



Deutsche Richterakademie
Trier

Der CCC, Hackerkultur und Computer(un)sicherheit

Sebastian Zimmermann
Chaos Computer Club München
E-Mail: info@muc.ccc.de
18.03.2015





Inhalt des Vortrags

1. Teil: Chaos Computer Club und Hackerkultur

- Chaos Computer Club (CCC)
- Hackerkultur
- Beispiele der thematischen Arbeit des CCC

2. Teil: IT-Security / Methodik Penetrationstests

- Kurzeinführung Internet-Grundlagen
- Sniffing, Vulnerability Scanning und Exploiting
- Webapp-Sicherheit
- E-Mails: Datenspuren und Manipulationsmöglichkeiten
- Grundlagen der Verschlüsselung



1. Teil

Chaos Computer Club (CCC) und Hackerkultur



Selbstverständnis des CCC

Die Entwicklung zur Informationsgesellschaft erfordert ein neues Menschenrecht auf weltweite, ungehinderte Kommunikation. Der Chaos Computer Club ist eine galaktische Gemeinschaft von Lebewesen, unabhängig von Alter, Geschlecht und Abstammung so wie gesellschaftlicher Stellung, die sich grenzüberschreitend für Informationsfreiheit einsetzt und mit den Auswirkungen von Technologien auf die Gesellschaft sowie das einzelne Lebewesen beschäftigt und das Wissen um diese Entwicklung fördert.

Aus der Präambel der Satzung des CCC e.V.



Aktionen

TUWAT, TKT Version

Daß die innere Sicherheit erst durch Computereinsatz möglich wird, glauben die Mächtigen heute alle. Daß Computer nicht streiken, setzt sich als Erkenntnis langsam auch bei mittleren Unternehmen durch. Daß durch Computereinsatz das Telefon noch schöner wird, glaubt die Post heute mit ihrem Bildschirmtextsystem in „Feidversuchen“ beweisen zu müssen. Daß der „personal computer“ nun in Deutschland dem videogesättigten BMW-Fahrer angedreht werden soll, wird durch die nun einsetzenden Anzeigenkampagnen klar. Daß sich mit Kleinkomputern trotzdem sinnvolle Sachen machen lassen, die keine zentralisierten Großorganisationen erfordern, glauben wir. Damit wir als Computerfreaks nicht länger unkoordiniert vor uns hinwuseln, tun wir wat und treffen uns am 12.9. 81 in Berlin, Wattstr. (TAZ-Hauptgebäude) ab 11.00 Uhr. Wir reden über: internationale Netzwerke - Kommunikationsrecht - Datenrecht (Wem gehören meine Daten?) - Copyright - Informations- u. Lernsysteme - Datenbanken - Encryption - Computerspiele - Programmiersprachen - processcontrol - Hardware - und was auch immer.
Tom Twiddlebit, Wau Wolf Ungenann (2)*

*Damit hing es an
'Die Tageszeitung'
1.9.81*



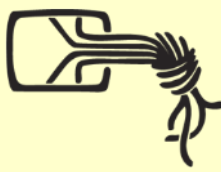
Was macht eigentlich der CCC?

- Geschichte
 - Entstanden vor 32 Jahren als Treff von Computerfreaks („Tuwat“-Treffen am 12.9.1981 in den Räumen der Tageszeitung am großen Tisch der Kommune I, initiiert von Wau Holland)
 - Seit 1984 Herausgabe der Zeitschrift "Datenschleuder" und Veranstaltung des jährlichen Chaos Communication Congress
 - 1986 Gründung des Chaos Computer Club e.V.
 - Heute dezentrale Hackerspaces und lokale Vereine (z.B. CCC München seit 1999)
 - Stand 2014: mehr als 5000 Mitglieder

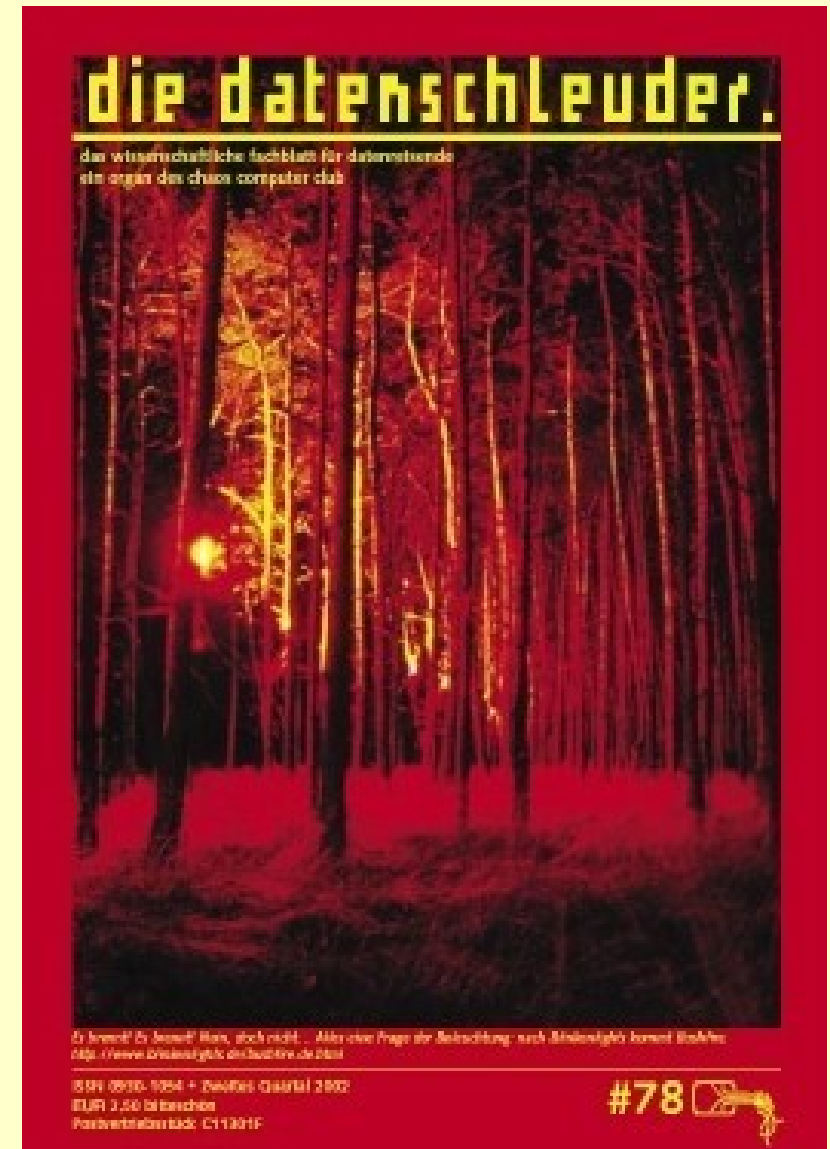
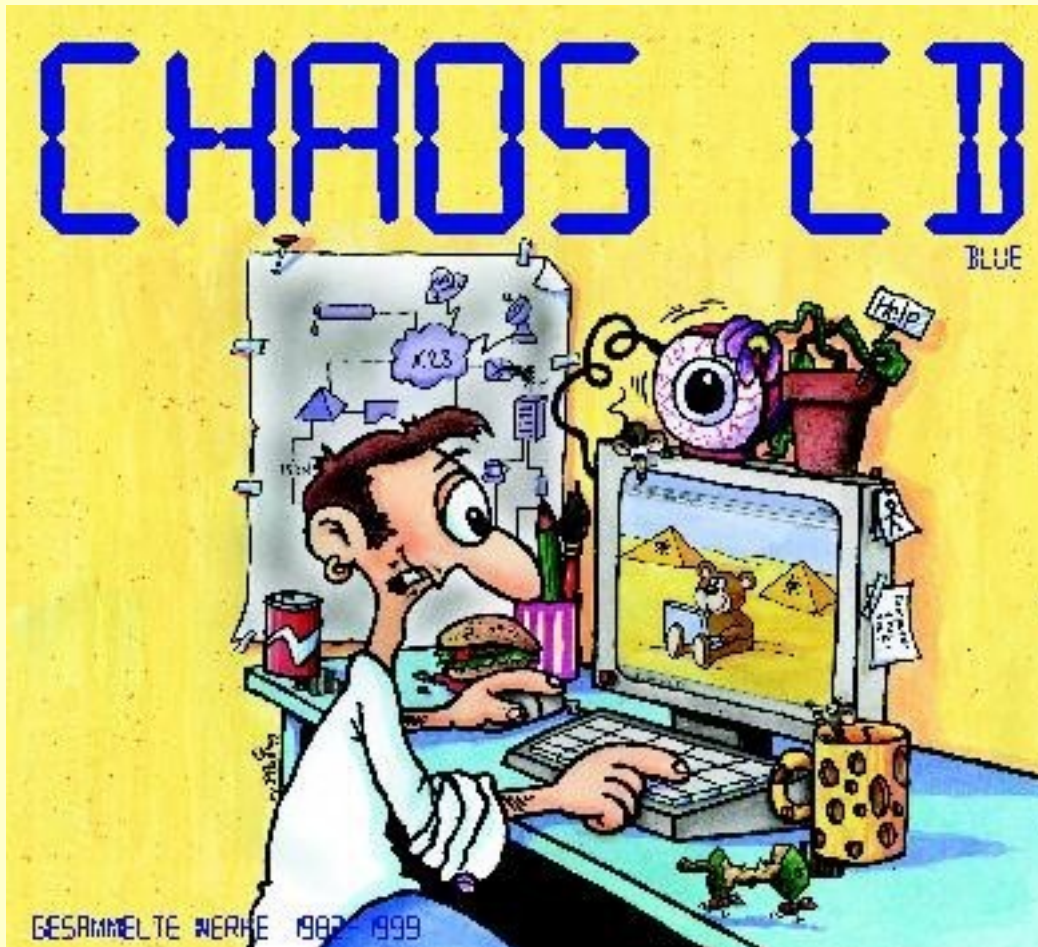


Was macht eigentlich der CCC?

- Vereinsziele
 - Einsatz für ein Menschenrecht auf weltweite ungehinderte Kommunikation
 - Förderung von Informationsfreiheit und Transparenz
 - Auseinandersetzung mit gesellschaftlichen Folgen von Technologie (Risiken und Chancen)
 - Aufklärung / Debattenbeiträge



Publikationen



Chaos Communication Congress



Bild: Wikipedia / Tobias Klenze / CC-BY-SA 3.0



Bild: Wikipedia / Tobias Klenze / CC-BY-SA 3.0

Bild: blinkenarea.org, Lizenz: CC BY-SA 2.0



Chaos Communication Camp

Finowfurt, 2011



Zunkel (CC-BY-NC 2.0)

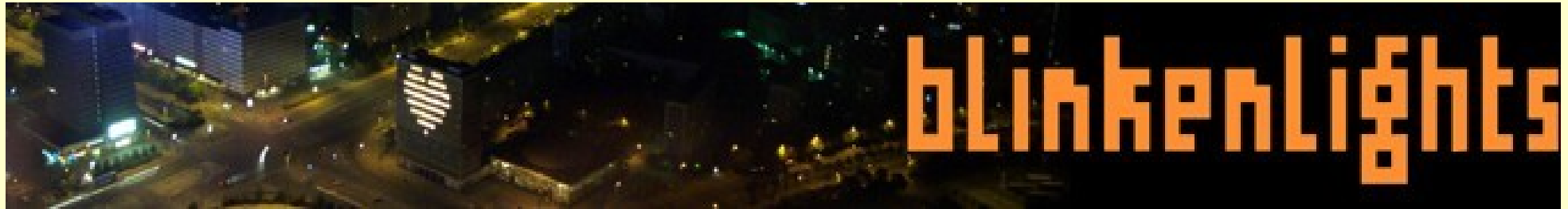


Chaos Communication Camp



Berlin 1999

Hackerkultur kreative Technikanwendungen



blinkenlights /blink'*n-li:tz/ n.

[common] Front-panel diagnostic
lights on a computer.



Hackerkultur

Kreative Technikanwendungen



Arcade

Nuit Blanche
2002
Paris





(Netz-) Politische Themen





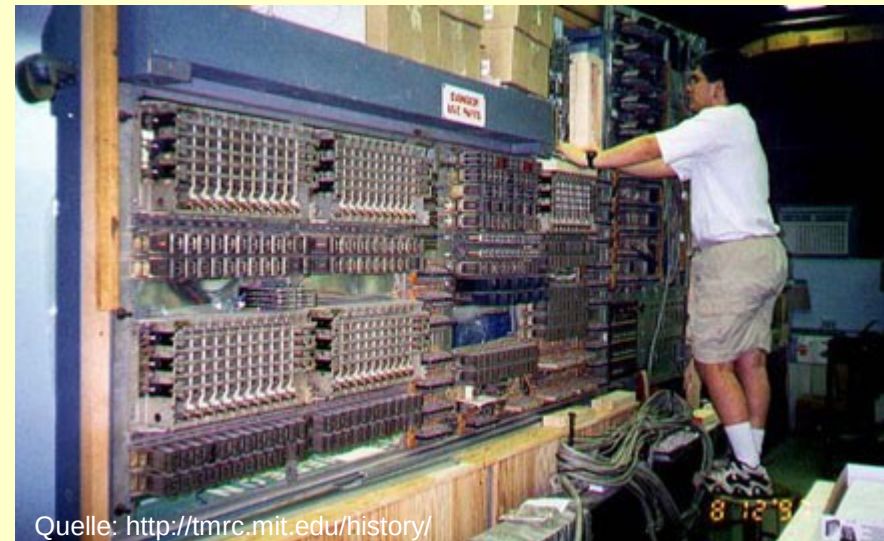
„Hacker“

- In der Presse und Öffentlichkeit:
 - Personen, die in Computer einbrechen
- Hacker selbst:
 - Kreativer Umgang mit Technik (z.B. Kaffeekochen mit dem Toaster)
 - „Man kann Kunst und Schönheit mit dem Computer schaffen.“ (z.B. Blinkenlights)
 - Nichts als gegeben hinnehmen
- Hacken ist eine Lebensanschauung!



