UNIVERSITÄT
KOBLENZ · LANDAU
Institut für Wirtschafts-
und Verwaltungsinformatik

FB 4
Informatik

E-Mail-Forensik – IP-Adressen und ihre Zuordnung zu Internet-Teilnehmern und ihren Standorten

öffentliche Version 05.05.2010

Rüdiger Grimm
Daniel Pähler

Nr. 5/2010

Arbeitsberichte aus dem Fachbereich Informatik

Universität Koblenz-Landau • Campus Koblenz • Universitätsstraße 1 • 56070 Koblenz
Telefon +49 261 287-0 • http://www.uni-koblenz.de

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Zöbel

Kontaktdaten der Verfasser

Rüdiger Grimm, Daniel Pähler
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
EMail: grimm@uni-koblenz.de, tulkas@uni-koblenz.de

E-Mail-Forensik – IP-Adressen und ihre Zuordnung zu Internet-Teilnehmern und ihren Standorten

Rüdiger Grimm
Daniel Pähler
Öffentliche Version 7.5.2010
(ohne Kap. 10 und 11)

Zusammenfassung

Wesentliches Element des weltweiten Internets bildet der Adressraum der IP-Adressen, die den am Internet teilnehmenden Geräten („IP-Hosts“) zugewiesen sind. IP-Adressen (der Version 4) bestehen aus vier Zahlen zwischen 0 und 255 und repräsentieren viermal acht Bits, mit welchen insgesamt über vier Milliarden Adressen unterschieden werden können. Die zentrale Organisation IANA vergibt an fünf regionale Adressregistraturen Adressräume, welche sie an lokale Registraturen, Telecomanbieter und Internet-Service-Provider weiter verteilen. Diese Adressverteilung ist relativ stabil. Diese Zuordnung ist öffentlich zugänglich über so genannte *whois*-Abfragen aus Datenbanken der regionalen Registraturen.

Die Internet-Service-Provider (ISP) vergeben IP-Adressen an ihre Nutzer. Die Zuordnung wird teilweise statisch mit langfristiger Bindung vorgenommen und teilweise dynamisch nur für die Dauer einer Datenverbindung. Die dynamische Adressverwaltung erlaubt es Internet-Service-Providern, mehr Nutzer zu bedienen, als ihr Adressraum an verschiedenen IP-Adressen zulässt, da die Adressen von Geräten, die aus dem Internet ausscheiden, nicht wie bei der statischen Vergabe frei gehalten werden müssen, sondern an sich neu mit dem ISP verbindende Geräte vergeben werden können. In internen Tabellen verwalten die Internet-Service-Provider die Zuordnung von IP-Adressen zu den konkreten Anschlüssen ihrer Nutzer, außerdem protokollieren sie, welcher Anschluss wann welche IP-Adresse hatte . Diese Daten sind öffentlich nicht zugänglich, sondern müssen bei Bedarf mit gesetzlich geregelten Einschränkungen (Datenschutz) erfragt werden.

E-Mails werden von Mailserver zu Mailserver („Store and Forward“) von ihrem Ausgangsort zu ihrem Zielort transportiert. Normalerweise vermerkt jeder Mailserver den Durchgang einer E-Mail in einer „Received“-Kopfzeile, die er der E-Mail hinzufügt. Daher trägt jede E-Mail ihre Wegspur durch das Mailserver-Netz des Internets in der Liste ihrer „Received“-Kopfzeilen mit sich bis zum Empfänger. Dieser kann sie durch erweiterte Ansicht der Kopfzeilen zur Kenntnis nehmen und auswerten.

Wie die Internet-Service-Provider speichern auch die E-Mail-Services den Zugang ihrer E-Mail-Nutzer mit ihren IP-Adressen für die Dauer einer Sitzung, in der sie E-Mails abrufen und versenden. Diese Einwahldaten sind ebenfalls nicht öffentlich zugänglich, sondern müssen den entsprechenden Einschränkungen erfragt werden.

Die „Received“-Kopfzeile ist das wichtigste Werkzeug zur Identifikation eines Weges einer E-Mail zurück bis zu ihrer Abgabe durch den absendenden Nutzer:

Die IP-Adresse der untersten „Received“-Kopfzeile ist dem tatsächlichen Absender durch seinen Internet-Service-Provider für den Moment der Abgabe der E-Mail zugeordnet worden.

Unter gewissen Einschränkungen ist es möglich, die IP-Adresse des Absenders diesem auch geographisch zuzuordnen. Dazu nutzt der Rechercheur eine öffentlich verfügbare *whois*-Datenbankabfrage bei einer Regionalen Internet-Registratur: dort erfährt er die geographische Adresse des Internet-Service-Providers des Absenders. Schließlich vermutet der Rechercheur

die geographische Lage des Absenders in der Nähe (mindestens im selben Land, oft in engerer regionaler Umgebung) des Internet-Service-Providers.

Die Einschränkungen dieser Zuordnung liegen in folgenden Punkten:

1. Die geographische Nähe zum Internet-Service-Provider beruht auf keiner sensorischen Ortung des Absenders sondern auf einer Vermutung über eine gängige betriebliche Praxis, dass die Internet-Service-Provider ihre Kunden nicht in allzu großer physikalischer und rechtlicher Entfernung bedienen.
2. Die *whois*-Abfrage liefert die gegenwärtige Zuordnung einer IP-Adresse zu ihrem Internet-Service-Provider. Die Zuordnung der Adressräume ist zeitlich ziemlich stabil, so dass eine Überprüfung in die Vergangenheit nur in Fällen begründeten Zweifels erforderlich ist. Die erweiterte „*whois –B*“-Abfrage liefert die zugehörigen Zeitstempel.
3. Ein Absender könnte sich über einen VPN-Tunnel ins Internet eingewählt haben: die Spur müsste dann weiter über den VPN-Server verfolgt werden.
4. Ein Absender könnte sich zuvor in ein anderes Netz eingeloggt haben (Technik der Bot-Netze): die Spur müsste dann weiter über den Login-Server verfolgt werden.
5. Der Absender könnte seine E-Mail per *telnet* manuell abgesendet haben: das macht eine weitere Spurenverfolgung über den *telnet*-Ursprung erforderlich (s.u. Anhang C).
6. Jeder Lieferant einer E-Mail könnte gefälschte „Received“-Kopfzeilen vorschalten und dadurch eine andere Vorgeschichte der E-Mail vortäuschen. Das ist gängige Technik von manipulativen SPAM-Programmen und kann mit *telnet* direkt simuliert werden.
7. Der E-Mail-Service kann falsche E-Mails und Login-Daten vorspiegeln. Das ginge nur aufgrund eines *Insider*-Angriffs oder eines externen *Hacks*.

Die ersten beiden Punkte der eingeschränkten geographischen und zeitlichen Zuordnung müssen in jedem Fall bedacht werden, lassen aber eine grobe geographische Zuordnung durchaus zu. Die anderen Punkte beziehen sich auf spezielle Angriffe, Fälschungen und Unterdrückungen, deren Möglichkeit in jedem Einzelfall gesondert zu untersuchen ist. Für unbefangene Nutzer des Internets kommen sie nicht in Betracht, da sie großes technisches Wissen und einigen Aufwand bedeuten. Manipulationen eines E-Mail-Service-Providers setzen einen Sicherheitseinbruch (der in letzter Zeit nicht bekannt geworden ist) oder die Mitwirkung von Insidern voraus.

Die folgenden Kapitel dienen der genaueren Erläuterung der einzelnen Methoden und ihrer Grenzen zur Identifikation der Herkunft von E-Mail im Internet.

1. Internet-Routing und Datentransport

Das Ziel von Computernetzen ist der Austausch von Daten zwischen so genannten „Hosts“ (deutsch: Netzknoten). Typische Hosts sind Laptops, PCs, Server, Smartphones, Drucker, usw. Der Datenaustausch findet zwischen Ein- und Ausgabebuchsen der Hosts über elektronische Drähte (LAN) oder elektromagnetische Ausstrahlung durch die Luft (WLAN, GSM, UMTS) statt und wird über interne Programme in den Hosts gesteuert.

Das Internet stellt keine eigene Netztechnologie dar, sondern ein Austauschformat *zwischen* Netztechnologien: daher der Name *Inter*net. Das Internet ist ein gemeinsamer Standard für die Formatierung von Datenpaketen, für Austauschregeln dieser Datenpakete und für die Adressierung der Sender und Empfänger. Der Oberbegriff dieses Standards ist „IP – Internet Protokoll“. Die bestehenden lokalen Netze, zwischen denen das IP vermittelt, beruhen auf so unterschiedlichen Technologien wie Ethernet, Fast Ethernet, Token Ring, X.25, FDDI, u.v.a.m. Jedes Gerät, das in seinem lokalen Netz Daten senden und empfangen kann, wird dadurch ein „IP-Host“, d.h. eine im gesamten Internet erreichbare Stelle, dass er eine *weltweit eindeutige IP-Adresse* zugewiesen bekommt[1] und seine Dateninhalte („Payload“) als IP-Paket bzw. als Menge von IP-Paketen formatiert. IP-Pakete sind i.d.R. jeweils bis zu 1.500 Bytes lang, um in Ethernet-Frames zu passen. An der Grenze zwischen verschiedenen lokalen Netzen werden die Pakete ausschließlich nach den IP-Regeln ausgetauscht. Insofern bildet IP die Weltsprache des Internet, in die und aus der jede andere Netztechnologie übersetzen kann.

2. IP-Adressraum

IP-Pakete enthalten in ihrem Kopfteil jeweils eine Absenderadresse des sendenden IP-Hosts und eine Empfängeradresse des intendierten Ziel-IP-Hosts. Zentrales Element des Weltstandards „Internet“ ist der IP-Adressraum. Es gibt hierfür zwei Formate, das ältere Format ist die Version 4 („IPv4“) und wird im weit überwiegenden Teil des gesamten Internets verwendet. Das neuere Format ist die Version 6 („IPv6“). Ein wesentlicher Unterschied zwischen den Versionen 4 und 6 besteht in dem erheblich erweiterten Adressraum der Version 6 gegenüber der Version 4. Während Adressen der Version 4 32 Bits umfassen und damit $2^{32} \sim 4.3 * 10^9$verschiedene Adressen zum Ausdruck bringen kann, umfassen Adressen der Version 6 128 Bits für $2^{128} \sim 3 * 10^{38}$verschiedene Adressen. Aufgrund seiner geringen praktischen Relevanz wird IPv6 im Folgenden nicht weiter betrachtet.IPv4-Adressen werden in vier Zahlen zwischen 0 und 255, getrennt mit Punkten, geschrieben, zum Beispiel 127.0.0.1, 141.26.66.69, 212.227.126.186 und 10.79.128.2. Sie bilden damit den gesamten Adressraum von zweiunddreißig Bits ab, indem jede Zahl zwischen 0 und 255 genau eine Dualzahl aus 8 Bits repräsentiert (2^8=256).

IP-Adressen müssen (in der Regel) weltweit eindeutig sein, da es ja möglich sein soll, von jedem Internet-Host der Welt jeden anderen Internet-Host der Welt zu adressieren. Deshalb werden IP-Adressen IP-Hosts (Geräten) durch ISP, die typischerweise über eine gewisse Menge an IP-Adressen verfügen, *zugewiesen*. Der ISP, der die Zuweisung vornimmt, und der die zugehörigen Adressen verwaltet, kennt die Geräte und in aller Regel auch ihre Zuordnung zu natürlichen bzw. juristischen Personen.

Um die globale Weiterleitung von Datenpaketen zu vereinfachen, ist der gesamte IP-Adressraum ist in so genannte Subnetz-Adressräume aufgeteilt. *Jeder* IP-Host, der ein Datenpaket empfängt, trifft anhand der IP-Adresse des Pakets regelmäßig folgende Entscheidung:

---

1 Zur Einsparung von IP-Adressen wird von manchen Lokalen Netzen das sogenannte Source-NAT (Network Address Translation of Source IP Addresses) eingesetzt, indem mehreren privaten IP-Adressen nach außen nur eine öffentliche IP-Adresse zugeordnet wird)

- Ist die IP-Adresse meine eigene, d.h. ist das Paket für mich bestimmt? Wenn ja, dann behalte ich das Paket, sonst sende ich es an den zentralen für die Weiterleitung bestimmten IP-Host (Router) für mein Subnetz.

Diejenigen IP-Hosts, die mehrere Ausgangsbuchsen haben, die mit verschiedenen IP-Hosts verbunden sind, können eine differenziertere Entscheidung treffen:

1. Ist die IP-Adresse meine eigene, d.h. ist das Paket für mich bestimmt? Wenn ja, dann behalte ich das Paket, sonst:
2. gehört die IP-Adresse zu einem Subnetz, an das ich angeschlossen bin? Wenn ja, dann sende ich es direkt an den entsprechenden IP-Host, sonst:
3. gehört die IP-Adresse in ein fremdes Subnetz, zu dessen zentralen Router ich eine direkte Verbindung habe? Wenn ja, dann schicke ich es dorthin, sonst
4. schicke ich das Paket an einen von mir fest eingestellten zentralen Router, von dem ich hoffe, dass er das Paket richtig weiterverschicken kann.

Alle Subnetze verfügen über mindestens einen IP-Host, dessen Aufgabe das Routing zu anderen Netzen ist. Sehr große Router, wie beispielsweise für Universitätscampi oder für ganze Telecom-Netze, können auf diesem Wege mehrere hundert oder tausend andere Router ansteuern. Kleine Endgeräte dagegen begnügen sich mit einem einzigen Anschluss an einen zentralen Router. Subnetze, die noch nicht an das Internet angeschlossen sind, können sich dadurch an das gesamte Internet anschließen, dass sie einen bisher noch nicht belegten IP-Adressraum zugewiesen bekommen (s.u. IP-Adressvergabe), an einen externen IP-Router angeschlossen werden und zunächst alle nicht für das eigene Subnetz bestimmten Pakete über diesen „erfahrenen“ Router leiten. Dieser muss im Gegenzug wissen, zu welchem Subnetz der neu zugewiesene Adressraum gehört und wie er es erreichen kann.

