der Augenmerk vor allem auf die Aspekte gelegt werden sollte, was dort alles *nicht* gefordert wird. Der Einblick in den Aufbau einer Client/Server-Verbindung in Kombination mit dem Hinweis, dass E-Mail-Clients genau das und nicht mehr machen, vermittelt einen Blick hinter die Kulissen des Internet und verdeutlicht zusätzlich die Trennung der Netz-Architektur von den bunten Frontends der Benutzerprogramme.

Quellen

[BSI05a] Bundesamt für Sicherheit in der Informationstechnik: *Passwort-Fischer.* Internet (03.06.2005) http://www.bsi-fuer-buerger.de/abzocker/05_08.htm

[BSI05b] Bundesamt für Sicherheit in der Informationstechnik: *Antispam-Strategien. Unerwünschte E-Mails erkennen und abwehren.* Internet (03.06.2005): http://www.bsi.bund.de/literat/studien/antispam/antispam.pdf

[SB05] Statistsiches Bundesamt: *Kommunikation via E-Mail immer beliebter. Pressemitteilung vom 13.05.2005.* Internet (03.06.2005): http://www.destatis.de/presse/deutsch/pm2005/p2210024.htm

[Eb05] Ebay (Hrsg.): *Phishing E-Mmails.* Internet (03.06.2005) http://pages.ebay.de/education/spooftutorial/

[He04] Heise-Verlag: *Spammer verschicken gefälschte Heise-Newsletter [Update].* Internet (03.06.2005): http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/59136

[Hu05] Huth, Peter: *Phishing - Trickbetrug per E-Mail.* Internet (03.06.2005) http://www.peterhuth.de/trick03.php

[Ka05] Kantel, Gabriele/ Kantel, Jörg (2005): *Nigeria Connection*. Internet (03.06.2005): http://server-wg.de:8080/nigeria/muzenda_simon.html

[Po82] Postel, John (1982): *RFC* 82. *Simple Mail Transfer Protocol*. Internet (03.06.2005): http://www.faqs.org/rfcs/rfc821.html

[Zi02] Ziemann, Frank (2002): *Nigeria Connection. E-Mails mit kriminellen Absichten.* Internet (03.06.2005): http://www.tu-berlin.de/www/software/hoax/419.shtml

[Zi04] Ziemann, Frank (2004): *Identity Theft - Datendiebstahl. E-Mails täuschen zwecks Datenklau falsche Links vor.* Internet (03.06.2005): http://www.tu-berlin.de/www/software/hoax/idtheft.shtml