Ursprung der Hackerkultur

- MIT Tech Model Railroad Club (TMRC)
 - Gegründet 1946, Fokus auf Steuerungstechnik und Automatisierung
 - Hat viele Begriffe geprägt (ab Ende 50er Jahre)
 - **„Hack“: clevere und effektive technische Lösung**
 - „Foo – Bar“





Einige Begriffe aus der Hackerkultur

Hacker:	Neugier, Förderung von Informationsfreiheit und Transparenz "White Hat Hacker"
Cracker:	Befreiung eingesperrter Bits (Kopierschutz) auch: "Hacker" mit kriminellem Hintergrund "Black Hat Hacker"
Script-Kiddies:	Oft Jugendliche, kennen Hackertools, Machtgefühl, wenig Verständnis der Technik
Kriminelle:	materielle/eigennützige Interessen
Spione:	Zugang und Verfälschung von Informationen
Infowar:	Elektronische Kriegsführung

Personen, die aus Eigennutz in Computer eindringen und Daten stehlen, sind keine Hacker, sondern Kriminelle!



Hackerethik des CCC

- Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Mißtraue Autoritäten - fördere Dezentralisierung
- Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern.
- **Mülle nicht in den Daten anderer Leute.**
- **Öffentliche Daten nützen, private Daten schützen.**

(Ursprung: Buch "Hackers" von Steven Levy)

Kulturwandel zum „Spaß-Hacktivismus“: Anonymous



- Anonymous: hervorgegangen u.a. aus 4chan als "offene" Bewegung
- Proteste gegen Anonymous, RIAA, IFPI, Sony Mastercard, Payback und andere
- Angriffe auf Infrastrukturen werden als legitime Ausdrucksweise des Protests betrachtet.



FreedomFone gegen Internet-Sperren



Zensurfrees Internet mit FreedomFone: (01 90) 70 60 98

http://w2p.odem.org/ Google

FreedomFone

0190 70 60 98*

* nur 1,24 €/min. Bitte lesen Sie unsere [Allgemeinen Geschäftsbedingungen](#).

Sie nennen uns eine Internetseite - wir lesen Sie Ihnen vor!

Immer mehr Internetseiten werden abgeriegelt, um die Nutzer vor bestimmten Inhalten zu schützen: Nur noch eingeschränkt surfen lässt sich beispielsweise bereits in [Nordrhein-Westfalen](#) oder in [China](#).

Das ist erst der Anfang - der Markt an gefilterter Information wird täglich größer wie eine Studie der renommierten Bertelsmann-Stiftung zeigt ([Bertelsmann-Studie](#)).

[->Mehr Details zum FreedomFone-Service](#)

FreedomFone Top7:

Die beliebtesten Web-Adressen bei FreedomFone in den letzten 24 Stunden:

1. [terrorvictims.ir](#)
2. [tdcj.state.tx.us/stat/execut...](#)
3. [a-blast.org/www.angelfire.co...](#)
4. [ivvdn.de/antifa/](#)
5. [xmule.org](#)
6. [naziline.com](#)
7. [kpd.de](#)

My FreedomFone

- [Home](#)
- [Der FreedomFone-Service](#)
- [Häufig gestellte Fragen](#)
- [Karriere bei FreedomFone](#)
- [Presse](#)
- [Forum](#)
- [Allgemeine Geschäftsbedingungen](#)
- [English Version](#)

Jetzt anrufen:
0190 70 60 98*

FreedomFone Newsletter

em@il

Bitte tragen Sie hier Ihre Email-Adresse ein und drücken Sie "abonnieren", um regelmäßig Tipps zu den heißesten Internetseiten zu erhalten.

Member Login:

Name:

Passwort:

* nur 1,24 €/min. Bitte lesen Sie unsere [Allgemeinen Geschäftsbedingungen](#).

Wer braucht FreedomFone??

Manchmal ist ein ungefilterter Zugriff auf Internetseiten sinnvoll. FreedomFone wendet sich deshalb vor allem an:

- Journalisten, Studenten oder Lehrkräfte, die Forschungsarbeit leisten

ACHTUNG! 1. September 2004:

FreedomFone launcht neue Hochschulkampagne: Als Student oder Dozent einer Universität oder



Internet Mem

- Ein Mem ist ein Gedanke oder Bewusstseinsinhalt, der durch Kommunikation verbreitet wird und ähnlichen Mechanismen unterliegt wie ein Gen (nach Richard Dawkins, 1976).
- „Internet Meme“ sind Internet-Phänomene, bei denen sich bestimmte Bilder oder andere Medien schnell im Internet verbreiten. Sie sind meist humoristischer oder schockierender Natur.
- siehe auch: <http://knowyourmeme.com/>



Internet-Phänomen: Rickrolling

- „Internet-Spaß“: Locken von Leuten auf ein Video von Rick Astley (Never Gonna Give You Up).
- Beispiel:
 - Hier gibt es die [Abiprüfung](#) vorab!
- Ursprung:
 - vermutlich 4chan.org



Internet-Phänomen: Hitler reacts



Quelle: Youtube <https://www.youtube.com/watch?v=gAFyUVK7T8Q>



Beispiele der thematischen Arbeit des CCC:

**Wahlcomputer
Staatstrojaner**



Wahlcomputer

Wie man einen Wahlbetrug erkennt:



Dies ist ein Wahlcomputer

Dies ist ein manipulierter Wahlcomputer



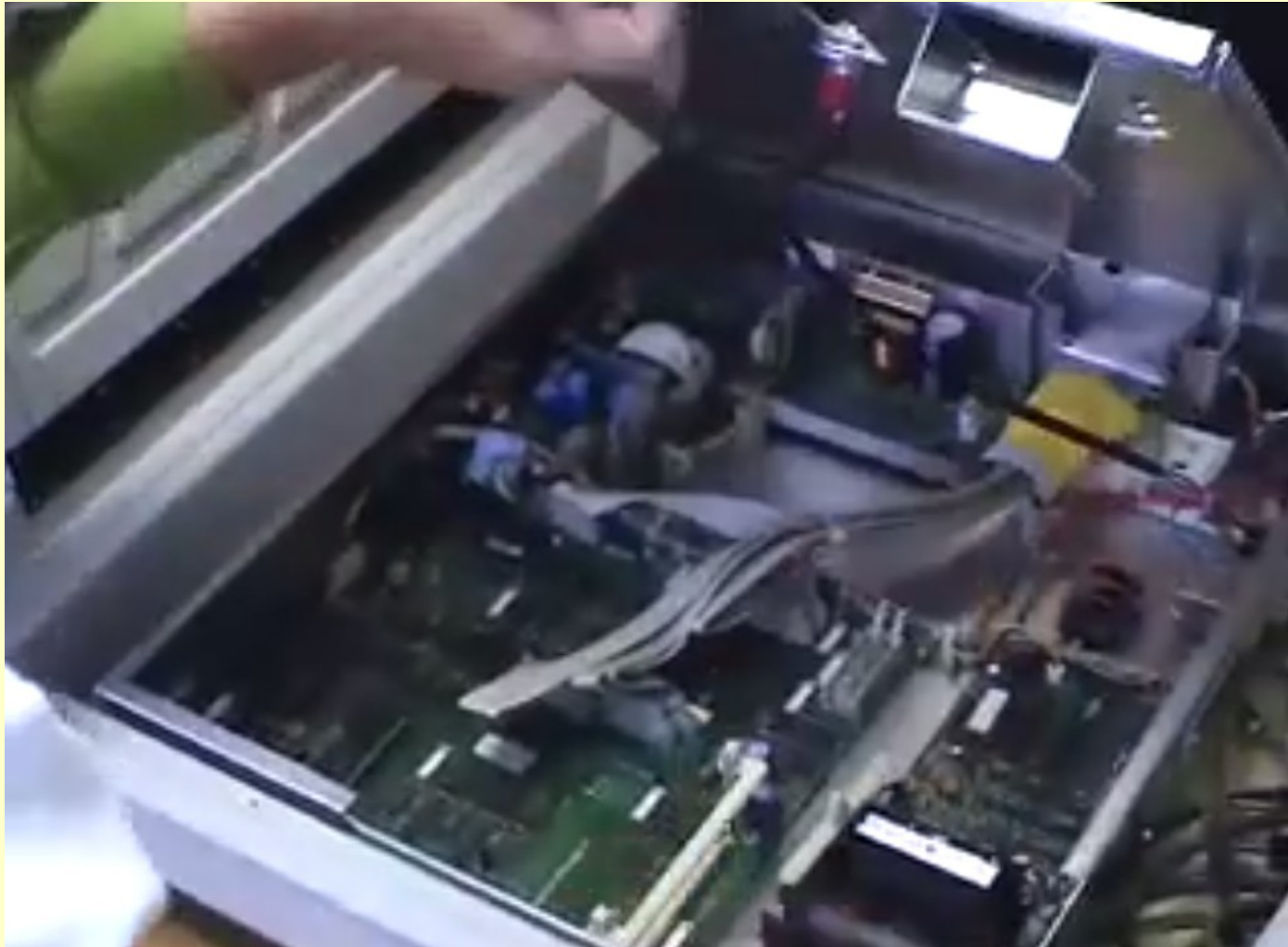
NEDAP Wahlcomputer



Quelle: <http://wijvertrouwenstemcomputersniet.nl>



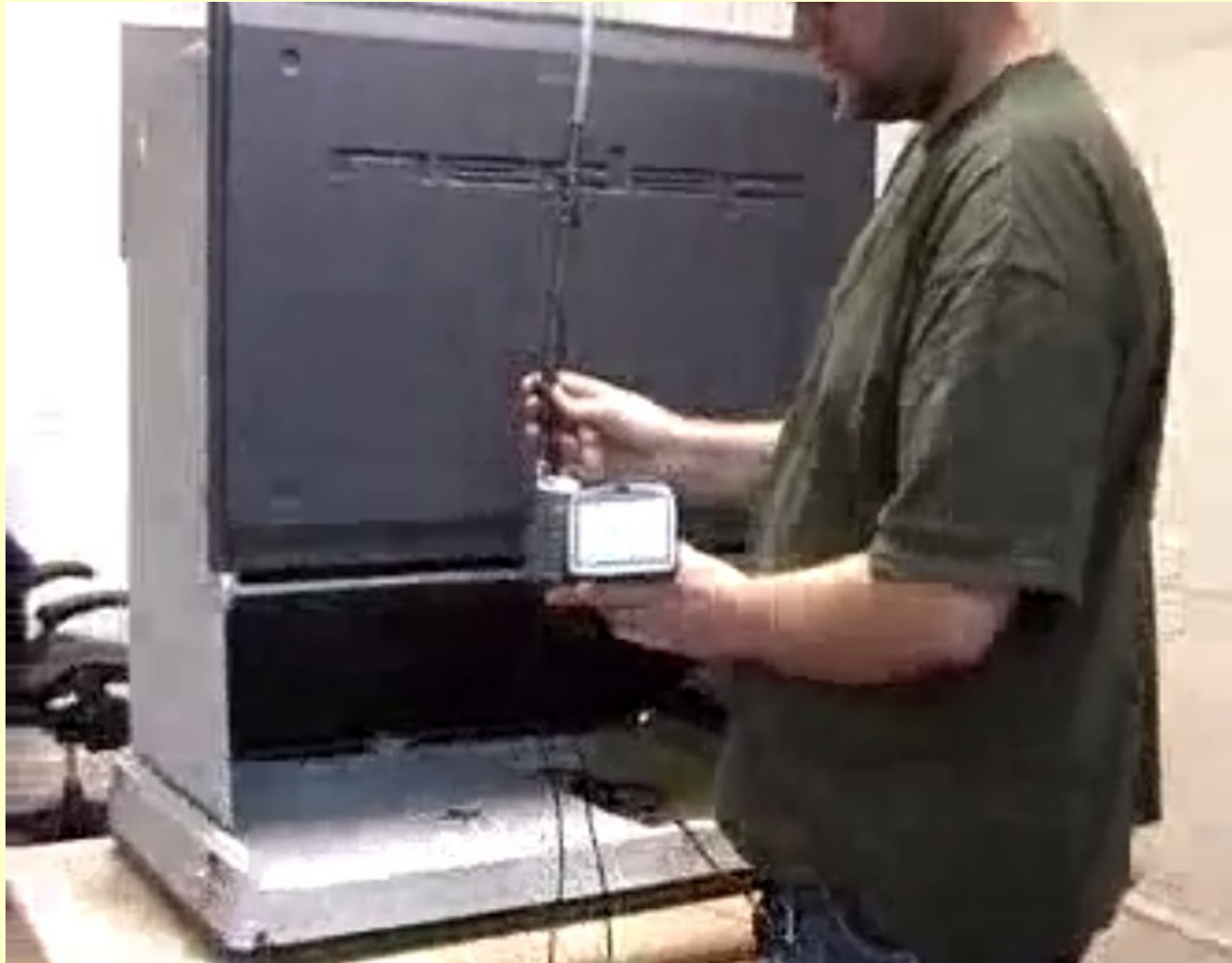
Austausch der Software



Quelle: <http://wijvertrouwenstemcomputersniet.nl>



Tempest-Angriff



Quelle: <http://wijvertrouwenstemcomputersniet.nl>

„Bundestrojaner“





Stellenanzeige Bundestrojaner

Bundeskriminalamt

Technische Unterstützung bei der Bekämpfung der Computer-Kriminalität

Moderne Technik steigert die Effektivität der Methoden der Strafverfolgung, aber auch Straftäter nutzen komplexe Technologie für bisher unbekannte Kriminalitätsformen.

Das **Kriminalistische Institut im Bundeskriminalamt** verstärkt seine Initiativen zur Bewältigung der Herausforderungen, die neue Technologien an die Deutsche Polizei stellen, durch eine personelle Verstärkung des technischen Servicezentrums für Informations- und Kommunikationstechnologien (TeSiT) in Mendenham.

Sie sind IT-Spezialist/in und haben Interesse an kriminalistischer Arbeit und daran, einen neuen Arbeitsbereich aktiv mitzugestalten?