Um die Entscheidung des Routers, welches Datenpaket wohin weitergeleitet wird, zu erleichtern, sind alle IP-Adressen in zwei Anteile aufgeteilt, der erste Anteil adressiert ein Subnetz, der zweite Anteil adressiert einen IP-Host innerhalb dieses Subnetzes. Dem Universitätscampus Koblenz ist beispielsweise die Subnetzadresse 141.26.-.- zugewiesen, so dass alle 256x256=65.536 IP-Adressen zwischen 141.26.0.0 und 141.26.255.255 zum Uni-Campus Koblenz gehören und dort frei vergeben werden können. Anhand des Subnetz-Adressanteils einer IP-Adresse kann man den verantwortlichen Netzbetreiber eines IP-Hosts identifizieren.

Sorgfältig von *IP-Adressen* zu unterscheiden sind die so genannten *Domain-Namen*. Domain-Namen wie „mercedes-benz.com“, „stanford.edu“, „mail.uni-koblenz.de“, sind sowohl maschinen-, als auch vor allem menschenlesbare Formen von IP-Adressen, bzw. IP-Adressräumen. Jedem Domain-Namen entspricht eine IP-Adresse, ein Bereich von IP-Adressen oder zumindest ein anderer Domain-Name, der seinerseits einer IP-Adresse zugewiesen werden kann. Die Zuordnung von Domain-Namen zu IP-Adressen und umgekehrt wird vom so genannten Domain-Name-Service (DNS) vorgenommen und kann über ein eigenes DNS-Protokoll von jedem Teilnehmer des Internet abgefragt werden. Unter Unix fragt man beispielsweise die zu einem Domain-Namen zugehörigen Adressen durch den *host*-Befehl ab:

```
> host stanford.edu
stanford.edu has address 171.67.216.9
stanford.edu has address 171.67.216.3
stanford.edu has address 171.67.216.4
stanford.edu has address 171.67.216.7
stanford.edu has address 171.67.216.8
stanford.edu mail is handled by 20 mx6.stanford.edu.
stanford.edu mail is handled by 20 mx1.stanford.edu.
```

```
stanford.edu mail is handled by 20 mx2.stanford.edu.
stanford.edu mail is handled by 20 mx3.stanford.edu.
stanford.edu mail is handled by 20 mx4.stanford.edu.
stanford.edu mail is handled by 20 mx5.stanford.edu.
```

3. IP-Adressvergabe durch IANA und RIR (Regional Internet Registry)

Während die Standardisierung des Internets einschließlich der Adressformate zentralisiert ist, ist die Betriebsorganisation des Internets dezentralisiert. Die Adressvergabe ist hierarchisch baumartig „von oben nach unten“ delegiert. Die zentrale Stelle des Internet ist die IANA – Internet Assigned Numbers Authority (http://www.iana.org/) mit den folgenden drei zentralen Verwaltungsaufgaben:

1. Vergabe von Domain-Namen
2. Vergabe von IP-Adressen
3. Verwaltung von Protokollen (Austauschregeln für Daten in Internetanwendungen)

Hier von Interesse ist der zweite Punkt, die Vergabe von IP-Adressen. IANA selbst vergibt fünf Bereiche für Subnetzadressen an fünf so genannte regionale Internet-Registraturen (RIR), die den großen Regionen der Erde zugeordnet sind, und zwar an

- AfriNIC– Afrika
- APNIC–Asien/Pazifik
- ARIN–Nordamerika
- LACNIC–Lateinamerika sowie einige karibische Inseln
- RIPE NCC–Europa, mittlerer Osten und Zentralasien

Diese vergeben die Subnetzadressen ihres Bereichs an *lokale Internet-Registraturen* (LIR) oder an *nationale Internet-Registraturen* (NIR) oder auch – wie die LIRs und NIRs – direkt an *Internet-Service-Provider* (ISP) oder an große Telecoms für ihre eigenen internen Netze. Die Deutsche Telekom und Arcor sind beispielsweise sowohl Internet-Sevice-Provider für ihre Kunden, denen sie Zugang zum Internet verschaffen, als auch Betreiber eigener (sehr großer) IP-Subnetze. Internet-Service-Provider schließlich bieten Endnutzern den Zugang zum Internet, indem sie deren Geräten IP-Adressen aus dem Subnetz-Adressraum zuweisen und das Routing für ihre IP-Pakete übernehmen, d.h. ihnen einen physikalischen Netzanschluss schalten. Alle ISPs sind bei ihren RIRs mit ihren Adressräumen und ihren juristischen Kontaktdaten registriert, dazu gehören Firmenadresse und Adressen von technisch und administrativ verantwortlichen Personen. Für die Deutsche Telekom als ISP und LIR hält der zuständige RIR „RIPE NCC“ beispielsweise unter anderen folgenden Eintrag in der Datenbank vor (*whois*-Abfrage von RIPE NCC, Genaueres dazu s.u.):

```
inetnum:  79.192.0.0 - 79.244.191.255
netname:  DTAG-DIAL24
descr:    Deutsche Telekom AG
country:  DE
admin-c:  DTIP
tech-c:   DTST
status:   ASSIGNED PA "status:" definitions
remarks:
*************************************************************
remarks: Abuse Contact: http://www.t-com.de/ip-abuse in case of Spam,
remarks: Hack Attacks, Illegal Activity, Violation, Scans, Probes, etc.
*************************************************************
```

```
mnt-by:   DTAG-NIC
changed:  lir.nic@t-com.net 20070607
source:   RIPE

person:   DTAG Global IP-Addressing
address:  Deutsche Telekom AG
address:  D-90492 Nuernberg
address:  Germany
phone:    +49 180 5334332
fax-no:   +49 180 5334252
e-mail:   ripe.dtip@telekom.de
nic-hdl:  DTIP
mnt-by:   DTAG-NIC
changed:  ripe.dtip@telekom.de 20031013
source:   RIPE

person:   Security Team
address:  Deutsche Telekom AG
address:  Germany
phone:    +49 180 5334332
fax-no:   +49 180 5334252
e-mail:   abuse@t-ipnet.de
nic-hdl:  DTST
mnt-by:   DTAG-NIC
changed:  abuse@t-ipnet.de 20030210
source:   RIPE

% Information related to '79.192.0.0/10AS3320'

route:    79.192.0.0/10
descr:    Deutsche Telekom AG, Internet service provider
origin:   AS3320
member-of: AS3320:RS-PA-TELEKOM
mnt-by:   DTAG-RR
changed:  lir.nic@t-com.net 20070606
source:   RIPE
```

Die Deutsche Telekom vergibt IP-Adressen aus ihrem Adressraum an ihre Kunden, die sie natürlich kennt, deren Einloggzeiten sie beobachtet, abrechnet und nach deutschem Recht (Abrechnung bzw. TK-Überwachungsverordnung) für gesetzlich vorgeschriebene Fristen aufbewahrt. Da sie für ihre Kunden nicht nur Adressen zuweist, sondern auch das Routing über physikalische Leitungen übernimmt, zerlegt sie ihren Adressraum in geographisch sinnvolle kleine Einheiten, die sie in eigenen Datenbanken verwaltet. Der Zugang zu diesen internen Datenbanken ist nicht generell öffentlich, als Alternative können aber oftmals so genannte Geolokation-Dienste (s.u.) genutzt werden, zu denen unter anderem der öffentlich zugängliche Internetdienst „*whatismyipaddress.com*“ (Genaueres dazu s.u.) gehört, der beispielsweise einem privaten IP-Router in Süd-Darmstadt mit der IP-Adresse 79.199.12.110 die Region Darmstadt-Griesheim zuordnet (das ist vom Standort des Routers ca. 10 km entfernt).

Im Rahmen der Recherche zu einer IP-Adresse kann die verantwortliche Stelle, an die ein IANA-RIR die IP-Adresse vergeben hatte, über eine *whois*-Abfrage bei der zuständigen RIR und durch eine zusätzliche Abfrage *bei einem Geolokations-Dienst* festgestellt werden. Die auf die *whois*-Anfrage zurückgegebene geographische Adresse entspricht nicht dem Standort des IP-Hosts, sondern der verantwortlichen Stelle, die die IP-Adresse zur Verwaltung in ihrem Nutzerkreis übertragen bekommen hatte. Diese ist aber in der Regel im selben Staat wie der IP-Host, und oft (aber nicht immer) auch in derselben nationalen Region. Der Grund der geographischen Nähe zwischen IP-Host und Verwaltungsstelle liegt darin, dass die

Verwaltungsstelle alle Pakete für den Host über physische Leitungen möglichst effizient auf kurzen Wegen und Routern organisieren muss.

Es ist wichtig darauf hinzuweisen, dass die zu vermutende geographische Nähe eines IP-Hosts zur Adresse des zugehörigen ISP bei einer *whois*- oder *Geolokations-Dienst*-Abfrage nicht das Ergebnis einer Ortung durch Sensoren ist, und noch nicht einmal technisch zwingend ist, sondern dass diese Vermutung aufgrund betrieblicher Abläufe und Regeln nahegelegt wird: Es gibt keinen ISP, der über weiträumige, womöglich fremde Netze hinweg, IP-Routing zu seinen Nutzern organisiert. Die geographische Zuordnung des ISP-Standorts bei einer *whois*-Abfrage beruht allein auf der Auswertung einer Adressinformation in einer Datenbank, die im Anmeldeprozess als Nutzer/Kunde/ISP formuliert worden war. Diese geographische Zuordnung ist daher nur so genau wie die Sorgfalt der Datenbankpflege durch den RIR und ISP. Beispielsweise wird der Standort des ISP des Universitätscampus Koblenz im RIPE NCC immer noch mit Koblenz-Rheinau angegeben, obwohl der Campus vor fünf Jahren einige Kilometer nordwestlich nach Koblenz-Metternich umgezogen war. Die RIR-Datenpflege ist insgesamt als sehr sorgfältig anzusehen, da die IANA und die fünf RIRs eine abgestimmte Datenpflege-Policy einhalten und diese gegenüber ihren LIRs und ISPs weltweit durchsetzen.

Wiederum zu unterscheiden davon ist das Zuordnungsverfahren von Domain-Namen. Die IANA hat die sog. „Top-Level-Domains“ festgelegt, dazu gehören u.a., .com, .edu. .org. .net, sowie alle zweistelligen Ländercodes der Welt, z.B. .de, .at, .uk und .ru. Den Top-Level-Domains sind Organisationen zugeordnet, die die untergeordneten Domain-Namen vergeben, für den Bereich „.de“ ist das die DENIC eG (http://www.denic.de).

4. IP-Adressvergabe durch ISP (Internet Service Provider)

Ein ISP (Internet Service Provider) verteilt die IP-Adressen des ihm vom RIR, LIR oder NIR zugewiesenen IP-Adressraumes an seine Nutzer. Es gibt dazu drei Verfahren

1. Statische Zuweisung: Jedem IP-Host wird langfristig eine IP-Adresse zugewiesen, die in dieser Zeit ausschließlich von ihm genutzt wird (Abfrage durch einen Directory-Client, bei SUN-Network Information System z.B. über „*ypcat hosts*“).
2. Dynamische Zuweisung: Jedem IP-Host wird über das DHCP-Protokoll dynamisch in dem Moment eine IP-Adresse zugewiesen, in dem er sich in das Netz einwählt, und in dem Moment wieder entzogen, in dem er sich vom dem Netz abwählt (DHCP-Logging). Listen über diese Zuordnungen werden mit begrenzten Fristen gespeichert und sind öffentlich nicht zugänglich.
3. Unsichtbare („private“) Adressen, ebenfalls dynamisch zugewiesen: Der ISP vergibt an die Teilnehmer Adressen, die nicht nach außen adressierbar sind, sondern die der ISP nur zur internen Adressierung der Teilnehmer verwendet. Den externen Datenverkehr dieser Teilnehmer leitet der ISP über einen zentralen „Proxy“ und gibt dabei als Absenderadresse immer nur seine eigene IP-Adresse an. Die Umsetzung für die eigenen Teilnehmer regelt der ISP-Proxy über eine interne Umsetzungstabelle und nach außen unsichtbar. Hierfür bietet IANA ganze Adressräume an, nämlich die drei Bereiche 10.-.-.-, 172.16-31.-.-, und 192.168.-.-, siehe RFC 1918, http://www.ripe.net/db/rfc1918.html und ftp://ftp.ripe.net/rfc/rfc1918.txt. Zuordnungs-Loggings werden mit begrenzten Fristen aufgehoben.

Um genau festzustellen, welche IP-Adresse von welchem IP-Host zu welchem Zeitpunkt genutzt wurde, ist die entsprechende Information vom ISP einzuholen. Diese Auskunft unterliegt gesetzlichen Einschränkungen (Datenschutz). Bei einem Vergleich der untersten „Received“-Kopfzeile einer E-Mail mit der Absenderadresse (s.u.) kann man oft (aber nicht

immer zuverlässig, s.u.) darauf schließen, dass der Absender unter genau dieser IP-Adresse seinen E-Mail-Client beauftragt hatte, diese E-Mail aufzugeben.

5. Geolokation

„Geolokation“ bezeichnet das Zuordnen einer IP-Adresse zu dem Ort, an dem sie aktuell verwendet wird, wobei die Granularität dieser Information von der Nennung des Landes bis hin zur genauen Nennung von Straße und Hausnummer in einer bestimmten Stadt reichen kann. Die Nutzung eines Geolokations-Dienstes ist für die Betreiber bestimmter Internet-Dienste sinnvoll, so können z.B. Webseiten Werbung für Geschäfte in der Nähe des Webseiten-Besuchers schalten oder Online-Video-Portale wie YouTube sicherstellen, dass Besucher nur Videos zu sehen bekommen, die an ihrem jeweiligen Standort keine Urheberrechtsverletzung darstellen.

Die Anbieter solcher Dienste pflegen Datenbanken, in denen sie IP-Adressbereiche konkreten Orten zuordnen. Als Quelle für die eingepflegten Daten dienen oftmals *whois*- sowie DNS-Abfragen, aber auch weitergehende Informationen über die Netzwerkinfrastruktur der Internet Service Provider, denen die jeweiligen Adressbereiche gehören. Diese Informationen können von den ISP direkt erworben worden sein, sie können aber auch in Kooperation mit anderen Dienstleistern zusammengetragen worden sein, die z.B. in der Lage sind, die Anschriften ihrer Nutzer deren IP-Adressen zuzuordnen. Abhängig davon, welche Daten ein Geolokations-Diensteanbieter zu einem bestimmten Adressbereich zusammentragen konnte, schwankt nicht nur die Granularität der Angaben. Insbesondere kann auch nicht zweifellos von ihrer Korrektheit ausgegangen werden; so kann es vorkommen, dass der in *whois* verzeichnete Hauptsitz eines ISP als der Ort der IP-Adressen-Nutzung angezeigt wird.