Wir haben unser Team im Bereich der Entwicklung neuer Ermittlungsmethoden zur Verfolgung von Straftaten unter Ausnutzung von Informations- und Kommunikationstechnologien aus und suchen einen:

wissenschaftliche/n Mitarbeiter/in Kennziffer: BKA-09-2008

zur Konzeption und Durchführung technischer Untersuchungen bei Straftaten im Zusammenhang mit Computernetzwerken

Ihre Aufgaben:

- Ausarbeitung und Durchführung von Entwicklungsvorhaben mit Bezug zur IuK-Kriminalität
- Entwicklung und Anpassung fachspezifischer Softwarewerkzeuge
- Analyse von Schadprogrammen und von Angriffsszenarien
- Beobachtung der technischen Entwicklung sicherheitsrelevanter Programme und technische Bewertung der Auswirkungen auf die polizeiliche Arbeit

Ihre Qualifikation:

- Hochschulabschluss einer technischen Fachrichtung (z.B. Informatik, Physik, Mathematik) und mehrjährige Berufserfahrung im Bereich IT-Sicherheit (vorzugsweise im Bereich Netzwerk-/Systemicherheit)
- Umfassende Kenntnisse der Internettechnologie und Kenntnisse über die verwendete Hardware einschl. Speichermedien
- Sehr gute Kenntnisse im Bereich der Sicherheit von Computernetzwerken
- Fundierte Betriebssystemkenntnisse Unix/Linux und Windows
- Sehr gute Kenntnisse und mehrjährige Erfahrung in Programmierung (C, C++)
- Kenntnisse einschlägiger Rechtsvorschriften sind wünschenswert

Darüber hinaus können Sie sich ziel- und lösungsorientiert in kriminalpolizeiliche Anforderungen einarbeiten und diese schnell umsetzen, sind team- und kommunikationsfähig.

Wegen der Vielzahl der internationalen Kontakte werden auch gute englische Sprachkenntnisse vorausgesetzt.

Darüber hinaus suchen wir einen:

Entwickler/in / Programmierer/in Kennziffer: BKA-10-2008

zur Konzeption und Durchführung technischer Untersuchungen bei Straftaten im Zusammenhang mit Computernetzwerken

Ihre Aufgaben:

- Mitarbeit in Forschungs- und Entwicklungsvorhaben mit Bezug zur IuK-Kriminalität
- Entwicklung und Anpassung fachspezifischer Softwarewerkzeuge
- Analyse von Schadprogrammen und von Angriffsszenarien
- Beobachtung der technischen Entwicklung sicherheitsrelevanter Programme und technische Bewertung der Auswirkungen auf die polizeiliche Arbeit

Ihre Qualifikation:

- Hochschulabschluss einer technischen Fachrichtung (z.B. Informatik, Physik, Mathematik) und mehrjährige Berufserfahrung im Bereich IT-Sicherheit (vorzugsweise im Bereich Netzwerk-/Systemicherheit)
- Umfassende Kenntnisse der Internettechnologie und Kenntnisse über die verwendete Hardware einschl. Speichermedien
- Sehr gute Kenntnisse im Bereich der Sicherheit von Computernetzwerken
- Fundierte Betriebssystemkenntnisse Unix/Linux und Windows
- Sehr gute Kenntnisse und mehrjährige Erfahrung in Programmierung (C, C++)
- Kenntnisse einschlägiger Rechtsvorschriften sind wünschenswert

Darüber hinaus können Sie sich ziel- und lösungsorientiert in kriminalpolizeiliche Anforderungen einarbeiten und diese schnell umsetzen, sind team- und kommunikationsfähig.

Wegen der Vielzahl der internationalen Kontakte werden auch gute englische Sprachkenntnisse vorausgesetzt.

Wir bieten Ihnen für beide Stellen:

- Ein vielfältiges Aufgabenspektrum, das Kreativität, Vision und ein hohes Maß an Eigeninitiative erfordert
- Die Möglichkeit, einen neuen Arbeitsbereich aktiv mitzugestalten
- Die Mitarbeit in einem hoch motivierten Team
- Aufgabenbezogene Aus- und Fortbildung
- Der Aufbau und die Nutzung nationaler und internationaler Kooperationen

Eine Bezahlung nach Entgeltgruppe 14 TVSO des Tarifvertrages für den öffentlichen Dienst (TVöD) für den wissenschaftlichen Mitarbeiter

Eine Bezahlung nach Entgeltgruppe 11 TVöD des Tarifvertrages für den öffentlichen Dienst (TVöD) für den Entwickler bzw. Programmierer

- Bona die üblichen Sozialleistungen des öffentlichen Dienstes
- Bis zum Inkrafttreten der neuen Entgeltordnung ist die hier dargestellte Eingruppierung vorläufig und begründet keinen Vertrauensschutz und keinen Bestands (§ 17 Abs. 3 Satz 1 TVöD-Günd).

Die Stellen sind auf 2 Jahre befristet.

Das Bundeskriminalamt fördert die Gleichstellung von Frauen und Männern und ist deshalb besonders an Bewerbungen von Frauen interessiert, um diesen Anteil auch im vergleichbar höheren Dienst zu steigern. Das Bundeskriminalamt unterstützt auch die Vereinbarkeit von Familie und Beruf durch flexible Arbeitszeiteinstellung im Rahmen der dienstlichen Möglichkeiten. Schwerbehinderte Bewerberinnen und Bewerber werden bei gleicher Eignung bevorzugt. Von ihnen wird nur ein Mindestmaß an körperlicher Eignung verlangt.

Füllen Sie sich angesprochen? Dann bewerben Sie sich bitte bis zum **05.03.2008** über das jeweilige im Internet eingestellte Online-System.

Der Link zur Kennziffer **BKA-09-2008** (wissenschaftliche/n Mitarbeiter/in) lautet:
<https://onlinebewerbung.dienstleistungszentrum.de/BKA-09-2008>

Der Link zur Kennziffer **BKA-10-2008** (Entwickler/in / Programmierer/in) lautet:
<https://onlinebewerbung.dienstleistungszentrum.de/BKA-10-2008>

Sie gelangen zu dem jeweiligen Online-System auch über www.dienstleistungszentrum.de (Personalgewinnung/Stellenausschreibungen). Passwort und Account erhalten Sie unter Angabe Ihrer E-Mail-Adresse. Übersenden Sie weitere Bewerbungsunterlagen (z.B. Zeugnisse, Referenzen, Beschäftigungsnachweise) bitte erst nach Aufforderung.

Für Fragen im Zusammenhang mit Ihrer Bewerbung steht Ihnen Herr Schweitz (Tel. 022893 358-5616) vom Servicezentrum Personalgewinnung des Bundesverwaltungsamtes gerne zur Verfügung.

Weitere Informationen über das Bundeskriminalamt finden Sie unter www.bka.de.

BKA

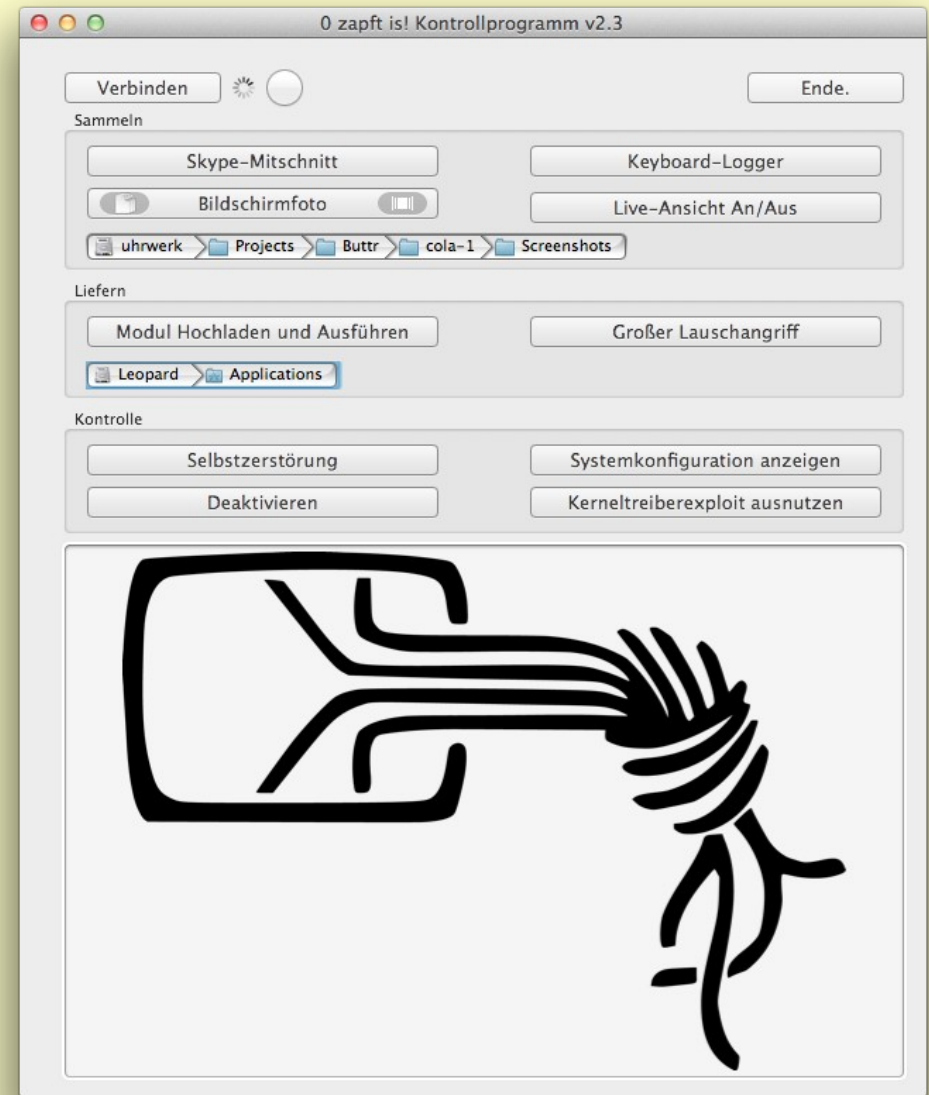
Ihre Aufgaben:

- Ausarbeitung und Durchführung von Entwicklungsvorhaben mit Bezug zur IuK-Kriminalität
- Entwicklung und Anpassung fachspezifischer Softwarewerkzeuge
- Analyse von Schadprogrammen und von Angriffsszenarien
- Beobachtung der technischen Entwicklung sicherheitsrelevanter Programme und technische Bewertung der Auswirkungen auf die polizeiliche Arbeit

Ihre Qualifikation:

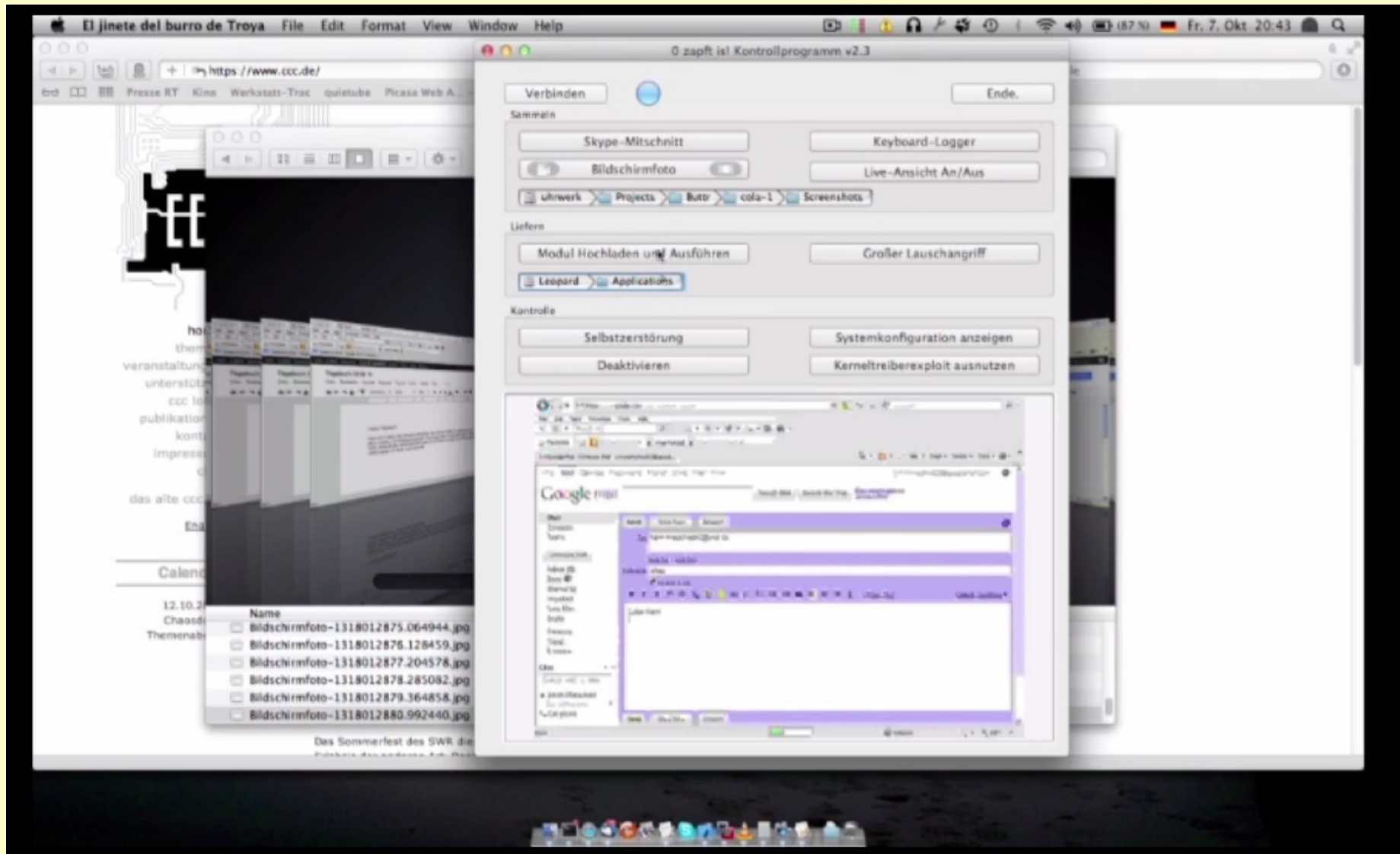
- Hochschulabschluss einer technischen Fachrichtung (z.B. Informatik, Physik, Mathematik) und mehrjährige Berufserfahrung im Bereich IT-Sicherheit (vorzugsweise im Bereich Netzwerk-/Systemicherheit)
- Umfassende Kenntnisse der Internettechnologie und Kenntnisse über die verwendete Hardware einschl. Speichermedien
- Sehr gute Kenntnisse im Bereich der Sicherheit von Computernetzwerken
- Fundierte Betriebssystemkenntnisse Unix/Linux und Windows
- Sehr gute Kenntnisse und mehrjährige Erfahrung in Programmierung (C, C++)
- Kenntnisse einschlägiger Rechtsvorschriften sind wünschenswert

Staatstrojaner-Analyse des CCC

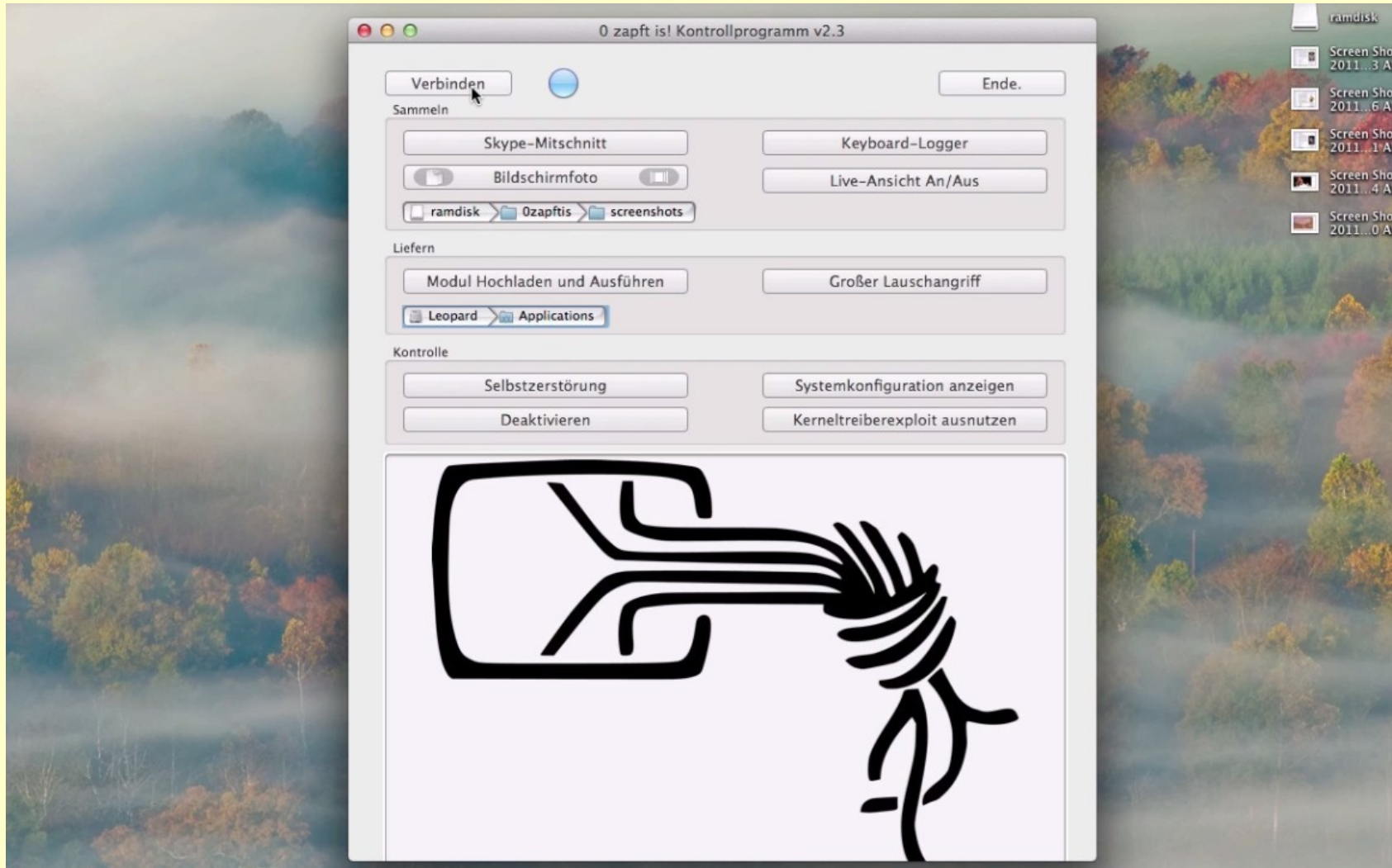




Staatstrojaneranalyse (Bayern)



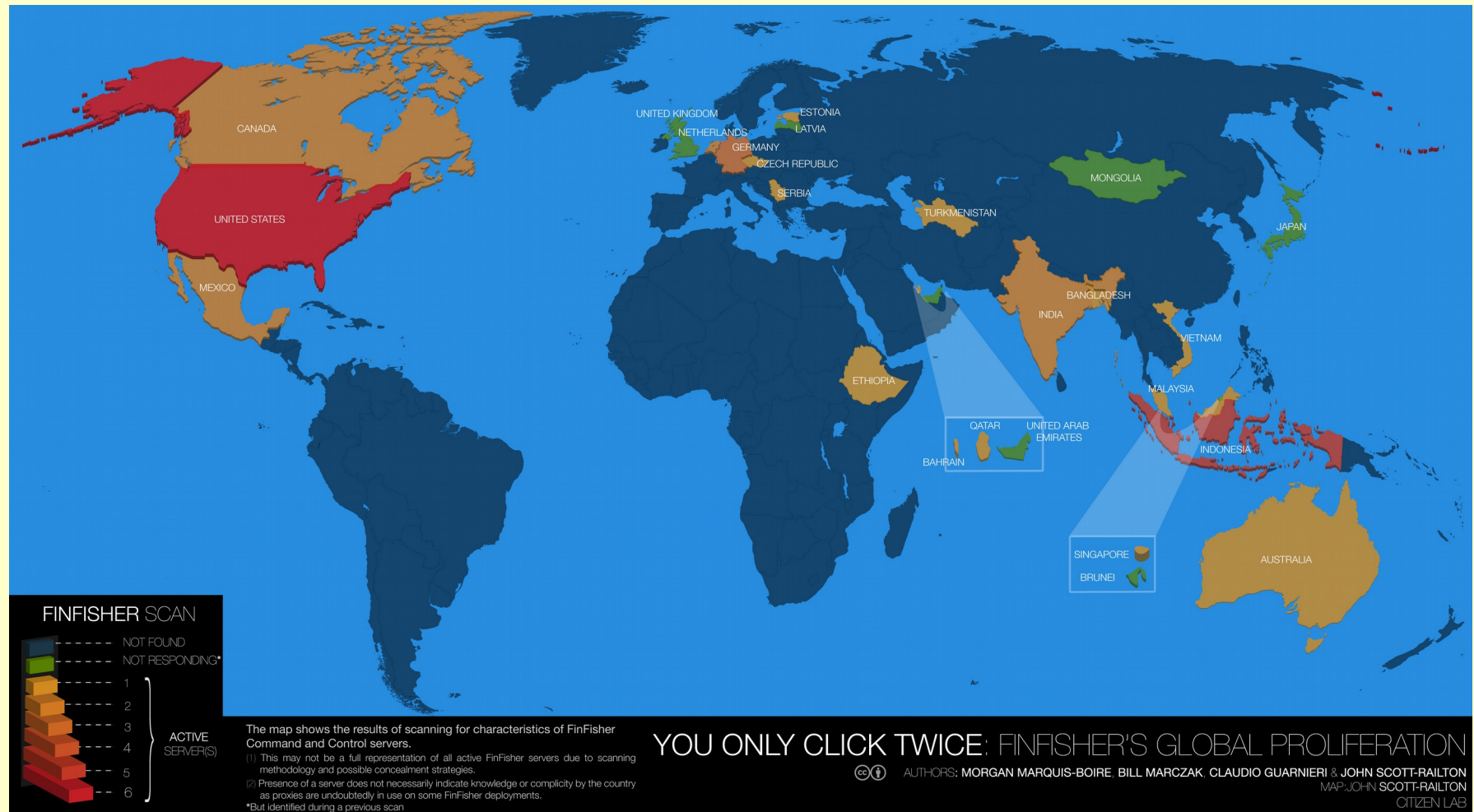
Staatstrojaneranalyse (BKA?)





FinFisher von Gamma International

genutzt u.a. in: Bahrain, Brunei, Äthiopien, Katar, Turkmenistan, Vereinigte Arabische Emirate, Vietnam



Lizenz: CC – Quelle: Citizenlab.org – Autoren: Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, John Scott-Railton



Stuxnet („Projekt Myrtus“)

- Wurm, entdeckt im Juni 2010
- Schadfunktion zielte auf SCADA-Systeme (industrielle Steueranlagen)
- Ziel vermutlich Frequenzumrichter von Zentrifugen zur Urananreicherung
- Verwendete vier bislang unbekannte Schwachstellen in Windows (Zero Days), sehr robust programmiert



Quelle:
<http://gentleseas.blogspot.com>

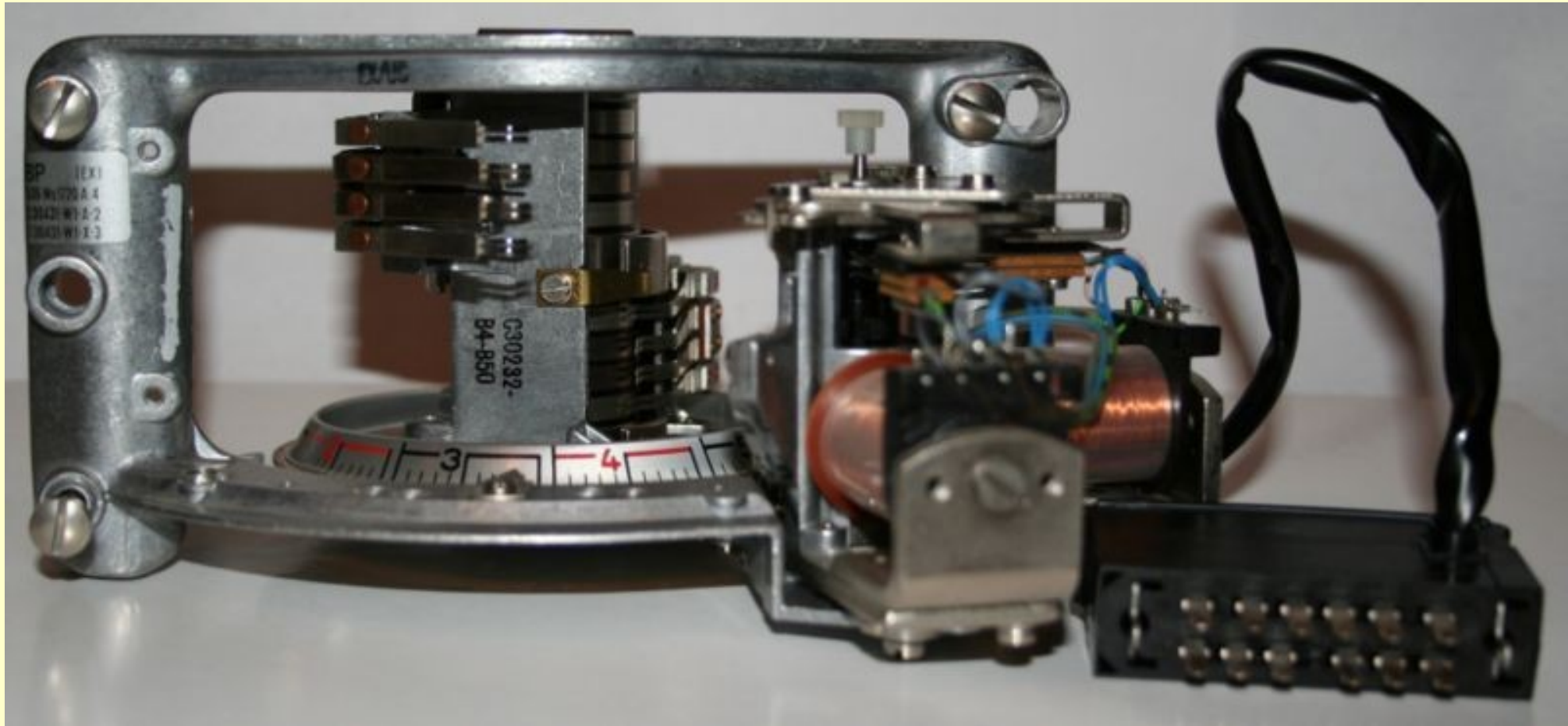


2. Teil

IT-Security Methodik Penetrationstests



Internet-Grundlagen



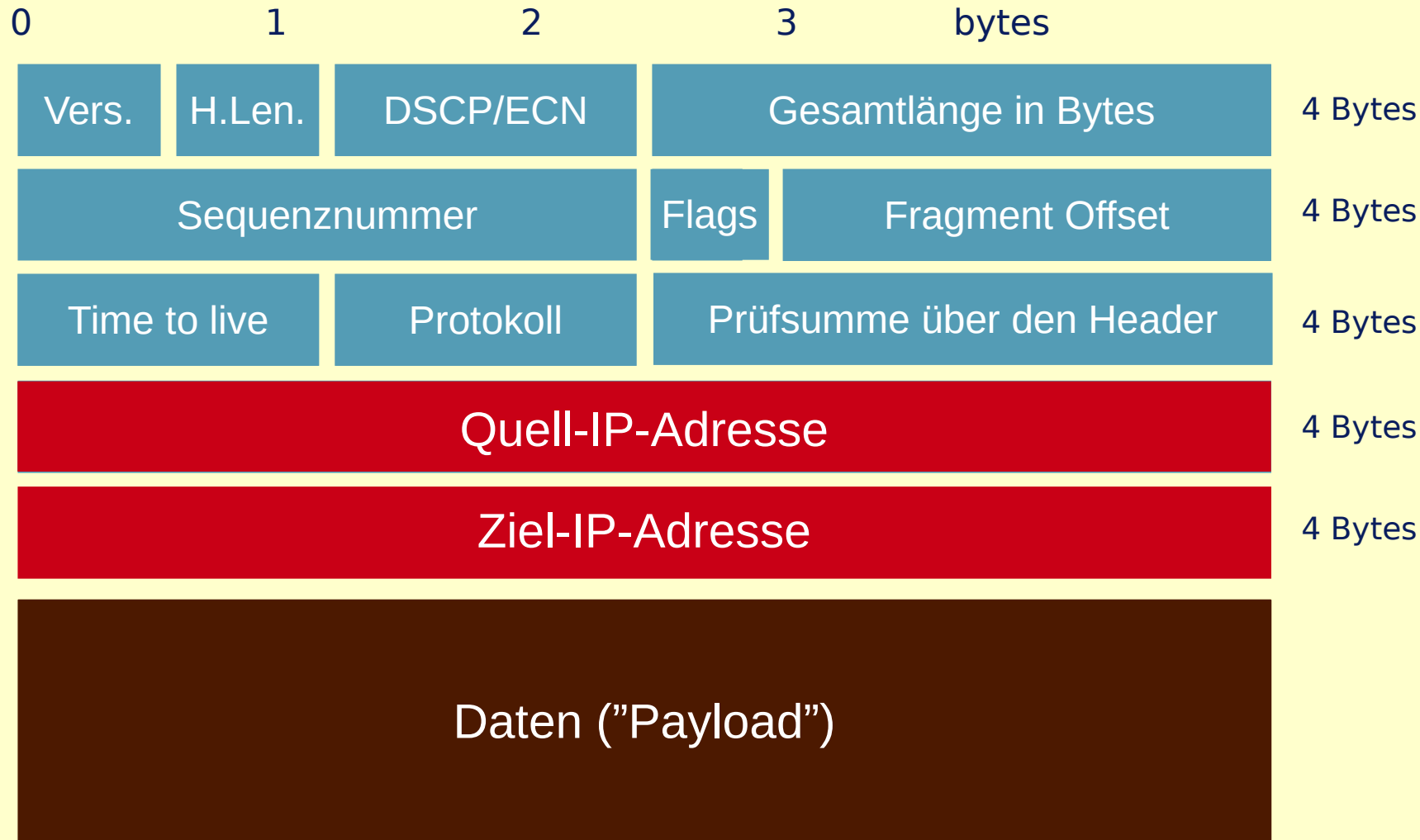
Edelmetall-Motor-Drehwähler

(Foto: Michael Gernoth, Creative Commons Attribution 2.5 Lizenz)