Da die Mehrzahl aller Geolokations-Dienste kommerziell betrieben wird und präzisere Daten einen Wettbewerbsvorteil darstellen, wird das genaue Verfahren, welche Adressdaten woher bezogen wurden, in der Regel nicht öffentlich bekanntgegeben. Für eine nicht-kommerzielle Datenbank ist das Verfahren in (Moore, 2000) beschrieben. Vielen dieser Dienste ist allerdings gemein, dass sie kostenlose Probezugänge bieten, anhand derer die Qualität der Daten abgeschätzt werden kann. So können oftmals die Ergebnisse eines Dienstes durch Abfragen bei weiteren Diensten verifiziert werden – eine rechtlich verbindliche Aussage über den Standort erhält man aufgrund der ungenauen Datenquellen allerdings nie (Hoeren, 2007).

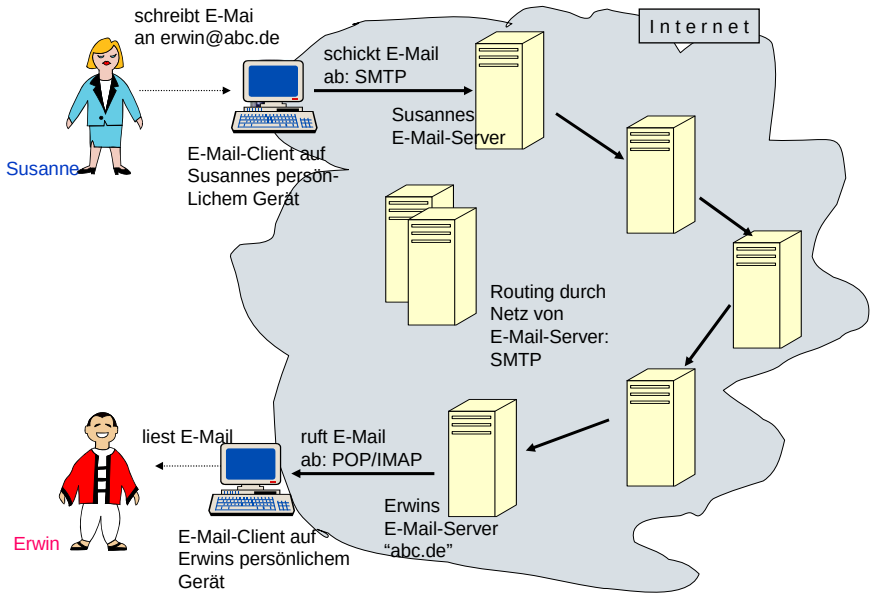
6. E-Mail-Routing

E-Mail ist eine auf weltweit anerkannten Standards basierende Anwendung des Internet. Jede E-Mail ist durchgängig im 8 Bit umfassenden ASCII-Zeichensatz kodiert, in den durch spezielle Kodierungsverfahren auch nicht-ASCII-Sonderzeichen sowie Binärdateien (Anhänge) eingebettet werden können. Eine E-Mail besteht aus einem Briefkopf und einem Briefkörper. Der Briefkörper enthält den Briefinhalt und ist ansonsten formatfrei. Der Briefkopf besteht aus Kopfzeilen mit vorgegebenem Format. Jede Kopfzeile beginnt mit einem Schlüsselwort (*From*, *To*, *Subject*, *Date*, *Received*, u.v.a.), gefolgt von einem Doppelpunkt und dem Inhalt der Kopfzeile. Die Kopfzeilen *From* und *To* enthalten die Absender-, bzw. Empfängeradresse.

E-Mail-Adressen entsprechen stets dem Format <Benutzername>@<Domain-Name>: *grimm@uni-koblenz.de*, *ruediger@rgrimm.de*, usw. Dem Domain-Namen ist durch den Domain Name Service (DNS) eine IP-Adresse des Mailservers zugeordnet, der die persönliche Mailbox, die zum Benutzernamen dieser Mailadresse gehört, verwaltet. Mailserver können zwei Aufgaben erfüllen: die Verwaltung der Mailboxen ihrer Nutzer, und

den Austausch von E-Mail mit anderen Mailservern. Server, über die E-Mails versendet werden können, heißen auch „Mail Transfer Agents (MTA)“. Das Verfahren zum Versenden von E-Mail an andere MTAs heißt „Simple Mail Transfer Protocol (SMTP)“.

Abb.: Store-and-Forward-Routing von E-Mail mit SMTP



Die Aufgabe eines Mail-Client (wie zum Beispiel *Thunderbird*, oder wie bei *Google Mail* und *Yahoo!* in einem Mailportal eines Webmailers integriert) ist es nun, bei einer neu geschriebenen E-Mail den Domainnamen des Empfängers zu analysieren und die E-Mail entweder direkt an den Mailserver des Empfängers zu schicken, sofern er einen direkten E-Mail-Verbindung zu diesem aufbauen kann, oder zumindest zu einem anderen Mail-Server, der „näher“ am Empfänger liegt als er selbst. Auf diese Weise wandern E-Mails von Mailserver zu Mailserver, „hop-by-hop“ dem eigentlichen Empfänger-Mailserver entgegen. Der letzte Mailserver, der als Domain-Namen gerade den Domainnamen der Empfänger-Mailadresse hat, erkennt, dass er die letzte Station ist, prüft, ob er den zugehörigen Benutzernamen kennt und legt im positiven Falle die empfangene E-Mail in das elektronische Postfach des Empfängers, das er ja lokal verwaltet. Andernfalls sendet er eine „Nichtzustellungsfehlermeldung“ an den Absender zurück. Diese Form des „Store-and-Forward“ von E-Mail über mehrere MTA-Stationen hinweg wird durch einen eigenen Routing-Algorithmus bestimmt, den jeder MTA-Verwalter für sich festlegt. Die Wahl des Routing-Algorithmus ist den Verwaltern freigestellt, allerdings müssen sie darauf achten, dass keine Schleifen entstehen.

Die E-Mail ist zugestellt, wenn sie am E-Mail-Server mit dem Domain-Namen des Empfängers ankommt, auch wenn der Empfänger selbst gar nicht online ist. Der Benutzer kann sich später bei dem E-Mail-Server anmelden und dann über ein spezielles, von SMTP unterschiedliches Verfahren (POP oder IMAP) die Mail mit seinem Mail-Client abrufen, wobei der Client die Wahl hat, ob dadurch die E-Mail vom Server gelöscht wird oder dort gespeichert bleibt.

Jeder MTA, der eine E-Mail annimmt, vermerkt dies in einer eigenen „Received“-Kopfzeile und fügt diese vor die zuletzt erzeugte „Received“-Kopfzeile in den Briefkopf ein, wenn er

die E-Mail empfängt. Dadurch wird die Spur des Store-and-Forward-Weges durch das MTA-Netz des Internets in der E-Mail selbst festgehalten.

7. Die „Received"-Kopfzeile in E-Mail (RFC 822) und ihre geographische Zuordnung

Die „Received"-Kopfzeile wird vom Weiterleitungs-Server des SMTP-Mailsystems (MTA) vor die zuletzt geschriebene „Received"-Kopfzeile hinzugefügt. Zur Rekonstruktion des Weges einer E-Mail durch das Weiterleitungssystem des E-Mailsystems im Internet liest man die „Received"-Kopfzeilen also von unten nach oben.

Die „Received"-Kopfzeile enthält neben einigen Erläuterungen und Kommentaren im Wesentlichen die Information, von welchem vorherigen MTA („from") der hier protokollierende MTA („by") die vorliegende Mail mit welchem Protokoll („with") empfangen hat, und die Empfängeradresse für die sie zuständig ist („for"), sowie die Uhrzeit in der Zeitzone des empfangenden MTA. Die MTAs werden (soweit möglich) mit ihren Domain-Namen und ihrer IP-Adresse bezeichnet:

```
from deliver.uni-koblenz.de (deliver.uni-koblenz.de [141.26.64.15])
by mx.kundenserver.de (node=mxeu3) with ESMTP (Nemesis) id 0MKqIe-
1Lq6Ur2NLT-00018c for ruediger@rgrimm.de; Sat, 04 Apr 2009 16:05:21
+0200
```

Außerdem vermerken einige MTAs Zusatzinformationen in nicht durch den Standardabgedeckten, typischerweise mit einem „X" beginnenden Kopfzeilen. So sagt z.B. „X-CHKRCPT" aus, dass der Absender auf Plausibilität und Berechtigung geprüft wurde:

```
X-CHKRCPT: Envelopesender vrfy grimm@uni-koblenz.de
```

„X-Greylist" zeigt, dass bei einem MTA das so genannte „Greylisting"-Verfahren als Schutz vor Spam-Mails eingesetzt wurde. Bei diesem Verfahren werden bei eingehenden E-Mails zunächst die IP-Adresse des sendenden MTA, die E-Mail-Adresse des Absenders und die E-Mail-Adresse des Adressaten daraufhin überprüft, ob sie in dieser Kombination schon einmal vorgekommen sind. Ist dies der Fall, wird die E-Mail sofort weitergeleitet. Anderenfalls wird dem zustellenden MTA eine Fehlermeldung mitgeteilt und die E-Mail verworfen. Standardkonforme MTAs versuchen (im Gegensatz zu den meisten Spam-Versand-Programmen) nach einiger Zeit, die E-Mail erneut zuzustellen; dieser zweite Versuch wird nun vom empfangenden MTA akzeptiert. Dass eine Mail zunächst verworfen, dann beim zweiten Zustellversuch aber akzeptiert wurde, ist an der folgenden Kopfzeile zu sehen:

```
X-Greylist: delayed 393 seconds by postgrey-1.32 at deliver; Mon, 23 Feb
2009 01:53:40 CET
```

Schließlich signieren einige MTAs die komplette E-Mail samt Kopfzeilen, so dass Hinzufügungen (außer an oberster Stelle) oder Veränderungen durch fremde Autoren entdeckt werden können. Die zugehörige Signatur heißt „Domain Key Signature", die signierte Mail ist dann eine „Domain Key Identified Mail" (DKIM), das wird in Kap. 8 unten weiter ausgeführt.

```
DKIM-Signature:
v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=gamma;h=domainkey-
signature:received:received:message-id:date:from:to       :subject:mime-
version:content-type;bh=dhOdU7DNsgNSbynl2L2wVTZfslLyR8vGp9xqTfAlA5c=;b=h
bH492imkXoFQAGeml40BRXB1tTu5OG/FbRlcwKJh7nxIZWYOb9AyOU3PYHo/K299O 6xgdp9
E0L42jUCuXz+ZY+LyT6Nlc48J/vOI3XQgBm/e5RqWtY91lP82DL17vg0fZGjks skjPrPv5P
uwy00IrlXrVt+r8TUPOG4lMi1K2A=

DomainKey-Signature:
```

```
a=rsa-sha1;      c=nofws;      d=gmail.com;      s=gamma;      h=message-
id:date:from:to:subject:mime-version:content-type;  b=OGJ6QrpKlU6sc9to62L
CdSZw/75/gx+Ls8/kxo8IN0gtGVt0ru8DTI+XJwk+89/wnb  YHZW2giXt2EjV3IQSm3qEvNp
3UGKf9Nkib0/KqRo1wUyWAsd3UTPbHMOTlWpxyRmec+J  dMxhzyPxgPIV5Vcufdn54ZcUEwt
HYLn9we7wg=
```

Die IP-Adresse und der Domain-Name des „from“-Feldes einer „Received“-Kopfzeile gehören zu dem Sender der E-Mail in dem Augenblick, in dem der empfangende MTA, der die „Received“-Kopfzeile schreibt, die E-Mail von dem Sender unter dieser IP-Adresse annimmt. Der Sender kann hierbei ein anderer MTA, aber auch der Mail-Client des Absenders sein.

8. DomainKeys und DomainKeys Identified Mail Signatures

Im Mai 2007 wurde in RFC 4870 der Vorschlag zur Standardisierung des so genannten "DomainKeys"-Systems veröffentlicht, der bereits kurz danach (in RFC 4871) durch eine überarbeitete Version des vorgeschlagenen Standards namens "DomainKeys Identified Mail Signatures" (DKIM) überholt wurde. Beide Entwürfe verfolgen dieselben Ziele und unterscheiden sich nur in technischen Details.

Das Ziel von DomainKeys und DKIM war bzw. ist, durch das Signieren von E-Mails eine zusätzliche Authentizitätsprüfung zu ermöglichen. Hierzu werden digitale Signaturen verwendet, wie sie unter anderem auch beim Erstellen fortgeschrittener und qualifizierter elektronischen Signaturen gemäß SigG zum Einsatz kommen. Anders als bei diesen ist bei DomainKeys und DKIM allerdings nicht das Ziel, persönliche Unterschriften zu ersetzen und beispielsweise E-Mails so eindeutig ihrem Verfasser zuordenbar zu machen. Viel mehr signiert hier der MTA die E-Mail, der sie vom Nutzer in Empfang nimmt und darauf weitersendet. Der dabei verwendete private Schlüssel gehört nicht ihm exklusiv, sondern der Domain, der er angehört. Mittels DomainKeys/DKIM kann also unabstreitbar festgestellt werden, welche Domain dafür verantwortlich ist, eine E-Mail "in Umlauf" gebracht zu haben, sowie ob der Inhalt der E-Mail nachfolgend verändert wurde.

Das Ziel, das letztlich durch DomainKeys/DKIM angestrebt wird, ist die Vermeidung von SPAM- und Phishing-E-Mails. Dies kann wie folgt realisiert werden: ein MTA prüft beim Empfang der E-Mail zunächst, ob die Absender-Domain als bekannte Quelle von SPAM eingestuft wird. In diesem Fall leitet er die Mail nicht weiter, sondern verwirft sie oder legt sie in einem speziellen SPAM-Verzeichnis ab. Andernfalls kann er durch Prüfen der Signatur feststellen, ob die E-Mail wirklich von der angegebenen Domain stammt und die relevante "Received"-Kopfzeile keine Fälschung ist. Ist die Signatur valide, leitet er die E-Mail weiter.