IP-Paket: Aufbau

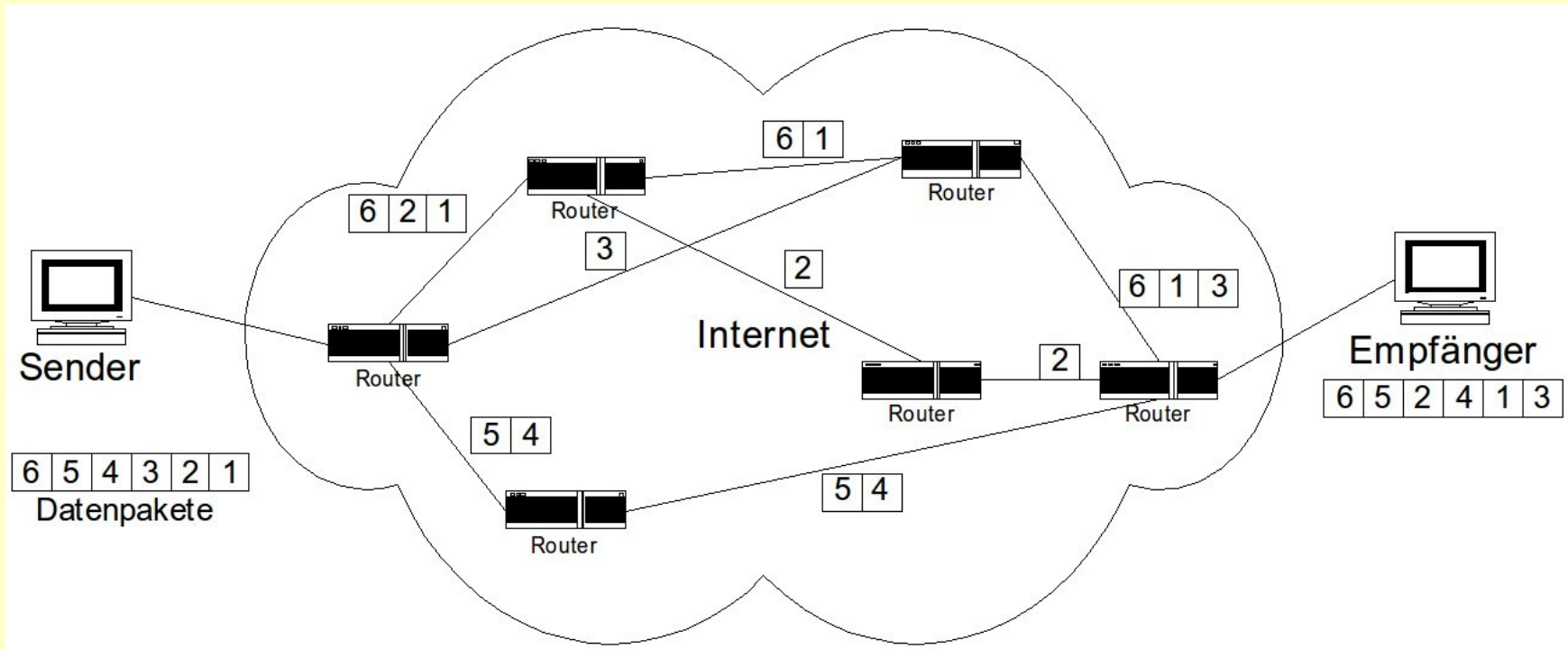
20 Byte Kopfinformationen (Header), zzgl.
Optionen



IP-Definition in RFC 791 (Request for Comments)
<http://www.rfc-editor.org/rfc/rfc791.txt>



Paketorientierte Kommunikation



- **Packet Routing vs. Circuit Switching** (Leitungsvermittlung): Datenpakete statt Datenkanäle
 - Keine feste Leitung vom Sender zum Empfänger, sondern Zerlegung der Daten beim Sender in Pakete, die einzeln auf die Reise geschickt und beim Empfänger wieder zusammengesetzt werden.
 - Jedes Paket kann einen anderen Weg nehmen.
 - **Sender und Empfänger müssen daher in jedem Paket angegeben sein.**



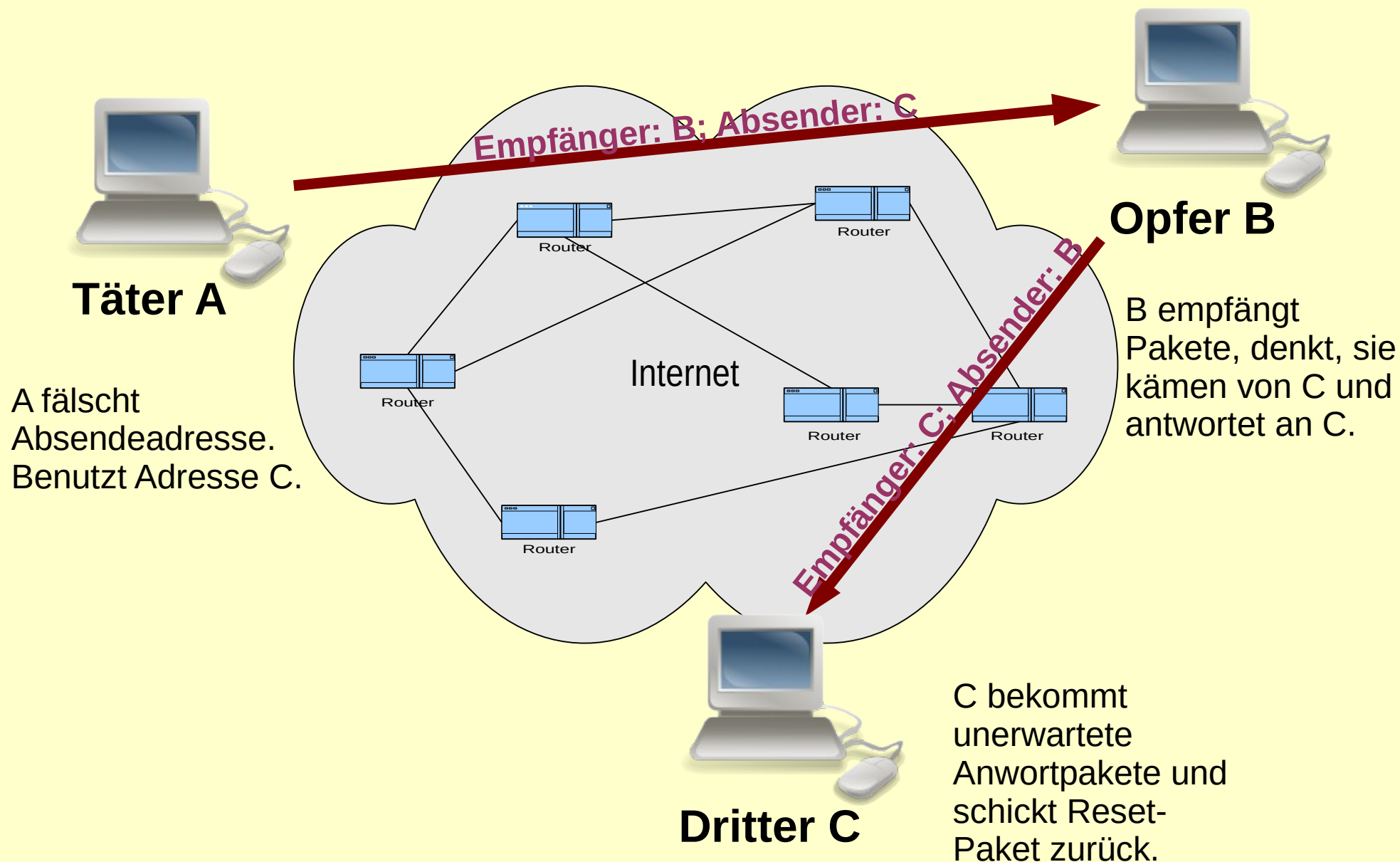
Nameserver

- Für Menschen sind numerische Adressen schwer zu merken.
- Daher sorgt das **DNS (Domain Name System)** dafür, dass Namen statt Nummern verwendet werden können.



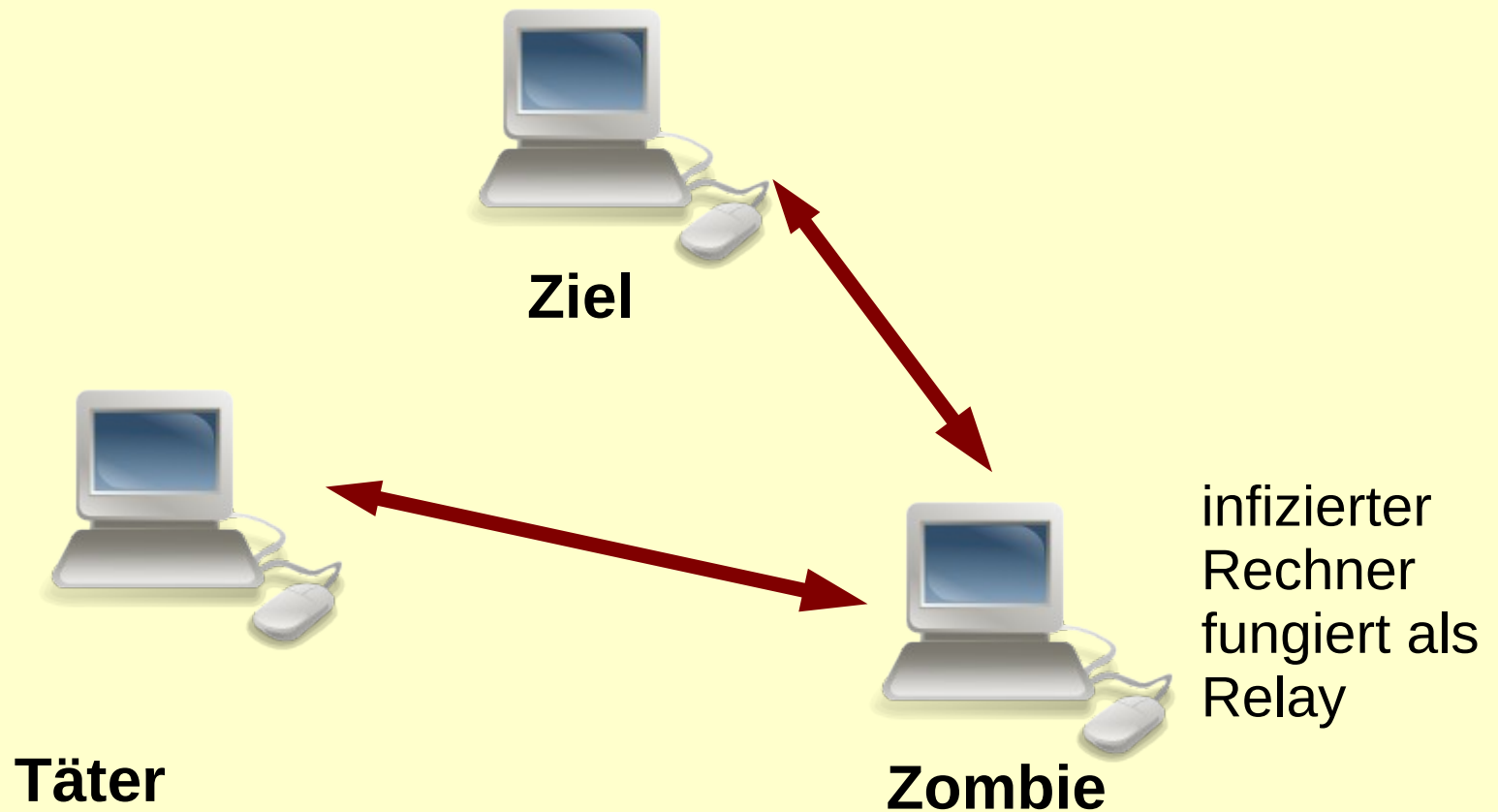
- Zu jedem Webseiten-Aufruf gehört eine Namensauflösung.
- Normalerweise Anfrage an Server des Providers
 - kann protokolliert werden
- **Pharming**: Gefälschte IP-Adresszuordnungen
 - Beispiel: gefälschte Bankenwebseite, z.B. durch Virus

IP-Spoofing („echtes IP-Spoofing“)





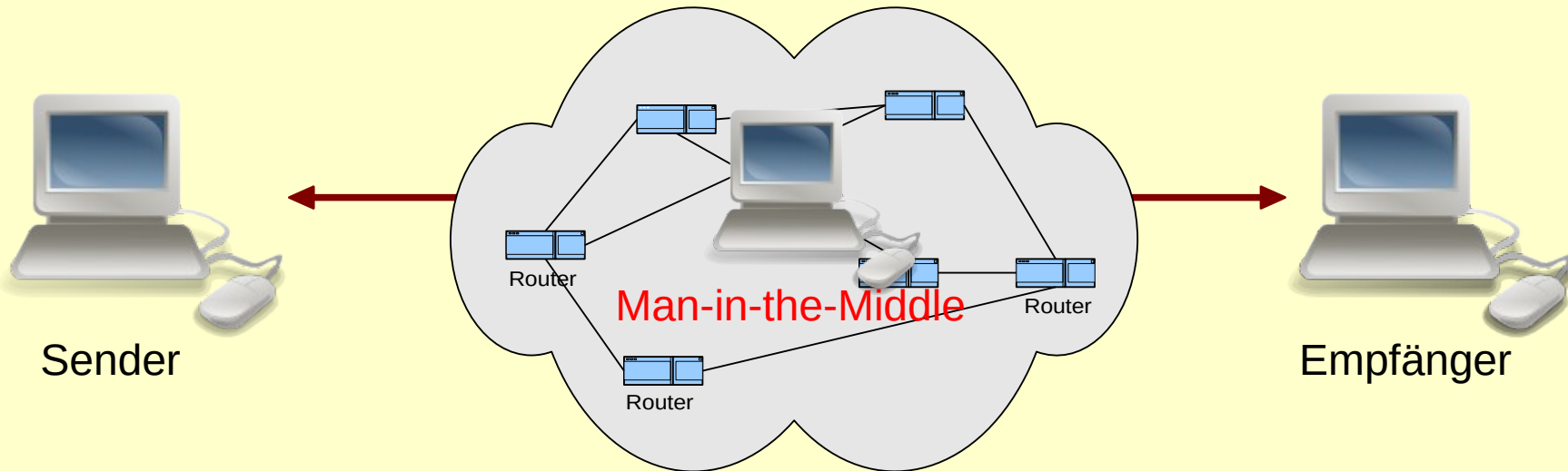
Zombies („unechtes IP-Spoofing“)



- Zombie als Relay



Man-in-the-middle / Sniffing



- Datenverkehr kann sehr leicht abgehört werden (sog. Sniffing).
- Angriff auf SSL-Verbindungen möglich!
- Erzwingen von Man-in-the-middle durch Manipulationen:
 - Routing-Protokolle
 - DNS-Spoofing
 - ARP-Spoofing



Demo: Sniffing

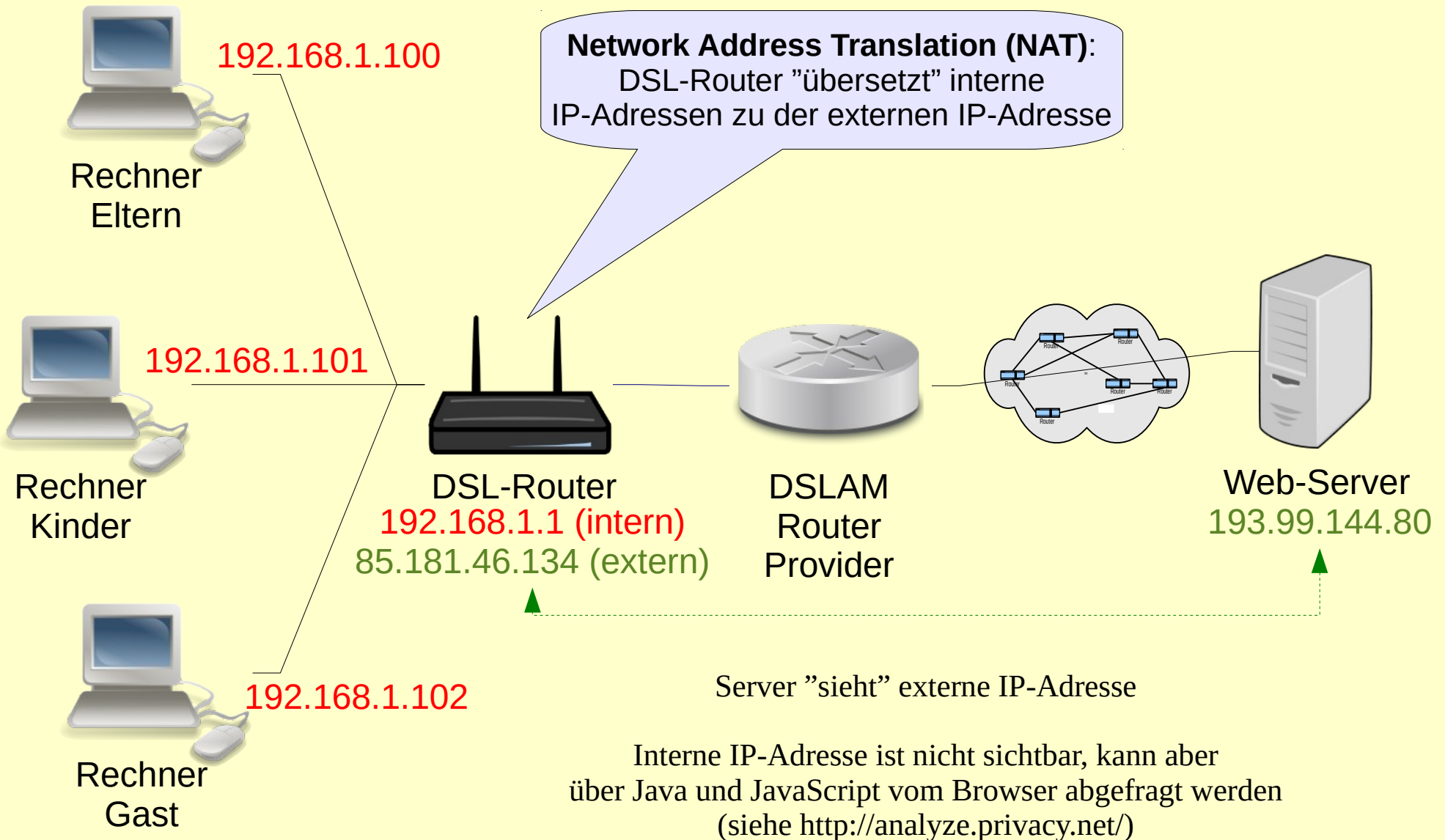
- `dsniff -i eth0`
- Wireshark



Dynamische IP-Adressen

- Temporäre Zuweisung durch Provider
 - Kunde authentisiert sich (Passwort/Username)
 - IP-Adresse wird zugewiesen
 - Nach Ende der Verbindung wird die IP-Adresse neu vergeben
 - Grund für Verfahren: Marktsegmentierung
- Provider kennt Zuordnung Kunde zu IP-Adresse
 - Fehler passieren: „RIAA verklagt 66-jährige Bildhauerin wegen Verbreitung von Gangsta-Rapp“
 - Auch in Deutschland: Zahlendreher im Auskunftersuchen
- IPv6

IP-Adressen im Heimnetzwerk (IPv4)



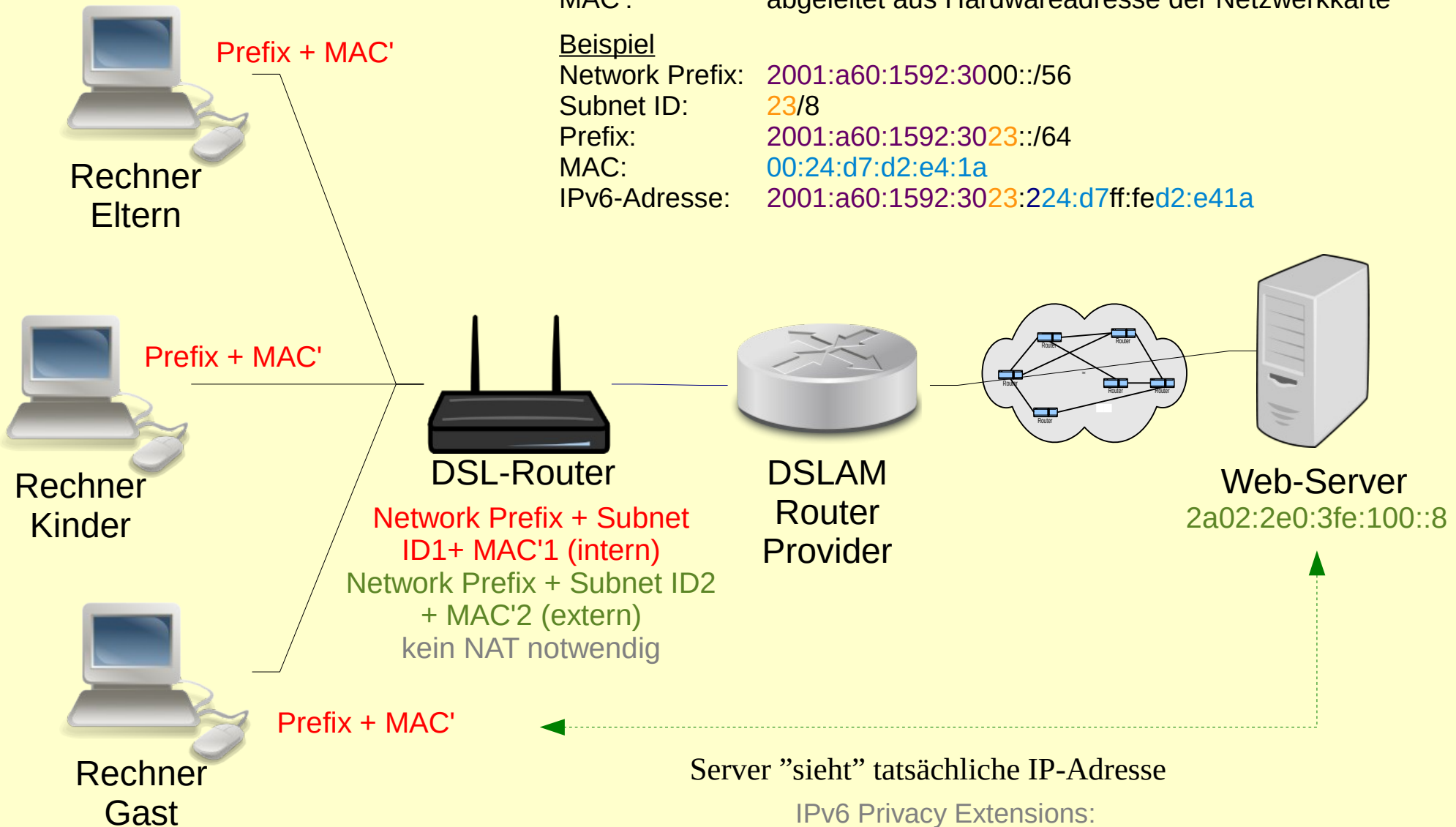
IP-Adressen im Heimnetzwerk (IPv6)



Network Prefix: wird vom ISP zugewiesen
Subnet ID: wird vom Router zugewiesen
MAC': abgeleitet aus Hardwareadresse der Netzwerkkarte

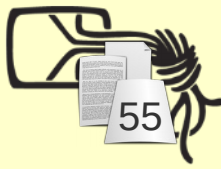
Beispiel

Network Prefix: 2001:a60:1592:3000::/56
Subnet ID: 23/8
Prefix: 2001:a60:1592:3023::/64
MAC: 00:24:d7:d2:e4:1a
IPv6-Adresse: 2001:a60:1592:3023:224:d7ff:fed2:e41a



IPv6 Privacy Extensions:
Statt der MAC wird eine zufällige Zahl verwendet.

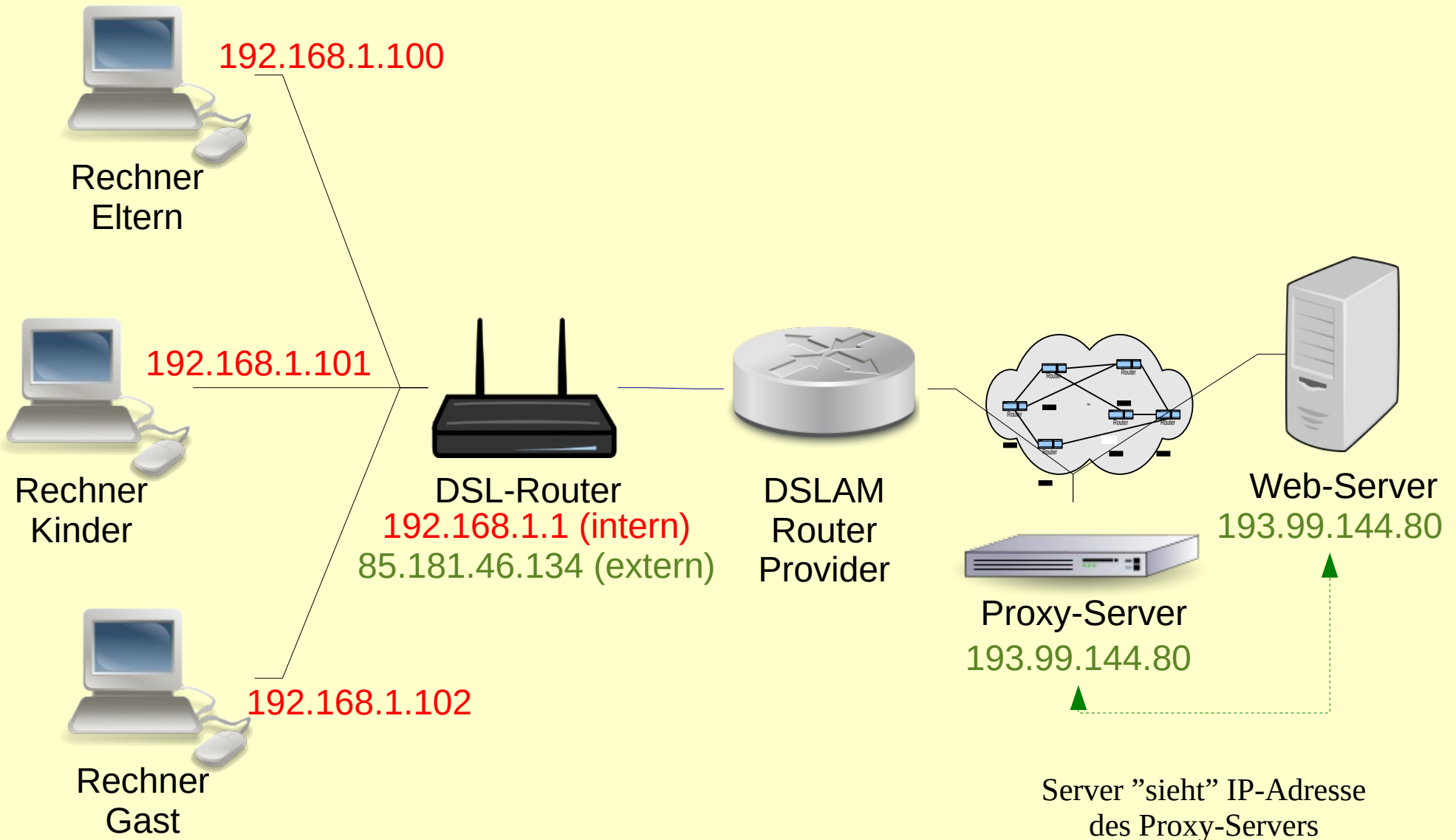
Verbreitung IPv6 Privacy Extensions



Betriebssystem	Privacy Extensions standardmäßig aktiv seit...
Windows XP	ab Service Pack 1 (2002)
Windows Vista, 7, 8, ff.	ja (2007)
OS X	ab Version 10.7 Lion (2011)
Linux (Ubuntu)	ab 12.04 (2012)
Linux (Debian)	nicht aktiv
Linux (RedHat)	nicht aktiv
iOS	ab Version 4.3 (2011)
Android	ab Version 4.0 Ice Cream Sandwich (2011)