Obwohl es nicht ihr vorrangiges Ziel ist, können die beiden Systeme auch in einem gewissen Maß zu Zwecken der E-Mail-Forensik verwendet werden: Die Signaturen sind wie erwähnt in "Received:"-Kopfzeilen eingebettet und erstrecken sich stets über den eigentlichen vom Nutzer verfassten Inhalt sowie alle der eigenen vorangegangenen "Received:"-Kopfzeilen. Der versendende MTA übernimmt also auch eine Gewähr dafür, dass die von ihm ergänzten Informationen wie der Versendezeitpunkt und (falls genannt) die IP-Adresse des Absenders korrekt sind und der Nutzer vorher authentifiziert wurde.

Technisch gesehen ist an DomainKeys/DKIM interessant, dass beide Systeme so konzipiert wurden, dass sie sich möglichst gut in vorhandene Infrastruktur einbetten lassen. So können die eingefügten Kopfzeilen von MTAs, die für keines der beiden Systeme konfiguriert wurden, ignoriert werden; auch in von Endnutzern verwendeten E-Mail-Programmen werden sie nicht angezeigt. Die zur Überprüfung der Signaturen notwendigen öffentlichen Schlüssel

werden nicht in Zertifikaten über eine PKI verteilt, sondern als Teil der für die jeweiligen Domains relevanten Einträge im DNS verbreitet.

Die Abfrage des öffentlichen Schlüssels über das DNS kann unter Unix auch über den *host*-Befehl realisiert werden, im Fall von Google Mail sieht dies wie folgt aus.

```
> host -t TXT gamma._domainkey.gmail.com

gamma._domainkey.gmail.com     descriptive     text     "k=rsa\;     t=y\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDIhyR3oItOy22ZOaBrIVe9m/iME3RqOJeas
ANSpg2YTHTYV+Xtp4xwf5gTjCmHQEMOs0qYu0FYiNQPQogJ2t0Mfx9zNu06rfRBDjiIU9tpx2T+
NGlWZ8qhbiLo5By8apJavLyqTLavyPSrvsx0B3YzC63T4Age2CDqZYA+OwSMWQIDAQAB"
```

9. Werkzeuge zur Verfolgung von Internet-Verkehr und E-Mail-Herkunft

9.1 Die E-Mail mit vollem Kopfzeilenausdruck

Die Kopfzeilen „From“, „To“ und „Date“ geben an, zu welchem Zeitpunkt („Date“) diese E-Mail vom Absender, der in der „From“-Adresse genannt ist, an den Empfänger, der in der „To“-Adresse genannt ist, abgesendet worden war. Zusätzlich zum „To“-Empfänger wird die E-Mail auch weitergeleitet an die Adressen, die in den „CC“ („Carbon Copy“)-Kopfzeilen genannt wird, sowie an sogenannte „BCC“ („Blind Carbon Copy“)-Empfänger, die aber ausdrücklich in keiner Kopfzeile genannt sind. Datum und Uhrzeit in der „Date“-Kopfzeile beziehen sich auf Abweichungen von der UTC (Universal Time Coordinated = Greenwich Mean Time), und zwar mit Minus nach Westen und mit Plus nach Osten.

9.2 Die Zeitangabe mit Zeitzonen in E-Mail-Kopfzeilen

11.42 -0700 entspricht der Ortszeit 11:42 an der Westküste Amerikas (British Columbia, Washington, Oregon, California): das sind 7 Stunden westlich von London, wird mit Pacific Standard Time (PST) bezeichnetund entspricht 18:42 UTC=GMT Ortszeit in London. Zudem entspricht diese Zeitangabe 20:42 +0200 Mitteleuropäischer Sommerzeit (MESZ) und 23:42 +0500 Pakistan Standard Time (PST).

In der „Date“-Kopfzeile steht die Zeitangabe aus Sicht des absendenden E-Mail-Clients. Die Zeitangaben in den „Received“-Kopfzeilen (s.u. Abschnitt 9.3) entsprechen der Sicht des jeweils empfangenden E-Mail-Servers.

9.3 Die „Received“*-Kopfzeile mit Absender, Empfänger und Datum*

Zwischen Absender („From“) und Empfänger („To“, bzw. „CC“ und „BCC“) werden E-Mails von Mailserver zu Mailserver („Store and Forward“) von ihrem Ausgangsort zu ihrem Zielort transportiert. Normalerweise vermerkt jeder Mailserver den Durchgang einer E-Mail in einer „Received“-Kopfzeile, die er der E-Mail hinzufügt. Daher trägt jede E-Mail ihre Wegspur durch das Mailserver-Netz des Internets in der Liste ihrer „Received“-Kopfzeilen mit sich bis zum Empfänger. Dieser kann sie durch erweiterte Ansicht der Kopfzeilen zur Kenntnis nehmen und auswerten (s.o. Kap. 7 über die „Received“-Kopfzeile).

Die unterste (d.h. früheste) „Received“-Kopfzeile trägt der erste Mailserver ein, bei dem der Nutzer die E-Mail aufgegeben hat. Dabei vermerkt der Mailerver die IP-Adresse des Clients, mit dem der Nutzer zu dem Mailserver Kontakt aufgenommen hat, sei es ein *Thunderbird*-Client oder ein *Browser*, mit dem er den Webmailer aufgerufen hat, sowie das Kommunikationsprotokoll, mit dem der Client ihn aufgerufen hat. *Die hier vermerkte IP-Adresse ist neben der E-Mail-Adresse des Absenders das erste Datum, das ein Rechercheur analysiert, um den Aufenthaltsort des Absenders festzustellen.*

Die „Received“-Kopfzeilen müssen in einem zeitlich und netztechnisch nachvollziehbaren Zusammenhang untereinander stehen. Ein MTA kann alle „Received“-Kopfzeilen vor Eingang in seinen Bereich verändern und spurlos löschen. Seine eigene „Received“-Kopfzeile kann er unterdrücken oder beliebig ausfüllen. Nach ihm kommende „Received“-Zeilen kann er allerdings nicht beeinflussen. Ebenso kann der Nutzer die „Received“-Kopfzeilen, die nach Abgabe seiner E-Mail entstehen, nicht mehr beeinflussen.

Allerdings kann ein Nutzer, sofern er *telnet*-Zugang zu einem MTA hat, sich dort einloggen und dann manuell ein SMTP-Protokoll mit dem MTA fahren, das heißt: der Nutzer kreiert nach den Regeln des SMTP (RFC 5321) Zeile für Zeile eine E-Mail und fügt dabei „Received“-Kopfzeilen ein; auf diese Weise täuscht die E-Mail eine beliebige Vorgeschichte vor. Das nutzen beispielsweise SPAM-Programme aus. Die großen Mailerdienste bieten ihren Nutzern keinen solchen Login-Zugang und verhindern über SPAM-Filter unwahrscheinliche Paarungen aus Absender und Empfänger.

9.4 Wireshark *zum Mitlesen von aktuellem Datenverkehr, hier SMTP*

Zur Beobachtung der gesamten laufenden Kommunikation über das Internet im eigenen lokalen Netz bietet das Programm *Wireshark* eine Mitlese- und Analysemöglichkeit. Es erlaubt, bestimmte Protokolle zu filtern, bspw. HTTP für das Filtern von Web-Kommunikation oder SMTP für das Filtern von E-Mail-Kommunikation. *Wireshark* legt die Protokolldatenelemente bis ins letzte Bit offen, so dass auch die Adressen bis auf IP-Ebene beobachtet werden können. Diese Beobachtung dient aber nicht der forensischen *ex post*-Analyse, sondern der forensichen *live*-Beobachtung laufender Aktivitäten. Sie erfordert Zugang zum lokalen Netz.

9.5 Die whois*-Abfrage beim RIR*

Jeder der fünf RIR (Regional Internet Registry zur Vergabe von IP-Adressräumen) bietet über sein Web-Portal eine Datenbankabfrage, die zu einer IP-Adresse den Namen und die Adresse des verantwortlichen Adressraumverwalters (häufig ISP) enthält. Die Datenbank enthält weitere Informationen zum verantwortlichen ISP, die für die technische Administration des Internet nützlich sein kann, wie zum Beispiel Namen und E-Mail-Adressen von technisch und administrativ tätigen Personen, sowie Zeitstempel über Eintragsänderungen. *Einschränkungen der Aussagekraft dieser Datenbankabfrage*:

1. Die geographische Adresse des ISP ist nicht identisch mit der geographischen Adresse des IP-Hosts der abgefragten IP-Adresse. Allerdings liegen die geographischen Adressen des ISP und der von ihm verwalteten IP-Adressen aus betrieblichen Gründen nicht weit auseinander: sie gehören i.d.R. zum selben Staat und sind je nach Netzabdeckung regional enger beschränkt.
2. Die Korrektheit der geographischen Adresse des ISP in der RIR-Datenbank ist nur so genau wie die Sorgfalt der Datenbankpflege durch den RIR und ISP. (s.o. Kap. 3 über die IP-Adressvergabe durch IANA und RIR). Die IANA und RIRs setzen eine restriktive Datenpflege-Policy bei ihren LIRs und ISPs durch, daher gelten die Datenbankeinträge weltweit als zuverlässig.
3. Die Datenbank enthält Information darüber, wann dieser Adressraum zugewiesen worden war und lässt insofern einen (begrenzten) Blick in die Vergangenheit zu. Die Zeitangaben in den „changed“-Feldern der Datenbank können gezielt abgefragt werden („*whois –B*“).

9.6 Die Adressabfrage bei einem Geolokationsdienst

Da ein sehr großer Internet Service Provider (ISPs) oder ein Telekom-Anbieter mit einem großen Netz für seine Nutzer nicht nur Adressen zuweist, sondern auch das Routing über physikalische Leitungen übernimmt, zerlegt er seinen Adressraum in geographisch sinnvolle kleine Einheiten, die er in eigenen Datenbanken verwaltet. Der Zugang zu diesen internen Datenbanken ist nicht generell öffentlich, wird aber bestimmten Internetdiensten gewährt, die wiederum öffentlich genutzt werden können. Dazu gehört der öffentlich zugängliche Internetdienst „*whatismyipaddress.com*“, der beispielsweise meinem privaten IP-Router in Süd-Darmstadt mit der IP-Adresse 79.199.12.110 die Region Darmstadt-Griesheim der Deutschen Telekom AG zuordnet – das ist vom Standort des Routers ca. 10 km entfernt.

Andere Anbieter, wie zum Bespiel der WinShuttle des Deutschen Forschungsnetzes (DFN), der Einzelarbeitsplätzen in ganz Deutschland, gerade auch von zu Hause aus, Internet-Zugänge schaltet, bietet keinen Einblick in seine regionalen Unterbereiche und liefert daher bei *whatismyipaddress.com* regelmäßig die Adresse der Berliner Geschäftstelle des DFN. Gleichwohl beschränken sich auch die WinShuttle-Zugänge auf Deutschland.

Eine weitere Methode der regionalen Zuordnung von IP-Adressbereichen, die Adressaufklärungsdienste wie *whatismyaddress.com* verwenden, ist das sogenannte *Harvesting* mit *Auto-Shooting*, bei dem mobile WLAN-Clients durch besiedelte Gebiete fahren und an der Luftschnittstelle mitlesen, welche IP-Adressen dort verwendet werden. Im Übrigen behandeln solche Dienste ihre Methoden als Geschäftsgeheimnis. Es gibt dennoch Anlass darauf zu vertrauen, dass sie verlässliche Informationen liefern. Das Geschäftsmodell dieser Dienste liegt nämlich in der Online-Werbung, deren Preise sich durch die Anzahl einwählender Nutzer bestimmen. Jeder Nutzer eines solchen Dienstes bekommt aber als erstes seinen eigenen Standort zurückgemeldet. Wenn der allzu sehr daneben liegt, wird er diesen Dienst nicht mehr aufrufen, und in der Masse würde das die Einnahmen des Anbieters für Adressaufklärung schmälern.

Es ist wichtig darauf hinzuweisen, dass dieser Kenntnis keine Ortung durch Sensoren zugrunde liegt, sondern allein die Auswertung einer Adressinformation in einer Datenbank, die im Anmeldeprozess als Nutzer/Kunde/ISP formuliert wird. Diese geographische Zuordnung ist daher nur so genau wie die Sorgfalt der Datenbankpflege durch den RIR und ISP, allerdings setzen IANA und die RIRs mit einer strikten Datenpflege-Policy durch, dass ihre Einträge weltweit als zuverlässig angesehen werden.

9.7 Die Zuordnungstabelle von IP-Adressen zu IP-Hosts beim ISP

Internet Service Provider (ISP) verwalten die statisch und dynamisch an ihre Hosts vergebenen IP-Adressen in internen Tabellen und Datenbanken. Diese Zuordnungslisten werden mit gesetzlich geregelten Fristen (Abrechnung, TK-Überwachungsverordnung, Datenschutz) aufgehoben. Sie stehen externen Personen ohne zusätzliche Vollmachten nicht zur Abfrage zur Verfügung.

Eine lokale Verwaltung (wie ein Universitätsrechenzentrum) weiß in der Regel, welche natürliche Person für das jeweilige Gerät verantwortlich, d.h. ihr „Besitzer“ ist. Dieses Wissen hat aber ein großer ISP mit externen Kunden nicht. Er kennt nur die Zuordnung von vergebenen IP-Adressen an die (zahlenden) Kunden. Die Zuordnung „IP-Adresse zu IP-Host zu Besitzer“ ist datenschutzrechtlich geschützt.

a) Statische IP-Adresszuordnung: Die statisch an IP-Hosts vergebenen IP-Adressen werden von der Verwaltung eines Netzes in einer Datenbank vermerkt. Sein Inhalt ist über einen so genannten „Directory“-Dienst (z.B. LDAP – Lightweight Directory Access Protocol) abrufbar. Speziell unter dem SUN-„Network Information System“

liegt die Information in der Textdatei „hosts“, die man unter Unix mit dem Kommando *„ypcat hosts*“ abfragen kann, sofern man Zugang zum lokalen Netz hat.

b) Dynamische IP-Adresszuordnung: Die dynamisch an IP-Hosts vergebenen IP-Adressen werden von der Verwaltung eines Netzes in einer Datenbank vermerkt. Dieses wird in einem Ablaufprotokoll festgehalten und mit gewissen Fristen aufgehoben. Es gibt kein Netzkommando, diese Datei abzufragen, da sie Verhaltensmuster von Nutzern aufdecken kann.

9.8 Die Login-Liste beim Webmailer

Fast alle Anbieter von E-Mail-Konten bieten einen Zugang zum E-Mail-Dienst über einen Web-Server an. Zu diesen so genannten „Webmailern“ gehören unter anderem *Google Mail, Yahoo!, WEB.DE* und *GMX*.

Um E-Mail von seinem Konto zu lesen, zu bearbeiten oder neue E-Mail zu versenden, „loggt“ sich der Nutzer mit User-ID und Passwort, die extra für diesen Zweck eingerichtet werden, bei dem Webmailer einn, und nach getaner Arbeit loggt er sich wieder aus. Der Webmailer hält für jeden Nutzer einen Stammdatensatz, der den Nutzer ihm gegenüber nach den gesetzlichen Vorschriften persönlich ausweist. Diese Information ist in organisatorischen Maildiensten (wie in Hochschulrechenzentren) zuverlässig, in großen externen Maildiensten wie *Yahoo!* und *Google Mail* aber beruhen diese allein auf den Angaben der Nutzer selbst und gelten als höchst unzuverlässig. Datenschützer empfehlen sogar, bei der Anmeldung zu einem Webmailer falsche Angaben zu machen.

Der Webmailer vermerkt die Ein- und Ausloggvorgänge seiner Nutzer in „Login“-Protokolldateien. Diese Information ist vom Nutzer nicht fälschbar und gilt daher als genauso zuverlässig wie der Webmailer selbst, der durch Insider-Angriffe diese Informationen natürlich fälschen könnte.

10. und 11. Die Zuverlässigkeit einer Adress-Zuordnung und Konspiratives E-Mailing

Um zu vermeiden, eine Anleitung zum konspirativen E-Mailing ungesteuert in der Öffentlichkeit zu verbreiten, sind diese beiden Kapitel aus dem öffentlichen Teil des Arbeitsberichts entfernt worden. Interessierte Leser mögen sich mit einem persönlichen Brief an die Autoren wenden.

12. Analyseschema für E-Mails

Für eine strukturierte forensische Analyse von E-Mails wird folgende systematische Vorgehensweise vorgeschlagen.

12.1 Analyse der „offensichtlichen“ angezeigten Kopfzeilen

Als erster Ansatzpunkt empfiehlt sich die genauere Betrachtung der Kopfzeilen, die E-Mail-Clients in der Regel standardmäßig bei empfangenen E-Mails anzeigen. Dies sind auch die einzigen Kopfzeilen, die ein nicht näher an der Analyse interessierter Nutzer zu sehen bekommt.

Für alle nachfolgend genannten Kopfzeilen gilt, dass sie während ihres Transports durch die weiterleitenden MTAs verändert werden können, ohne dass dies dem Empfänger auffällt. Gewähr für ihre Authentizität kann nur eine digitale Signatur auf Basis von DomainKeys/DKIM leisten, da hierbei (anders als bei PGP und S/MIME) die beim Absenden

bereits vorhandenen Kopfzeilen mit signiert werden. Diese Art von Signatur ist allerdings vom Empfänger nicht ohne weiteres verifizierbar, da E-Mail-Clients sie üblicherweise nicht auswerten. Es ist außerdem zu beachten, dass DomainKeys/DKIM-Signaturen nicht von einem Nutzer, sondern von einem MTA erstellt werden – sie können sie lediglich belegen, dass nach der Weiterleitung durch diesen MTA keine Änderungen mehr an den relevanten Kopfzeilen vorgenommen wurden.

Betreff (Subject): Die Betreffzeile ist vom Absender frei definierbar und wird (von Manipulationen durch MTAs einmal abgesehen) so angezeigt, wie der Absender sie geschrieben hat.

Von (From): Diese Zeile gibt die E-Mail-Adresse (sowie evtl. den Namen) des Absenders an. Zu beachten ist, dass sie nach dem SMTP-Standard frei definierbar ist und nicht zwangsläufig einer Plausibilitätsprüfung unterliegt. In der Praxis hängt es vom Anbieter ab, ob er seinen Nutzern eine beliebige Absenderadresse erlaubt oder den Eintrag in der Absender-Zeile auf E-Mail-Adressen limitiert, deren Zugehörigkeit zum jeweiligen Nutzer er im Vorfeld überprüft hat.

An (To): Diese Zeile enthält typischerweise die E-Mail-Adresse des Empfängers, allerdings kann dies auch variieren. So lässt der SMTP-Standard es zu, das Empfänger-Feld und die Adressaten, die die E-Mail bekommen, vollkommen unabhängig voneinander zu definieren. Die den Autoren bekannten E-Mail-Clients unterstützen dies zwar nicht, über eine Telnet-Verbindung zum MTA kann aber das „Fälschen“ der Empfänger-Adresse realisiert werden: das eigenständige Protokolldatum „rcpt to:“ gibt den eigentlichen Empfänger an, an den der MTA die Mail weiterleitet, ist aber in den vom Mail-Client angezeigten Daten später nicht mehr zu sehen. Das „To:“-Feld hingegen gibt den in der E-Mail sichtbaren Empfänger an und kann auch völlig separat definiert werden.

Es zeigt sich, dass die im E-Mail-Client sichtbaren Kopfzeilen im Rahmen der forensischen Analyse zwar betrachtet werden können und müssen, allerdings hängt die Authentizität bzw. die Verwertbarkeit der darin enthaltenen Informationen von Rahmenbedingungen wie dem verwendeten E-Mail-Provider und den technischen Kenntnissen des Absenders ab.

Datum (Date): Diese Zeile gibt das Datum und die Uhrzeit an, wann die E-Mail vom Absender versendet wurde. Zu beachten ist, dass dieses Feld vom Absender im Prinzip frei definierbar ist und von den weiterleitenden Servern nicht geprüft wird. Geht z.B. die Systemuhr des Absenders um eine Woche nach, so kann beim Empfänger der Eindruck entstehen, er erhalte eine E-Mail, deren Zustellung eine Woche statt weniger Minuten gedauert hat. Eine Analyse der „Received“-Kopfzeilen kann eine falsche Absendezeit aufdecken, falls die von den MTAs eingetragenen Zeitpunkte maßgeblich von der im Datumsfeld abweichen.

12.2 Analyse der ausgeblendeten Kopfzeilen

„Received“-Kopfzeilen

Die mit „Received“ beginnenden Kopfzeilen sind aus forensischer Sicht besonders interessant, da sie vom Absender nur sehr begrenzt verfälscht werden können. Bei den hier beschriebenen Analysemöglichkeiten ist allerdings zu bedenken, dass der Absender in einer Telnet-Sitzung dem MTA gefälschte „Received“-Kopfzeilen übersenden kann, die dieser unter Umständen ungeprüft weitergibt. Das Prinzip, dass jeder empfangenden MTA seine „Received“-Kopfzeile oberhalb der bereits vorhandenen einträgt, bleibt allerdings erhalten: die vom Absender gefälschten Einträge sind in jedem Fall die untersten.

Es existieren einige Anhaltspunkte, anhand derer gefälschte „Received“-Kopfzeilen identifiziert werden können:

1. Die Empfangszeiten müssen zueinander passen. Typisch sind Übertragungszeiten im Sekundenbereich. Sind die Zeitunterschiede zu gering (die E-Mail wurde früher empfangen als gesendet) oder zu groß – (die E-Mail brauchte mehrere Sekunden bis Stunden), so müssen die beteiligten MTAs daraufhin überprüft werden, ob ihre Systemuhren evtl. falsch gehen oder ob sie die Anti-SPAM-Technik „Graylisting“ verwenden, durch die die Zustellung verzögert werden kann.
2. Die Abfolge der beteiligten Rechner muss stimmen. Steht in der ersten „Received“-Kopfzeile, dass Rechner A die E-Mail empfangen hat, so muss A auch in der zweiten Zeile als Sender angegeben sein.
3. Die angeblich beteiligten Rechner müssen während des Versands auch wirklich online gewesen sein und die Funktion als Client bzw. Server gehabt haben. Für den Fälscher ist es zwar leicht, eine real verfügbare IP-Adresse als die des versendenden Clients anzugeben, deren Zugehörigkeit im Nachhinein nur noch über den verantwortlichen ISP ermittelt werden kann. Alle anderen beteiligten Rechner müssen allerdings MTAs, d.h. Server sein, die normalerweise dauerhaft online sind und bei denen daher leicht nachprüfbar ist, ob sie wirklich als SMTP-Server agieren. Da die tatsächliche IP-Adresse des Absenders zwangsläufig in der ersten nicht gefälschten „Received“-Kopfzeile vorkommt, würde spätestens hier eine IP-Adresse, die nicht einem bekannten MTA zugeordnet werden kann, auffallen.

DomainKeys/DKIM-Signaturen

Sind diese (bereits in Kapitel 7 beschriebenen) Signaturen in einer E-Mail vorhanden, so können sie mit Hilfe spezieller Tools wie dem Perl-Skript *dkimverify.pl* verifiziert werden. Hierbei ist zu beachten, dass ein Scheitern der Verifikation nicht zwangsläufig ein Hinweis darauf ist, dass der Inhalt der E-Mail manipuliert wurde, da es ebenso möglich ist, dass der empfangende E-Mail-Client Änderungen an der E-Mail vorgenommen und die Signatur dadurch ungültig gemacht hat.

Sonstige Kopfzeilen

Neben den bereits genannten existieren diverse weitere Kopfzeilen, die teilweise durch die Standards für SMTP und die damit transportierten Nachrichten (aktuell RFCs 5321 bzw. 5322) und teilweise (wie z.B. DomainKeys/DKIM) auch durch weitere Standards definiert sind.

Zusätzlich zu den durch konkrete Standards beschriebenen Kopfzeilen fallen mitunter auch solche auf, die mit „X-“ beginnen. Hierbei handelt es sich um Einträge, deren Bedeutung ausdrücklich nicht durch den SMTP-Standard definiert ist. Per Konvention werden bevorzugt solche „X-“Kopfzeilen von E-Mail-Clients wie auch von MTAs verwendet, um Zusatzinformationen einzutragen, die nur in einem jeweils speziellen Kontext verwendet werden. Im Rahmen einer Analyse muss jeweils individuell untersucht werden, welche Kopfzeile welche Bedeutung hat.

12.3 PGP und S/MIME

Signaturen, die auf Basis von PGP oder S/MIME erstellt wurden, ermöglichen die Zuordnung des Inhalts einer E-Mail zum Verfasser, der damit prinzipbedingt dem Empfänger ein mögliches Beweismittel in die Hand gibt, das ihn selbst belasten könnte. Enthält eine forensisch zu untersuchende E-Mail eine solche Signatur, stellt sich daher zunächst die Frage, warum der Absender seine Nachricht trotzdem signiert hat.

Eine naheliegende Möglichkeit ist hierbei, dass dem Empfänger ermöglicht werden sollte, die Authentizität der E-Mail zu prüfen. In diesem Fall rechnete der Absender entweder nicht

damit, dass die Signatur im Rahmen forensischer Untersuchungen gegen ihn verwendet werden könnte, oder er verwendete ein Pseudonym, das seinem Kommunikationspartner zwar bekannt ist, das aber von potentiellen Ermittlern nicht oder nur schwer seiner wahren Identität zugeordnet werden kann.

Eine weniger offensichtliche, aber im kriminellen Kontext denkbare Möglichkeit ist die, dass ein Angreifer A beim Signieren die Identität einer real existierenden Person B vortäuscht, um B eine Aussage unterzuschieben und ihn damit gezielt zu belasten. Um Gewissheit über die Identität des Absenders zu haben, müssen die folgenden Punkte bei der Prüfung der Signatur bedacht werden.

Das PGP-System beruht darauf, dass sich Nutzer gegenseitig die Zuordnung von privatem Schlüssel und Identität bestätigen („Web of Trust“, siehe PGP 7.0 User’s Guide). Unter falschem Namen ein Schlüsselpaar zu erstellen und sich diese Zuordnung von einigen (evtl. ebenfalls gefälschten) Nutzern bestätigen zu lassen ist daher relativ einfach, folglich ist der beschriebene Angriff mit PGP vergleichsweise leicht durchzuführen. S/MIME unterscheidet sich besonders darin von PGP, dass hier keine Einzelnutzer für die Schlüssel/Identität-Zuordnung bürgen, sondern Institutionen, die so genannten „Certificate Authorities“ (CAs), für die wiederum, hierarchisch gegliedert, andere CAs bürgen, bis hin zu einer Wurzel-CA. Soll nun eine die Authentizität einer S/MIME-Signatur geprüft werden, stellt sich letztlich nur die Frage, ob die verantwortliche Wurzel-CA als vertrauenswürdig eingestuft wird. Da viele CAs von staatlichen oder wirtschaftlichen Organisationen geleitet werden, die genau darauf achten, für wessen Identität sie bürgen, ist es hier schwerer, den privaten Schlüssel einem falschen Namen zuordnen zu lassen.

Letztlich bleiben noch Möglichkeiten, dass der Angreifer die Signatur ohne weitere Hilfsmittel gefälscht hat oder dass er den privaten Schlüssel des Opfers entwenden und zum Signieren nutzen konnte. Ersteres ist bei den heute üblichen Schlüssellängen derart aufwändig, dass eine Fälschung der Signatur praktisch ausgeschlossen werden kann. Ob ein privater Schlüssel entwendet wurde, kann nur festgestellt werden, falls das Opfer dies bemerkt und bei der jeweils verantwortlichen zentralen Stelle bekanntgegeben hat (zu Zertifikatssperrlisten s. RFC 5280).

12.4 Analyse der Login-Datei

Einige E-Mail-Anbieter heben die Login-Daten ihrer E-Mail-Nutzer auf, in denen vermerkt ist, zu welchem Zeitpunkt von welcher IP-Adresse aus auf ein E-Mail-Konto zugegriffen worden ist. Darüber hinaus speichern einige Anbieter auch die Historien der Kontodaten, in denen vermerkt ist, zu welchem Zeitpunkt von welcher IP-Adresse aus die Kontodaten in welcher Weise verändert worden sind. Alle Login-Daten unterliegen dem Datenschutz und können im Rahmen staatsanwaltlicher Ermittlungen der Analyse zur Verfügung gestellt werden.