Seit etwa 2011 sind die IPv6 Privacy Extensions standardmäßig bei den meisten Betriebssystemen für Clients aktiv. Allerdings gilt dies nicht für Betriebssysteme für Server und Router oder Eingebettete Systeme. Dort sind diese üblicherweise inaktiv.

IP-Adressen bei Proxy-Verwendung





Penetrationstests

- Standard-Vorgehen in der IT-Sicherheitsbranche
 - Informationssammlung
 - Identifikation der Zielsysteme
 - Analyse der Zielsysteme (Portscan, Fingerprinting)
 - Schwachstellenanalyse (Vulnerability Scan)
 - Exploiting (Ausnutzen von Schwachstellen)

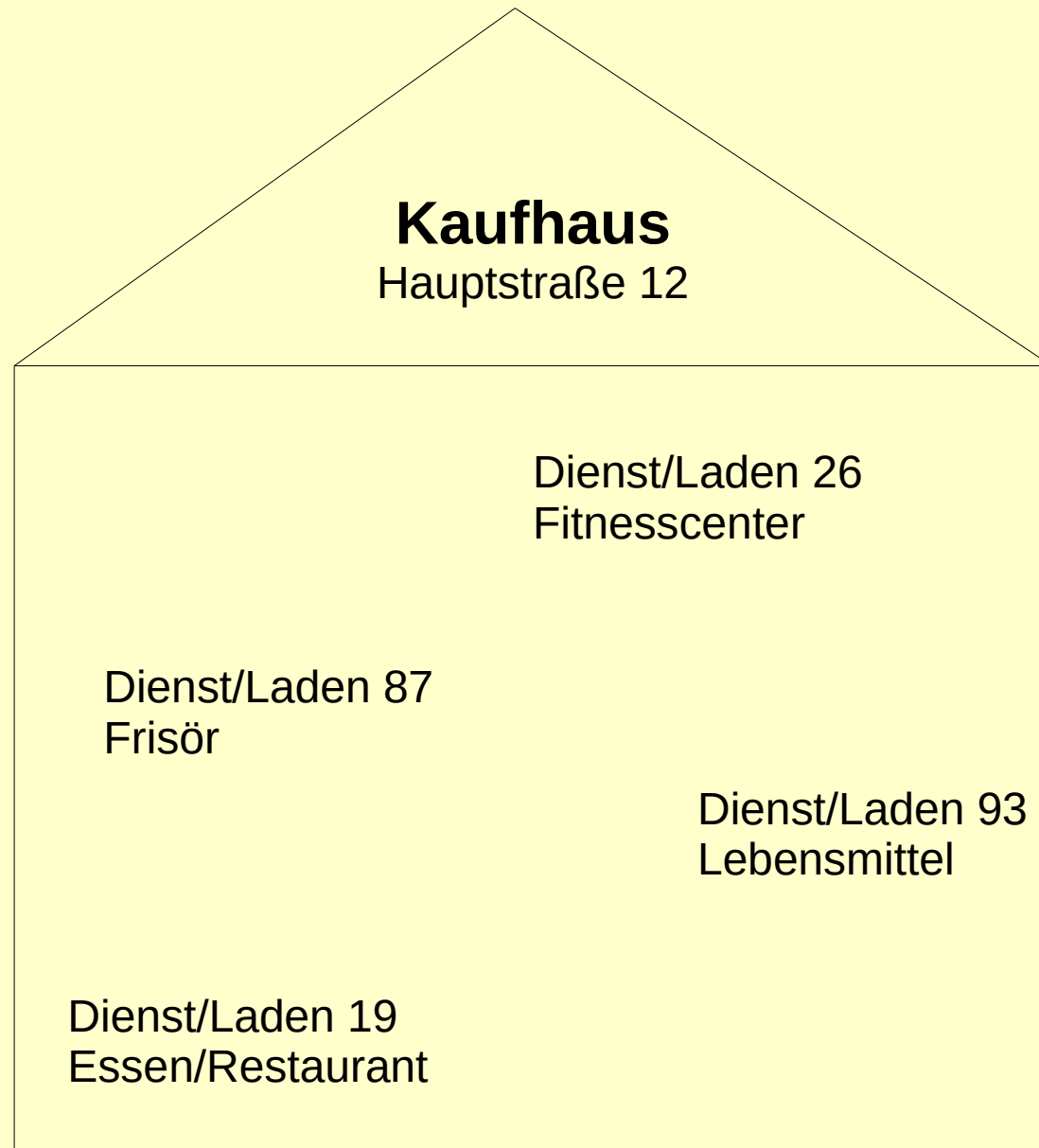


Informationsphase

- Informationen zur IP-Adresse
 - whois-Informationen:
 - <http://www.ripe.net> (Europa)
 - <http://www.arin.net> (USA)
 - <http://www.apnic.net> (Asien/Pazifik)
- Informationen zum Domain-Namen
 - whois-Informationen:
 - <http://www.denic.de> (.de-Domains)
 - <http://www.internic.com> (.com/.net/.org-Domains)
 - DNS-Abfragen
- Informationen über die Firma / Personen
 - Suchmaschinen für Webinhalte
 - <http://www.google.de>
 - Newsgroups



IP-Adresse und Port

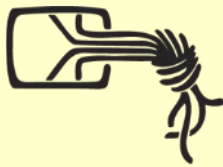




Demo: Portscanning

- `nmap -sS -O 192.168.55.101`

Portscanning ist Service Detection und keine Angriffshandlung!



nmap -sS -O 192.168.55.101

Starting Nmap 6.00 (<http://nmap.org>) at 2012-11-19 17:53 CET

Nmap scan report for 192.168.55.101

Host is up (0.00028s latency).

Not shown: 989 closed ports

PORT	STATE	SERVICE
------	-------	---------

7/tcp	open	echo
-------	------	------

9/tcp	open	discard
-------	------	---------

13/tcp	open	daytime
--------	------	---------

17/tcp	open	qotd
--------	------	------

19/tcp	open	chargen
--------	------	---------

21/tcp	open	ftp
--------	------	-----

135/tcp	open	msrpc
---------	------	-------

139/tcp	open	netbios-ssn
---------	------	-------------

445/tcp	open	microsoft-ds
---------	------	--------------

8000/tcp	open	http-alt
----------	------	----------

8080/tcp	open	http-proxy
----------	------	------------

MAC Address: 08:00:27:FA:E4:9C (Cadmus Computer Systems)

Device type: general purpose

Running: Microsoft Windows XP

OS CPE: cpe:/o:microsoft:windows_xp::sp2

cpe:/o:microsoft:windows_xp::sp3

OS details: Microsoft Windows XP SP2 or SP3

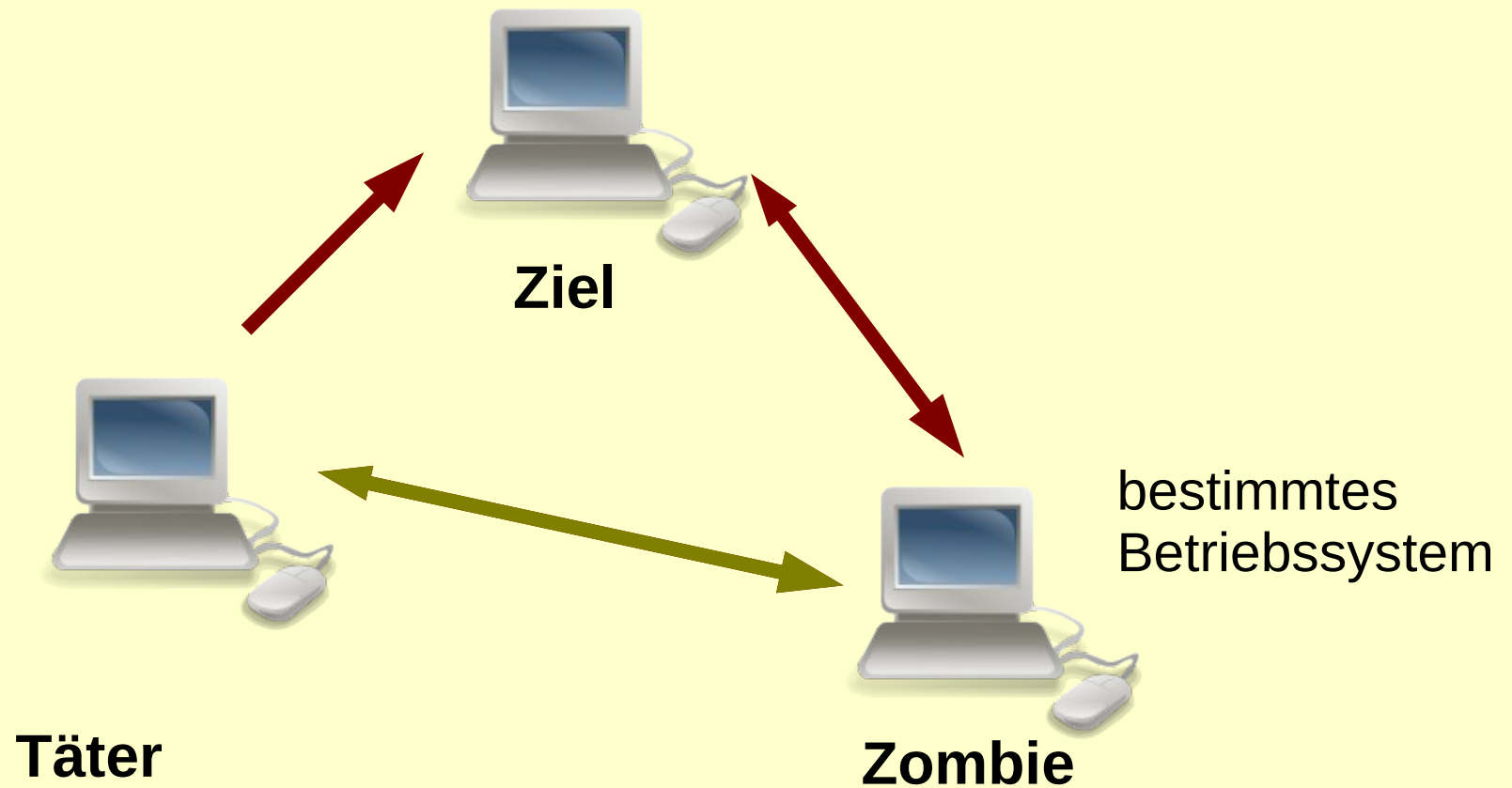
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
<http://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 3.70 seconds



Idle Scan (indirekter Portscan)






Demo: Vulnerability Scanning

- OpenVAS



 **Greenbone**
Security Assistant

Logged in as Admin [admin](#) | [Logout](#)

Mon Nov 19 20:19:23 2012 UTC




Scan ManagementAsset ManagementConfigurationExtrasAdministrationHelp

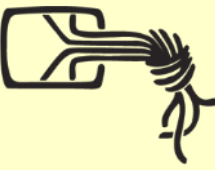
Task Summary ? ? ? ? ? ? ? ? ? ?

Name: WinXP Demp [Tasks](#)
Comment:
Scan Config: [Full and fast ultimate](#)
Escalator:
Schedule: (Next due: over)
Target: [WinXP Demp](#)
Slave:
Status: Done
Reports: 1 (Finished: 1)
Observers:

Scan Intensity
Maximum concurrently executed NVTs per host: 4
Maximum concurrently scanned hosts: 20

Reports for "WinXP Demp" ? √Apply overrides ? ?