Zugriffszeiten und IP-Adressen können mit empfangener, versendeter und nur als Entwurf bearbeiteter E-Mail verglichen werden. Sie geben Hinweise zum Leseverhalten von empfangener E-Mail und von E-Mail-Entwürfen. Weiterhin können sie Aufschluss darüber geben, ob auf ein E-Mail-Account von verschiedenen Seiten aus oder gar von verschiedenen Personen zugegriffen worden ist. Das ist besonders dann hilfreich, wenn die E-Mail pseudonym verwaltet wird und wenn die in der E-Mail vorhandenen Informationen, etwa „Received“-Kopfzeilen, lückenhaft sind. Insofern kann die Analyse der Login-Daten die Erkenntnisse aus der Analyse der Kopfzeilen der E-Mail erweitern, abrunden oder zumindest erhärten.

12.5 Analyse des Inhalts

Neben der Analyse aller äußeren Merkmale einer E-Mail darf auch die Untersuchung des eigentlichen Inhalts (hierzu zählen auch evtl. angehängte Dateien) nicht vernachlässigt werden. Da hier der Absender praktisch beliebige Freiheiten hat, ist es allerdings schwierig, ein konkretes Vorgehen zu empfehlen. Vielmehr muss im Einzelfall der Inhalt im Kontext weiterer Ermittlungen ausgewertet und im Falle eines konkreten Verdachts auch auf linguistisch oder technisch steganografisch verborgene Botschaften untersucht werden.

Dank für Unterstützung

Bei der Erstellung dieses Texts und der Präzisierung der hier getroffenen Aussagen haben uns Kollegen des Deutschen Forschungsnetzes (LIR und ISP), insbesondere Karsten Leipold, Holger Wirtz und Dr. Marcus Pattloch unterstützt. Weitere Hintergrundinformationen aus der betrieblichen Praxis eines ISP hat der Leiter des Hochschulrechenzentrums Koblenz Uwe Arndt beigetragen. Für diese Unterstützung möchten wir uns ausdrücklich bedanken. Verbliebene Fehler und Ungenauigkeiten sind selbstverständlich uns zuzurechnen.

Anhang A Literaturverweise

Johannes Buchmann: Einführung in die Kryptographie, Springer, 4. Auflage 2008.

Douglas Comer: Internetworking with TCP/IP. Volume 1: Principles Protocols, and Architecture, 5th Edition, Prentice Hall, Englewood Cliffs, NJ, 2006.

Thomas Hoeren: Zoning und Geolocation - Technische Ansätze zu einer Reterritorialisierung des Internet. Multimedia und Recht Zeitschrift für Informations-, Telekommunikations- und Medienrecht, 3, 2007.

Heiko Holtkamp: Einführung in TCP/IP. Bes. Kap. 3 zu TCP/IP. AG Rechnernetze und Verteilte Systeme, Technische Fakultät, Universität Bielefeld. 18.6.1997, zuletzt geändert 14.2.2002. White Paper, 59 Seiten. http://www.rvs.uni-bielefeld.de/~heiko/tcpip/ [4.4.4009]

D. Moore, R. Periakaruppan, J. Donohoe, K. Claffy: Where in the World is netgeo.caida.org?. Proceedings of the International Networking Conference (INET), 2000.

F. Petitcolas, S. Katzenbeisser, F.A. Petitcolas (Eds.) Introduction to information hiding Information Hiding: Techniques for Steganography and Digital Watermarking, Artech House, Inc., 2000.

PGP 7.0 User's Guide. Introduction to Cryptography, PGP 7.0 MacOS User's Guide, PGP 7.0 Windows 95/98/NT/2000 User's Guide. http://www.pgpi.org/doc/guide/7.0/en/ [29.3.2010]

RFC 791: Jonathan B. Postel: Internet Protocol. Sep 1981. (Obsoletes RFC0760)

RFC 793: Jonathan B. Postel: Transmission Control Protocol. Sep 1981.

RFC 821: Jonathan B. Postel: Simple Mail Transfer Protocol (SMTP). August 1982.

RFC 822: David H. Crocker: Standard for the Format of ARPA Internet Text Messages. August 1982.

RFC 1918: Y. Rekhter et al.: Address Allocation for Private Internets. Feb 1996.

RFC 1122: Requirements for Internet Hosts – Communication Layers. In: Internet Engineering Task Force (IETF), R. Braden, Editor, Oct 1989.

RFC 1180: T. Socolofsky, C. Kale: A TCP/IP Tutorial. Jan 1991.

RFC 4871: E. Allmann et al.: DomainKeys Identified Mail (DKIM) Signatures. May 2007.

RFC 5280: D. Cooper et al.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. May 2008.

RFC 5321: J. Klensin: Simple Mail Transfer Protocol. October 2008.

RFC 5322: P. Resnick et al.: Internet Message Format. October 2008.

RFC 5751: B. Ramsdell, S. Turner: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification. Jan 2010.

Siehe www.rfc-editor.org/

Richard W. Stevens: TCP/IP Illustrated, Vol.1. Addison Wesley, Reading MA etc., 1993.

Andrew Tanenbaum: Computer Networks. 4th Edition., Prentice Hall, Englewood Cliffs, NJ, 2003.

Anhang B Abkürzungsverzeichnis

AfriNIC: African Network Information Center (s. RIR)

APNIC: Asia Pacific Network Information Centre (s. RIR)

ARIN: American Registry for Internet Numbers (s. RIR)

ASCII: American Standard Code for Information Interchange (urspr. 7-Bit-, heute oftmals durch Unicode mit 8/16/32-Bit-Zeichenkodierung für druckbare Zeichen ersetzt)

BOT: Botnet oder Botnetz: „Roboter“-Netz (ferngesteuert durch einen Botnetz-Operator, oft illegal gekaperte und vernetzte Rechner zur Verschleierung von illegalen Netzaktivitäten)

DENIC: Deutsches Network Information Center (zentrale Registrierungsstelle für Domain-Namen unter dem Top-Level-Domain „de“)

DFN: Deutsches Forschungsnetz (LIR und ISP für seine Mitglieder der deutschen Forschungslandschaft, www.dfn.de)

DHCP: Dynamic Host Configuration Protocol (Dynamische Zuweisung von IP-Adresse an IP-Host durch ISP für die Dauer einer Sitzung)

DKIM: Domain Key Identified Mail (Signaturbasierter Beweis, ob die Mail verändert wurde und ob der Domain-Name des Absender korrekt ist)

DNS: Domain Name Service (Abbildung von Domain-Namen auf IP-Adressen)

DTAG: Deutsche Telekom AG

Ethernet: Keine Abkürzung. „Ether“ steht für „Äther“ (Standard für ein Lokales Netz)

FDDI: Fiber Distributed Data Interface (Standard für ein Lokales Netz)

GSM: Group Speciale Mobile, oder Global System for Mobile Communications (Standard für Mobiltelefonie)

HTTP: Hypertext Transfer Protocol (Internet Standard für die Web-Kommunikation)

IANA: Internet Assigned Numbers Authority

IP: Internet Protocol (Regeln für den Austausch von Internet-Datenpaketen zwischen IP-Hosts)

IPv4, IPv6: IP Version 4 (Adressraum viermal acht Bits), IP Version 6 (Adressraum achtmal sechzehn Bits)

IMAP: Internet Mail Access Protocol (ein Standard für die Auslieferung von E-Mail an den Endnutzer; ein anderer Standard ist POP)

ISP: Internet Service Provider

LACNIC: Latin American and Caribbean Internet Addresses Registry (s. RIR)

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol (Abfrage von Adressinformationen im Netz)

LIR: Local Internet Registry (erhält von RIR IP-Adressräume zur Weiterverteilung)

MEST/MESZ: Middle European Summer Time (entspricht UTC+0200)

MET/MEZ: Middle European Standard Time (entspricht UTC+0100)

MTA: Message Transfer Agent (Mailserver zur Weiterleitung von E-Mail)

NAT: Network Address Translation (z. B. zur Einsparung von IP-Adressen, indem mehreren privaten IP-Adressen nach außen nur eine öffentliche IP-Adresse zugeordnet wird)

NIR: National Internet Registry (erhält von RIR IP-Adressräume zur Weiterverteilung)

PC: Personal Computer (Tischgerät oder Laptop i.d.R. mit Zugang zum Internet)

POP: Post Office Protocol (ein Standard für die Auslieferung von E-Mail an den Endnutzer; ein anderer Standard ist IMAP)

PKT: Pakistan Standard Time (entspricht UTC+0500)

PST: Pacific Standard Time (entspricht UTC-0800)

PDT: Pacific Daylight Saving Time (entspricht UTC-0700)

RFC: Request for Comment (Namenspräfix für die Internet-Standards)

RFC 821/822/5321/5322: Internet-Standards für den Austausch und die Formatierung von E-Mail

RIPE NCC: Réseaux IP Européens, Network Coordination Centre (RIR für Europa, Mittlerer Osten und Zentralasien)

RIR: Regional Internet Registry (Die fünf RIRs der Welt sind AfriNIC (Africa Region), APNIC (Asia/Pacific Region), ARIN (North America Region), LACNIC (Latin America and some Caribbean Islands), RIPE NCC (Europe, the Middle East, and Central Asia))

SMTP: Simple Mail Transfer Protocol (RFC 821, Internet Standard für den Austausch von E-Mail)

SPAM: Keine Abkürzung, übernommen aus einem Monty-Python-Clip (unerwünschte Werbemail)

TCP:	Transmission Control Protocol (Datentransport zwischen Anwendungen in IP-Hosts)
TCP/IP:	Transmission Control Protocol / Internet Protocol (Grundlegendes Regelwerk zum Austausch von Datenpaketen im Internet)
UMTS:	Universal Mobile Telecommunications System (für mobile Datenübertragung, auch Telefonie)
UTC:	Universal Time Coordinated (bedeutet dasselbe wie GMT = Greenwich Mean Time, Ortszeit London)
VPN:	Virtual Private Network (verschlüsselte Verbindung zwischen Nutzer und Betreiber mit Unterdrückung der Nutzeradresse nach außen)
WLAN:	Wireless Local Area Network (Drahtloser Anschluss an LAN)

Anhang C Beispiel einer E-Mail-Analyse

E-Mail Beispiel

```
Betreff: Merry Christmas!
Von:     tanvioswal@gmail.com
Datum:   Wed, 24 Dec 2008 18:52:46 +0530
An:      ruediger@rgrimm.de
X-Account-Key:     account4
X-UIDL:            1193853765.17109
X-Mozilla-Status:  0003
X-Mozilla-Status2: 00000000
Return-Path:       <SRS0=12hp=45=gmail.com=tanvioswal@srs.kundenserver.de>

Received: from mail.uni-koblenz.de ([unix socket]) by mail (Cyrus v2.2.12) with
LMTPA; Wed, 24 Dec 2008 14:22:49 +0100
X-Sieve: CMU Sieve 2.2

Received:
from deliver.uni-koblenz.de (deliver.uni-koblenz.de [141.26.64.15]) by mail.uni-
koblenz.de (Postfix) with ESMTP id 8A4D23800257 for <grimm+forward@uni-koblenz.de>;
Wed, 24 Dec 2008 14:22:49 +0100 (CET)

Received:
from localhost (localhost [127.0.0.1]) by deliver.uni-koblenz.de (Postfix) with
ESMTP id 7C663789AB2B; Wed, 24 Dec 2008 14:22:49 +0100 (CET)

Received:
from deliver.uni-koblenz.de ([127.0.0.1]) by localhost (deliver.uni-koblenz.de
[127.0.0.1]) (amavisd-new, port 10024) with ESMTP id 00672-01; Wed, 24 Dec 2008
14:22:48 +0100 (CET)
X-CHKRCPT: Envelopesender noch
srs0=12hp=45=gmail.com=tanvioswal@srs.kundenserver.de

Received:
from mout-xforward.kundenserver.de (mout-xforward.kundenserver.de [212.227.17.5])
by deliver.uni-koblenz.de (Postfix) with ESMTP id 98A63789AB1B for
<grimm+forward@uni-koblenz.de>; Wed, 24 Dec 2008 14:22:48 +0100 (CET)

Received-SPF:
pass (mxeu24: domain of gmail.com designates 209.85.198.237 as permitted sender)
client-ip=209.85.198.237; envelope-from=tanvioswal@gmail.com; helo=rv-out-
0506.google.com;

Received:
from rv-out-0506.google.com (rv-out-0506.google.com [209.85.198.237]) by
mx.kundenserver.de (node=mxeu24) with ESMTP (Nemesis) id 0MKtd6-1LFThH1v9l-000kkk ;
Wed, 24 Dec 2008 14:22:48 +0100

Received:
by rv-out-0506.google.com with SMTP id f6so3019235rvb.55 for <multiple recipients>;
Wed, 24 Dec 2008 05:22:46 -0800 (PST)

DKIM-Signature:
v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=gamma;h=domainkey-
signature:received:received:message-id:date:from:to :subject:mime-version:content-
type;bh=dhOdU7DNsgNSbynl2L2wVTZfslLyR8vGp9xqTfAlA5c=;b=hbH492imkXoFQAGeml40BRXB1tTu
5OG/FbRlcwKJh7nxIZWYOb9AyOU3PYHo/K299O
6xgdp9E0L42jUCuXz+ZY+LyT6Nlc48J/vOI3XQgBm/e5RqWtY91lP82DL17vg0fZGjks
skjPrPv5Puwy00IrlXrVt+r8TUPOG4lMi1K2A=

DomainKey-Signature:
a=rsa-sha1; c=nofws; d=gmail.com; s=gamma; h=message-id:date:from:to:subject:mime-
version:content-type;
b=OGJ6QrpKlU6sc9to62LCdSZw/75/gx+Ls8/kxo8IN0gtGVt0ru8DTI+XJwk+89/wnb
YHZW2giXt2EjV3IQSm3qEvNp3UGKf9Nkib0/KqRo1wUyWAsd3UTPbHMOTlWpxyRmec+J
dMxhzyPxgPIV5Vcufdn54ZcUEwtHYLn9we7wg=

Received:
```

```
by 10.140.166.16 with SMTP id o16mr4298044rve.25.1230124966277; Wed, 24 Dec 2008
05:22:46 -0800 (PST)

Received:
by 10.141.48.5 with HTTP; Wed, 24 Dec 2008 05:22:46 -0800 (PST)

Nachricht-ID: <cc62165b0812240522s78ce1002j343bc121ababb5ee@mail.gmail.com>

MIME-Version:    1.0
Content-Type:    multipart/alternative; boundary="----
=_Part_72595_5123804.1230124966280"
X-Virus-Scanned: amavisd-new at uni-koblenz.de
X-Spam-Status:   No, score=0.458 tagged_above=-100 required=5
                 tests=[BAYES_00=-2.599, HTML_10_20=1.351, HTML_MESSAGE=0.001,
                 SARE_MSGID_LONG40=0.637, SPF_HELO_PASS=-0.001, SPF_NEUTRAL=1.069]
X-Spam-Score:    0.458

hallo! Hallo! hallo!
Liebe [...]

Viele Liebe Gruesse
Tanvi
```

Analyse des Beispiels

Im Folgenden wird die oben im Klartext gezeigte E-Mail anhand des in Kapitel 12 beschriebenen Schemas analysiert.

1. Analyse der „offensichtlich“ angezeigten Kopfzeilen

Die „Von“-Kopzeile gibt an, dass die E-Mail von tanvioswal@gmail.com kommt, was sich mit der textuellen Signatur („Viele Liebe Gruesse \ Tanvi“) deckt.

Die „An“-Kopfzeile benennt ruediger@rgrimm.de als Zieladresse. Mit dem Hintergrundwissen, dass unter dieser Adresse eine Umleitung zu grimm@uni-koblenz.de eingerichtet ist und die E-Mail dort abgerufen wurde, zeigt sich, dass die Zieladresse nicht manipuliert wurde.

Laut „Datum“-Kopfzeile wurde die E-Mail am 24.12.2008 um 18:52:46 IST (Indian Standard Time) versendet, dies entspricht 13:22:46 UTC (koordinierte Weltzeit). Im Vergleich mit den in den „Received“-Kopfzeilen enthaltenen Daten zeigt sich, dass das Datum vom Absender korrekt angegeben wurde.

2. Analyse der ausgeblendeten Kopfzeilen

Die erste (unterste) „Received“-Kopfzeile gibt an, dass die Nachricht von einem System mit der IP-Adresse 10.141.48.5 empfangen wurde und dass die Übertragungsart HTTP war. Letzteres deckt sich mit der Tatsache, dass Gmail (Google Mail) bekanntermaßen ein Webmail-Dienstleister ist. Die IP-Adresse des eigentlichen Absenders ist in dieser Kopfzeile nicht enthalten, was allerdings nicht den SMTP-Standard verletzt und für Webmail-Dienstleister nicht ungewöhnlich ist. Die IP-Adresse 10.141.48.5 scheint zu einem Server von Gmail zu gehören, da es sich aber um eine private, nur im Gmail-eigenen Netz gültige Adresse handelt, können zu ihr keine weiteren Details ermittelt werden. Die zweite „Received“-Kopfzeile lässt durch die ebenfalls private IP-Adresse erkennen, dass die E-Mail hier Gmail-intern weitergeleitet wurde.

Die nächsten zwei Blöcke enthalten die DomainKeys- und DKIM-Signaturen. Mit Hilfe des Tools *dkimverify.pl* konnte (unter Verwendung der vollständigen Mail, in der der Inhalt nicht gekürzt ist) bestätigt werden, dass beide Signaturen gültig sind. Hieraus lässt sich insbesondere ableiten, dass der Inhalt der E-Mail sowie die Kopfzeilen „Von“, „An“, „Datum“ und „Betreff“ nach dem Versenden durch Gmail nicht verfälscht wurden.

In der folgenden „Received“-Kopfzeile ist erstmalig ein öffentlich erreichbarer MTA genannt (rv-out-0506.google.com). Eine Überprüfung des Hostnamen mittels des Unix-Tools *host* zeigt, dass ihm mehrere IP-Adressen zugeordnet sind (eine gebräuchliche Methode, das DNS zur Lastverteilung einzusetzen), die nächste „Received“-Kopfzeile lässt hierbei erkennen, dass der Rechner mit der IP-Adresse 209.85.198.237 der an der Weiterleitung beteiligte war. Über *whatismyipaddress.com* kann diese Adresse dem Ort Mountain View in Kalifornien (USA) zugeordnet werden. Dies deckt sich mit dem zu erwartenden Ort, von dem aus die E-Mail erstmals in das Internet versendet wurde, da Google Inc. (Betreiber von Gmail) dort seinen Firmensitz hat.

Die eben bereits betrachtete vierte „Received“-Kopfzeile wurde von einem MTA mit dem Hostnamen mx.kundenserver.de eingetragen. Eine *whois*-Anfrage zeigt, dass diese Domain dem Unternehmen „Schlund+Partner AG“ gehört. Die Rolle eines MTAs dieses Unternehmens lässt sich folgendermaßen begründen: die Domain „rgrimm.de“, an die der MTA von Gmail die E-Mail schickt, wird, wie eine weitere *whois*-Anfrage zeigt, von der „1&1 Internet AG“ betrieben. Eine kurze Recherche per Suchmaschine ergibt, dass die „Schlund+Partner AG“ ein Teil der „1&1 Internet AG“ ist.

Die folgende Kopfzeile, die mit „Received-SPF“ beginnt, ist keine „Received“-Kopfzeile im Sinne des SMTP-Standards, sondern wurde als Teil des SPAM-Schutzmechanismus SPF (Sender Policy Framework) ergänzt, der prüft, ob der versendende MTA wirklich für die in der Absenderadresse genannte Domain verantwortlich ist. Für die Analyse der betrachteten Mail bringt sie keine neuen Erkenntnisse; beachtenswert ist allerdings, dass der letztlich für die Umleitung zu der Adresse „grimm@uni-koblenz.de“ verantwortliche MTA mout-xforward.kundenserver.de die Absenderadresse von „tanvioswal@gmail.com“ zu „srs0=12hp=45=gmail.com=tanvioswal@srs.kundenserver.de“ ändert, damit nachgelagerte MTAs, die ebenfalls SPF verwenden, nicht vergeblich versuchen, die Verantwortlichkeit von kundenserver.de für E-Mails der Domain gmail.com zu prüfen.

Die letzten vier „Received“-Kopfzeilen lassen Weiterleitung innerhalb der Uni Koblenz erkennen, wobei die E-Mail teilweise zwischen verschiedenen Diensten (wie z.B. einem „normalen“ MTA und einem E-Mail-Virenscanner) auf demselben Rechner ausgetauscht wird.

Die übrigen, teilweise oberhalb und teilweise unterhalb der „Received“-Kopfzeilen dargestellten „X“-Kopfzeilen wurden erst durch die MTAs der Uni Koblenz bzw. durch den empfangenden E-Mail-Client ergänzt und bieten keinen zusätzlichen Erkenntnissgewinn.

3. PGP und S/MIME

Signaturen dieser Art sind in der E-Mail nicht enthalten.

4. Analyse des Inhalts

Da die gezeigte E-Mail nur als Beispiel dient und keinem kriminellen Kontext entspringt, ist in dem (gekürzten) Inhalt keine verborgene Nachricht zu vermuten.

Anhang D Eine über *telnet* erzeugte E-Mail

Putty-Login linux.uni-koblenz.de

Bildschirmprotokoll 7. April 18:20

```
> login as:
grimm

> Using keyboard-interactive authentication.
> Password:
...

> Last login: Tue Apr  7 14:07:52 2009 from p4fc71108.dip0.t-ipconnect.de
> [...]
>
> [grimm@penguin2:~] 207 > telnet deliver.uni-koblenz.de 25
> Trying 141.26.64.15...
> Connected to deliver.uni-koblenz.de.
> Escape character is '^]'.
> 220 deliver.uni-koblenz.de ESMTP Postfix

HELO namenlos.nirgendwo
> 250 deliver.uni-koblenz.de

MAIL FROM: niemand@nirgends.de
> 250 Ok

RCPT TO: ruediger@rgrimm.de
> 250 Ok

DATA
> 354 End data with <CR><LF>.<CR><LF>

Ich bin über "putty" in linux.uni-koblenz.de eingeloggt.
Dort habe ich "telnet deliver.uni-koblenz.de 25" aufgerufen.
Jetzt schicke ich Zeile für Zeile Mail an ruediger@rgrimm.de (über 1und1).
Diese wird zurück an grimm@uni-koblenz.de weitergeleitet (forward).
Auf diesem Wege kommt sie in meine Koblenzer Mailbox und
kann auf die "RECEIVED"-Header-Spur ausgewertet werden.
Mal sehen was heraus kommt --- RüG
.
> 250 Ok: queued as 8E748789B017

quit
> 221 Bye
> Connection closed by foreign host.
> [grimm@penguin2:~] 207 >
```

Das Ergebnis ist folgende E-Mail:

```
Von:    niemand@nirgends.de
Datum:  Tue, 7 Apr 2009 18:13:10 +0200 (CEST)
An:     undisclosed-recipients:;
X-Account-Key:     account4
X-UIDL:            1193853765.21594
X-Mozilla-Status:  0001
X-Mozilla-Status2: 00000000
Return-Path:       <niemand@nirgends.de>

Received:
from mail.uni-koblenz.de ([unix socket]) by mail (Cyrus v2.2.12) with LMTPA; Tue,
07 Apr 2009 18:16:37 +0200
X-Sieve: CMU Sieve 2.2

Received:
```

```
from deliver.uni-koblenz.de (deliver.uni-koblenz.de [141.26.64.15]) by mail.uni-
koblenz.de (Postfix) with ESMTP id E1CD8380087F for <grimm+forward@uni-koblenz.de>;
Tue, 7 Apr 2009 18:16:37 +0200 (CEST)

Received:
from localhost (localhost [127.0.0.1]) by deliver.uni-koblenz.de (Postfix) with
ESMTP id D2B06789B017; Tue, 7 Apr 2009 18:16:37 +0200 (CEST)

Received:
from deliver.uni-koblenz.de ([127.0.0.1]) by localhost (deliver.uni-koblenz.de
[127.0.0.1]) (amavisd-new, port 10024) with ESMTP id 01602-03; Tue, 7 Apr 2009
18:16:37 +0200 (CEST)
X-CHKRCPT: Envelopesender unkn niemand@nirgends.de

Received:
from moutng.kundenserver.de (moutng.kundenserver.de [212.227.126.186]) by
deliver.uni-koblenz.de (Postfix) with ESMTP id B30DB789AA3B for <grimm+forward@uni-
koblenz.de>; Tue, 7 Apr 2009 18:16:37 +0200 (CEST)

Received:
from deliver.uni-koblenz.de (deliver.uni-koblenz.de [141.26.64.15]) by
mx.kundenserver.de (node=mxeu5) with ESMTP (Nemesis) id 0MKqpg-1LrDyX1Jhr-000iq0
for ruediger@rgrimm.de; Tue, 07 Apr 2009 18:16:37 +0200

Received:
from localhost (localhost [127.0.0.1]) by deliver.uni-koblenz.de (Postfix) with
ESMTP id 2071C789AA3B for <ruediger@rgrimm.de>; Tue, 7 Apr 2009 18:16:37 +0200
(CEST)

Received:
from deliver.uni-koblenz.de ([127.0.0.1]) by localhost (deliver.uni-koblenz.de
[127.0.0.1]) (amavisd-new, port 10024) with ESMTP id 01270-05 for
<ruediger@rgrimm.de>; Tue, 7 Apr 2009 18:16:36 +0200 (CEST)
X-CHKRCPT: Envelopesender unkn niemand@nirgends.de

Received:
from namenlos.nirgendwo (penguin2.uni-koblenz.de [141.26.66.69]) by deliver.uni-
koblenz.de (Postfix) with SMTP id 8E748789B017 for <ruediger@rgrimm.de>; Tue, 7 Apr
2009 18:13:10 +0200 (CEST)

Nachricht-ID:    <20090407161329.8E748789B017@deliver.uni-koblenz.de>
X-Virus-Scanned: amavisd-new at uni-koblenz.de
X-Virus-Scanned: amavisd-new at uni-koblenz.de
X-Spam-Status:   No, score=-0.781 tagged_above=-100 required=5
                 tests=[ALL_TRUSTED=-1.8, BAYES_00=-2.599, MISSING_SUBJECT=1.816,
                 NO_REAL_NAME=0.961, UNDISC_RECIPS=0.841]
X-Spam-Score:    -0.781

Ich bin über "putty" in linux.uni-koblenz.de eingeloggt.
Dort habe ich "telnet deliver.uni-koblenz.de 25" aufgerufen.
Jetzt schicke ich Zeile für Zeile Mail an ruediger@rgrimm.de (über 1und1).
Diese wird zurück an grimm@uni-koblenz.de weitergeleitet (forward).
Auf diesem Wege kommt sie in meine Koblenzer Mailbox und
kann auf die "RECEIVED"-Header-Spur ausgewertet werden.
Mal sehen was heraus kommt --- RüG
```

Bisher erschienen

Arbeitsberichte aus dem Fachbereich Informatik

(http://www.uni-koblenz-landau.de/koblenz/fb4/publications/Reports/arbeitsberichte)

Rüdiger Grimm, Daniel Pähler, E-Mail-Forensik – IP-Adressen und ihre Zuordnung zu Internet-Teilnehmern und ihren Standorten, Arbeitsberichte aus dem Fachbereich Informatik 5/2010

Christoph Ringelstein, Steffen Staab, PAPEL: Syntax and Semantics for Provenance-Aware Policy Definition, Arbeitsberichte aus dem Fachbereich Informatik 4/2010

Nadine Lindermann, Sylvia Valcárcel, Harald F.O. von Kortzfleisch, Ein Stufenmodell für kollaborative offene Innovationsprozesse in Netzwerken kleiner und mittlerer Unternehmen mit Web 2.0, Arbeitsberichte aus dem Fachbereich Informatik 3/2010

Maria Wimmer, Dagmar Lück-Schneider, Uwe Brinkhoff, Erich Schweighofer, Siegfried Kaiser, Andreas Wieber, Fachtagung Verwaltungsinformatik FTVI Fachtagung Rechtsinformatik FTRI 2010, Arbeitsberichte aus dem Fachbereich Informatik 2/2010

Max Braun, Ansgar Scherp, Steffen Staab, Collaborative Creation of Semantic Points of Interest as Linked Data on the Mobile Phone, Arbeitsberichte aus dem Fachbereich Informatik 1/2010

Marc Santos, Einsatz von „Shared In-situ Problem Solving“ Annotationen in kollaborativen Lern- und Arbeitsszenarien, Arbeitsberichte aus dem Fachbereich Informatik 20/2009

Carsten Saathoff, Ansgar Scherp, Unlocking the Semantics of Multimedia Presentations in the Web with the Multimedia Metadata Ontology, Arbeitsberichte aus dem Fachbereich Informatik 19/2009

Christoph Kahle, Mario Schaarschmidt, Harald F.O. von Kortzfleisch, Open Innovation: Kundenintegration am Beispiel von IPTV, Arbeitsberichte aus dem Fachbereich Informatik 18/2009

Dietrich Paulus, Lutz Priese, Peter Decker, Frank Schmitt, Pose-Tracking Forschungsbericht, Arbeitsberichte aus dem Fachbereich Informatik 17/2009

Andreas Fuhr, Tassilo Horn, Andreas Winter, Model-Driven Software Migration Extending SOMA, Arbeitsberichte aus dem Fachbereich Informatik 16/2009

Eckhard Großmann, Sascha Strauß, Tassilo Horn, Volker Riediger, Abbildung von grUML nach XSD soamig, Arbeitsberichte aus dem Fachbereich Informatik 15/2009

Kerstin Falkowski, Jürgen Ebert, The STOR Component System Interim Report, Arbeitsberichte aus dem Fachbereicht Informatik 14/2009

Sebastian Magnus, Markus Maron, An Empirical Study to Evaluate the Location of Advertisement Panels by Using a Mobile Marketing Tool, Arbeitsberichte aus dem Fachbereich Informatik 13/2009

Sebastian Magnus, Markus Maron, Konzept einer Public Key Infrastruktur in iCity, Arbeitsberichte aus dem Fachbereich Informatik 12/2009

Sebastian Magnus, Markus Maron, A Public Key Infrastructure in Ambient Information and Transaction Systems, Arbeitsberichte aus dem Fachbereich Informatik 11/2009

Ammar Mohammed, Ulrich Furbach, Multi-agent systems: Modeling and Virification using Hybrid Automata, Arbeitsberichte aus dem Fachbereich Informatik 10/2009

Andreas Sprotte, Performance Measurement auf der Basis von Kennzahlen aus betrieblichen Anwendungssystemen: Entwurf eines kennzahlengestützten Informationssystems für einen Logistikdienstleister, Arbeitsberichte aus dem Fachbereich Informatik 9/2009

Gwendolin Garbe, Tobias Hausen, Process Commodities: Entwicklung eines Reifegradmodells als Basis für Outsourcingentscheidungen, Arbeitsberichte aus dem Fachbereich Informatik 8/2009

Petra Schubert et. al., Open-Source-Software für das Enterprise Resource Planning, Arbeitsberichte aus dem Fachbereich Informatik 7/2009

Ammar Mohammed, Frieder Stolzenburg, Using Constraint Logic Programming for Modeling and Verifying Hierarchical Hybrid Automata, Arbeitsberichte aus dem Fachbereich Informatik 6/2009

Tobias Kippert, Anastasia Meletiadou, Rüdiger Grimm, Entwurf eines Common Criteria-Schutzprofils für Router zur Abwehr von Online-Überwachung, Arbeitsberichte aus dem Fachbereich Informatik 5/2009

Hannes Schwarz, Jürgen Ebert, Andreas Winter, Graph-based Traceability – A Comprehensive Approach. Arbeitsberichte aus dem Fachbereich Informatik 4/2009

Anastasia Meletiadou, Simone Müller, Rüdiger Grimm, Anforderungsanalyse für Risk-Management-Informationssysteme (RMIS), Arbeitsberichte aus dem Fachbereich Informatik 3/2009

Ansgar Scherp, Thomas Franz, Carsten Saathoff, Steffen Staab, A Model of Events based on a Foundational Ontology, Arbeitsberichte aus dem Fachbereich Informatik 2/2009

Frank Bohdanovicz, Harald Dickel, Christoph Steigner, Avoidance of Routing Loops, Arbeitsberichte aus dem Fachbereich Informatik 1/2009

Stefan Ameling, Stephan Wirth, Dietrich Paulus, Methods for Polyp Detection in Colonoscopy Videos: A Review, Arbeitsberichte aus dem Fachbereich Informatik 14/2008

Tassilo Horn, Jürgen Ebert, Ein Referenzschema für die Sprachen der IEC 61131-3, Arbeitsberichte aus dem Fachbereich Informatik 13/2008

Thomas Franz, Ansgar Scherp, Steffen Staab, Does a Semantic Web Facilitate Your Daily Tasks?, Arbeitsberichte aus dem Fachbereich Informatik 12/2008

Norbert Frick, Künftige Anfordeungen an ERP-Systeme: Deutsche Anbieter im Fokus, Arbeitsberichte aus dem Fachbereicht Informatik 11/2008

Jürgen Ebert, Rüdiger Grimm, Alexander Hug, Lehramtsbezogene Bachelor- und Masterstudiengänge im Fach Informatik an der Universität Koblenz-Landau, Campus Koblenz, Arbeitsberichte aus dem Fachbereich Informatik 10/2008

Mario Schaarschmidt, Harald von Kortzfleisch, Social Networking Platforms as Creativity Fostering Systems: Research Model and Exploratory Study, Arbeitsberichte aus dem Fachbereich Informatik 9/2008

Bernhard Schueler, Sergej Sizov, Steffen Staab, Querying for Meta Knowledge, Arbeitsberichte aus dem Fachbereich Informatik 8/2008

Stefan Stein, Entwicklung einer Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld, Arbeitsberichte aus dem Fachbereich Informatik 7/2008

Matthias Bohnen, Lina Brühl, Sebastian Bzdak, RoboCup 2008 Mixed Reality League Team Description, Arbeitsberichte aus dem Fachbereich Informatik 6/2008

Bernhard Beckert, Reiner Hähnle, Tests and Proofs: Papers Presented at the Second International Conference, TAP 2008, Prato, Italy, April 2008, Arbeitsberichte aus dem Fachbereich Informatik 5/2008

Klaas Dellschaft, Steffen Staab, Unterstützung und Dokumentation kollaborativer Entwurfs- und Entscheidungsprozesse, Arbeitsberichte aus dem Fachbereich Informatik 4/2008

Rüdiger Grimm: IT-Sicherheitsmodelle, Arbeitsberichte aus dem Fachbereich Informatik 3/2008

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik 2/2008

Markus Maron, Kevin Read, Michael Schulze: CAMPUS NEWS – Artificial Intelligence Methods Combined for an Intelligent Information Network, Arbeitsberichte aus dem Fachbereich Informatik 1/2008

Lutz Priese,Frank Schmitt, Patrick Sturm, Haojun Wang: BMBF-Verbundprojekt 3D-RETISEG Abschlussbericht des Labors Bilderkennen der Universität Koblenz-Landau, Arbeitsberichte aus dem Fachbereich Informatik 26/2007

Stephan Philippi, Alexander Pinl: Proceedings 14. Workshop 20.-21. September 2007 Algorithmen und Werkzeuge für Petrinetze, Arbeitsberichte aus dem Fachbereich Informatik 25/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS – an Intelligent Bluetooth-based Mobile Information Network, Arbeitsberichte aus dem Fachbereich Informatik 24/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS - an Information Network for Pervasive Universities, Arbeitsberichte aus dem Fachbereich Informatik 23/2007

Lutz Priese: Finite Automata on Unranked and Unordered DAGs Extented Version, Arbeitsberichte aus dem Fachbereich Informatik 22/2007

Mario Schaarschmidt, Harald F.O. von Kortzfleisch: Modularität als alternative Technologie- und Innovationsstrategie, Arbeitsberichte aus dem Fachbereich Informatik 21/2007

Kurt Lautenbach, Alexander Pinl: Probability Propagation Nets, Arbeitsberichte aus dem Fachbereich Informatik 20/2007

Rüdiger Grimm, Farid Mehr, Anastasia Meletiadou, Daniel Pähler, Ilka Uerz: SOA-Security, Arbeitsberichte aus dem Fachbereich Informatik 19/2007

Christoph Wernhard: Tableaux Between Proving, Projection and Compilation, Arbeitsberichte aus dem Fachbereich Informatik 18/2007

Ulrich Furbach, Claudia Obermaier: Knowledge Compilation for Description Logics, Arbeitsberichte aus dem Fachbereich Informatik 17/2007

Fernando Silva Parreiras, Steffen Staab, Andreas Winter: TwoUse: Integrating UML Models and OWL Ontologies, Arbeitsberichte aus dem Fachbereich Informatik 16/2007

Rüdiger Grimm, Anastasia Meletiadou: Rollenbasierte Zugriffskontrolle (RBAC) im Gesundheitswesen, Arbeitsberichte aud dem Fachbereich Informatik 15/2007

Ulrich Furbach, Jan Murray, Falk Schmidsberger, Frieder Stolzenburg: Hybrid Multiagent Systems with Timed Synchronization-Specification and Model Checking, Arbeitsberichte aus dem Fachbereich Informatik 14/2007

Björn Pelzer, Christoph Wernhard: System Description:“E-KRHyper“, Arbeitsberichte aus dem Fachbereich Informatik, 13/2007

Ulrich Furbach, Peter Baumgartner, Björn Pelzer: Hyper Tableaux with Equality, Arbeitsberichte aus dem Fachbereich Informatik, 12/2007

Ulrich Furbach, Markus Maron, Kevin Read: Location based Informationsystems, Arbeitsberichte aus dem Fachbereich Informatik, 11/2007

Philipp Schaer, Marco Thum: State-of-the-Art: Interaktion in erweiterten Realitäten, Arbeitsberichte aus dem Fachbereich Informatik, 10/2007

Ulrich Furbach, Claudia Obermaier: Applications of Automated Reasoning, Arbeitsberichte aus dem Fachbereich Informatik, 9/2007

Jürgen Ebert, Kerstin Falkowski: A First Proposal for an Overall Structure of an Enhanced Reality Framework, Arbeitsberichte aus dem Fachbereich Informatik, 8/2007

Lutz Priese, Frank Schmitt, Paul Lemke: Automatische See-Through Kalibrierung, Arbeitsberichte aus dem Fachbereich Informatik, 7/2007

Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, Marcel Weinand, Jörg Helbach: Security Requirements for Non-political Internet Voting, Arbeitsberichte aus dem Fachbereich Informatik, 6/2007

Daniel Bildhauer, Volker Riediger, Hannes Schwarz, Sascha Strauß, „grUML – Eine UML-basierte Modellierungssprache für T-Graphen“, Arbeitsberichte aus dem Fachbereich Informatik, 5/2007

Richard Arndt, Steffen Staab, Raphaël Troncy, Lynda Hardman: Adding Formal Semantics to MPEG-7: Designing a Well Founded Multimedia Ontology for the Web, Arbeitsberichte aus dem Fachbereich Informatik, 4/2007

Simon Schenk, Steffen Staab: Networked RDF Graphs, Arbeitsberichte aus dem Fachbereich Informatik, 3/2007

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik, 2/2007

Anastasia Meletiadou, J. Felix Hampe: Begriffsbestimmung und erwartete Trends im IT-Risk-Management, Arbeitsberichte aus dem Fachbereich Informatik, 1/2007

„Gelbe Reihe“
(http://www.uni-koblenz.de/fb4/publikationen/gelbereihe)

Lutz Priese: Some Examples of Semi-rational and Non-semi-rational DAG Languages. Extended Version, Fachberichte Informatik 3-2006

Kurt Lautenbach, Stephan Philippi, and Alexander Pinl: Bayesian Networks and Petri Nets, Fachberichte Informatik 2-2006

Rainer Gimnich and Andreas Winter: Workshop Software-Reengineering und Services, Fachberichte Informatik 1-2006

Kurt Lautenbach and Alexander Pinl: Probability Propagation in Petri Nets, Fachberichte Informatik 16-2005

Rainer Gimnich, Uwe Kaiser, and Andreas Winter: 2. Workshop "Reengineering Prozesse" – Software Migration, Fachberichte Informatik 15-2005

Jan Murray, Frieder Stolzenburg, and Toshiaki Arai: Hybrid State Machines with Timed Synchronization for Multi-Robot System Specification, Fachberichte Informatik 14-2005

Reinhold Letz: FTP 2005 – Fifth International Workshop on First-Order Theorem Proving, Fachberichte Informatik 13-2005

Bernhard Beckert: TABLEAUX 2005 – Position Papers and Tutorial Descriptions, Fachberichte Informatik 12-2005

Dietrich Paulus and Detlev Droege: Mixed-reality as a challenge to image understanding and artificial intelligence, Fachberichte Informatik 11-2005

Jürgen Sauer: 19. Workshop Planen, Scheduling und Konfigurieren / Entwerfen, Fachberichte Informatik 10-2005

Pascal Hitzler, Carsten Lutz, and Gerd Stumme: Foundational Aspects of Ontologies, Fachberichte Informatik 9-2005

Joachim Baumeister and Dietmar Seipel: Knowledge Engineering and Software Engineering, Fachberichte Informatik 8-2005

Benno Stein and Sven Meier zu Eißen: Proceedings of the Second International Workshop on Text-Based Information Retrieval, Fachberichte Informatik 7-2005

Andreas Winter and Jürgen Ebert: Metamodel-driven Service Interoperability, Fachberichte Informatik 6-2005

Joschka Boedecker, Norbert Michael Mayer, Masaki Ogino, Rodrigo da Silva Guerra, Masaaki Kikuchi, and Minoru Asada: Getting closer: How Simulation and Humanoid League can benefit from each other, Fachberichte Informatik 5-2005

Torsten Gipp and Jürgen Ebert: Web Engineering does profit from a Functional Approach, Fachberichte Informatik 4-2005

Oliver Obst, Anita Maas, and Joschka Boedecker: HTN Planning for Flexible Coordination Of Multiagent Team Behavior, Fachberichte Informatik 3-2005

Andreas von Hessling, Thomas Kleemann, and Alex Sinner: Semantic User Profiles and their Applications in a Mobile Environment, Fachberichte Informatik 2-2005

Heni Ben Amor and Achim Rettinger: Intelligent Exploration for Genetic Algorithms – Using Self-Organizing Maps in Evolutionary Computation, Fachberichte Informatik 1-2005