Report	Threat	Scan Results					Actions
		High	Medium	Low	Log	False Pos.	
Mon Nov 19 20:08:44 2012 Done	High	5	3	11	62	0	  




Exploiting

- Metasploit



Auktionsplattform für Exploits

[MarketPlace](#) [About](#) [Services](#) [FAQ](#) [Blog](#) [Contacts](#)



WabiSabiLabi
CLOSER TO ZERO RISK

[Home page](#) ▶ [Current bids](#)

Sign in
Username
Password
[Sign in](#)
New user? [Sign up here](#)

News
[PRESS RELEASE](#) 03/07/2007
Finally a Marketplace Site for Security Research

[See all news](#)

Current bids **MarketPlace history**

4 items found, displaying all items. Page 1

Code ↕	Time to live ↕	Title ↕	System ↕	Offer type	Bid	
ZD-00000007	8d 15h 37m	Local Linux kernel memory leak	Linux	Bidding	600€ 1 bid(s)	info
ZD-00000005	8d 15h 37m	Yahoo! Messenger 8.1 remote buffer overflow	Windows XP	Bidding	2.000€ 0 bid(s)	info
ZD-00000004	8d 15h 37m	Squirrelmail GPG Plugin Command Execution	Web application	Bidding Buy now at	600€ 1 bid(s) 1.750€	info
ZD-00000008	9d 15h 37m	MKPortal SQL injection	Web application	Bidding Buy now at	500€ 0 bid(s) 800€	info

WabiSabiLabi Ltd. Copyright ©2007

The art of continuous improvement of imperfect security



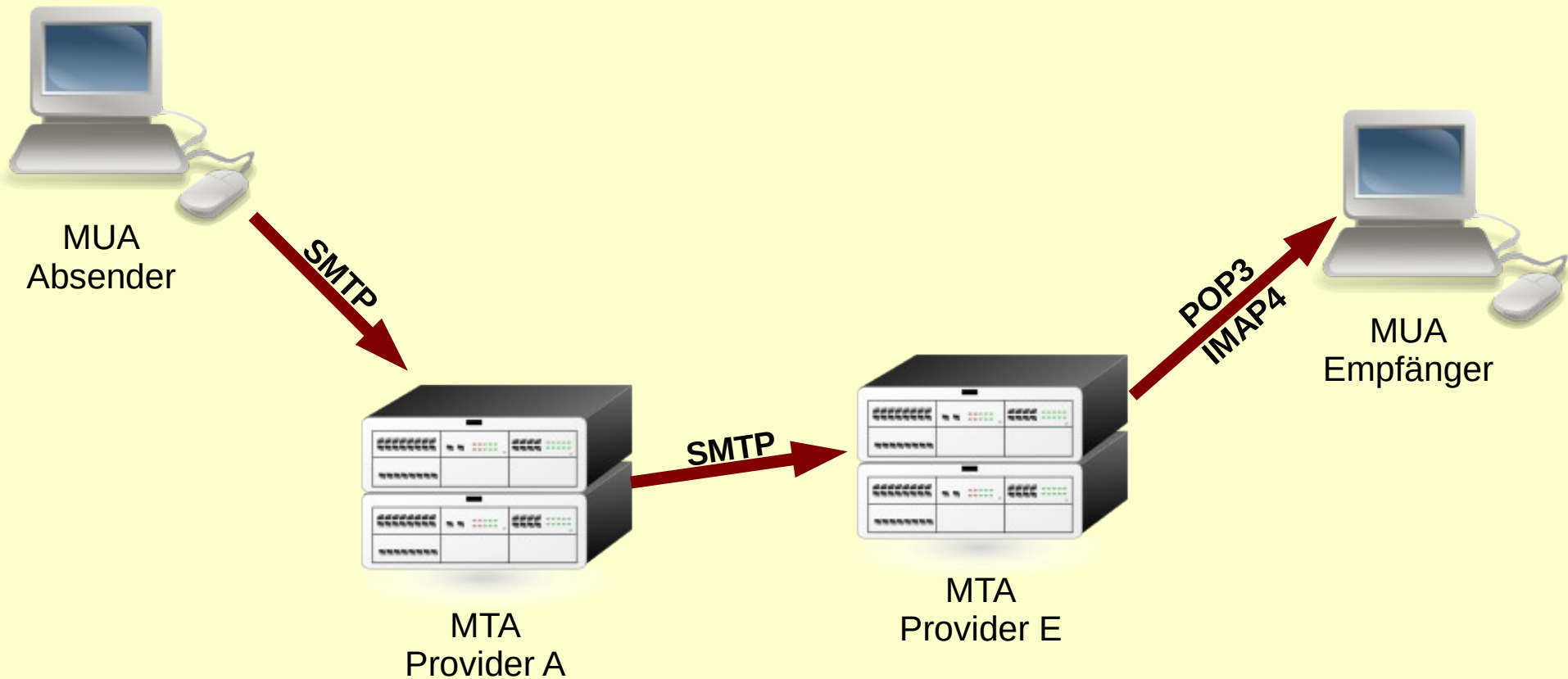
E-Mail-Versand

DEAR SIR,

I AM JOHN LEE, MANAGER OF BILLS/EXCHANGE AT THE FOREIGN REMITTANCE DEPARTMENT OF ABSA BANK LIMITED. IN MY DEPARTMENT, WE DISCOVERED AN ABANDONED SUM OF US\$25,500,000 (TWENTY FIVE MILLION, FIVE HUNDRED THOUSAND US DOLLARS) IN AN ACCOUNT THAT BELONGED TO ONE OF OUR FOREIGN CUSTOMERS WHO DIED ALONG WITH HIS ENTIRE FAMILY ON NOVEMBER 1994 IN A GHASTLY PLANE CRASH.



E-Mail-Kommunikation



- E-Mail-Transport über das Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP)



- Dient der Übertragung von E-Mails

HELO mail.email.de

OK

MAIL FROM: <schmidt@email.de>

OK

RCPT TO: <zimmermann@itsec-muc.de>

OK

DATA

From: Big Boss <bigboss@itsec-muc.de>

To: Sebastian Zimmermann <zimmermann@itsec-muc.de>

Subject: Schlüssel

Geben Sie den Schlüssel bitte an den Boten, der gleich vorbeikommt!

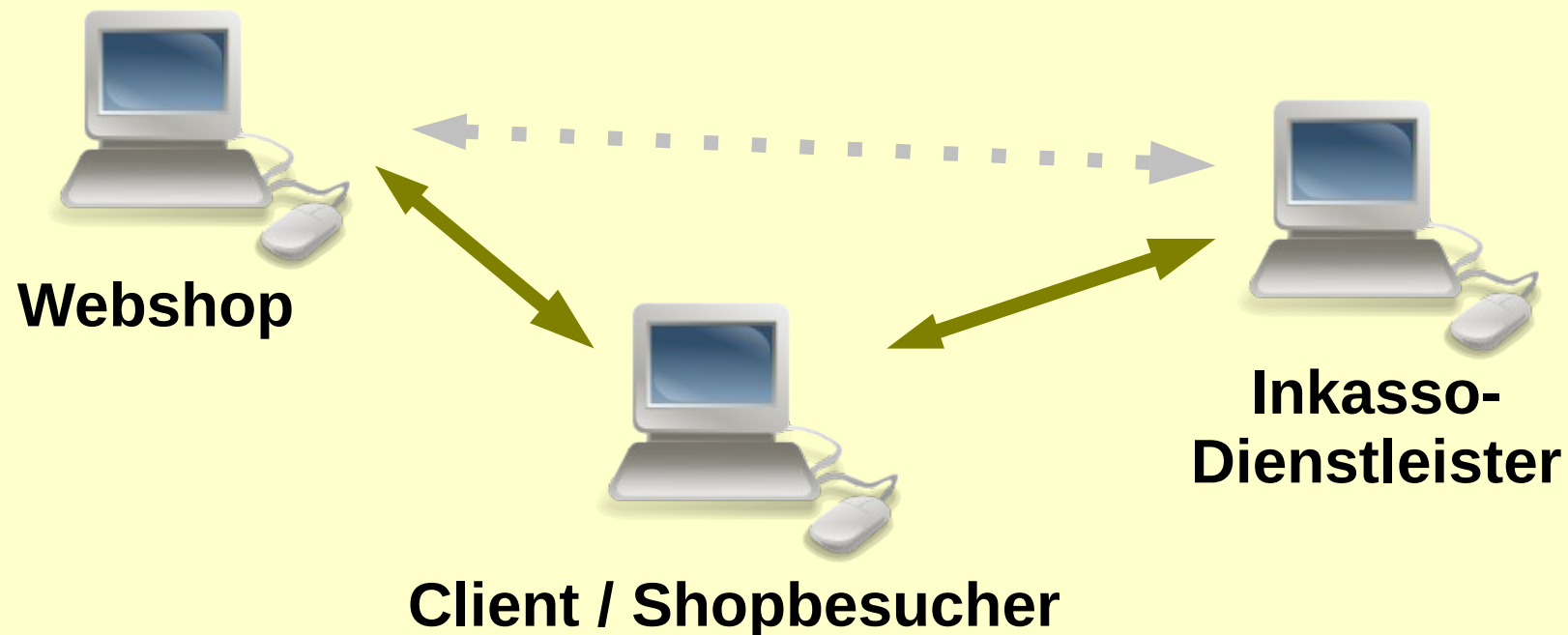
.
OK

- Absenderfälschung: „**Joe Job**“
- **Ein Absender/Empfänger lässt sich ohne zusätzliche kryptographische Mechanismen nie eindeutig feststellen!**



Webapp-Sicherheit: Client Data

- Grundsatz: Der Client kann alle Daten ändern.
- Beispiel: <http://www.coolcart.com/jewelrystore.html>



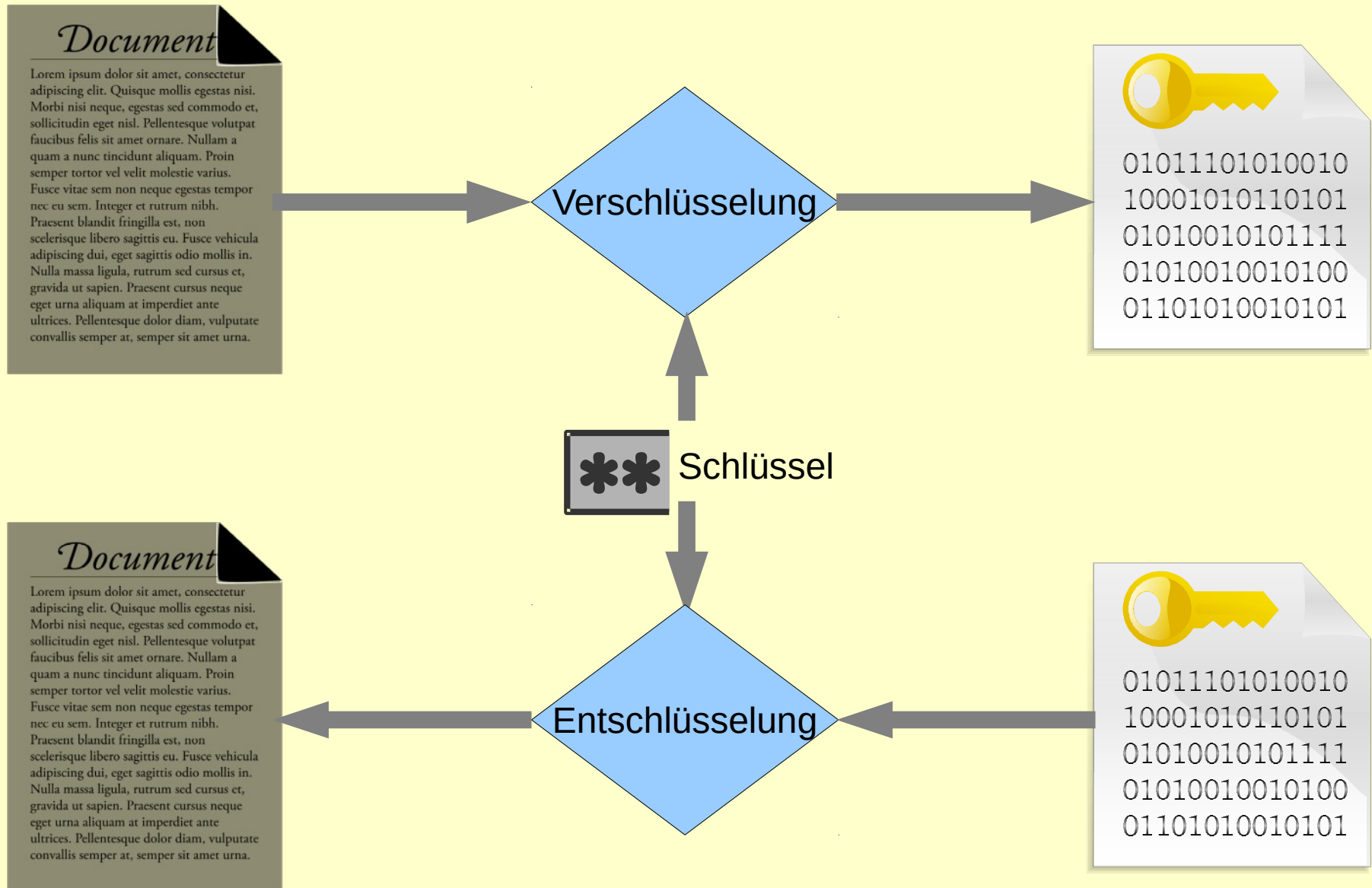


Verschlüsselung

- Verschlüsselung der Festplatte
 - Qualität des Passworts entscheidend
 - Glaubhafte Bestreitbarkeit (plausible deniability)
 - Daten sehen rein zufällig aus
 - Zwei Volumes – je nach Passwort, z.B. TrueCrypt
- Verschlüsselung der Datenverbindung
 - SSL – in der Regel sehr sicher
 - Problem: Authentizität der Gegenstelle
 - Verschlüsselung nutzt nichts, wenn man mit dem falschen spricht!
- „Online-Durchsuchung“



Symmetrische Verschlüsselung





Symmetrische Verschlüsselung

- Sicherheit hängt ab vom verwendeten Algorithmus (z.B. DES-ECB, 3-DES-CBC, AES-CBC), der Länge des Schlüssels, der Qualität des Schlüssels und der Geheimhaltung des Schlüssels (der verschlüsselte Text ist implizit öffentlich).
- Beispiel: Wikileaks und die US Cables:
 - Buch „WikiLeaks. Inside Julian Assange's War on Secrecy“, David Leigh and Luke Harding, Kapitel 11:

„ACollectionOfDiplomaticHistorySince_1966_ToThe_PresentDay#“

Qualität des Passworts (hier: bei Web-Diensten)



Top Panel (Tr0ub4dor&3):

- UNCOMMON (NON-GIBBERISH) BASE WORD
- ORDER UNKNOWN
- Tr0ub4dor&3
- CAPS? (indicated by '0')
- COMMON SUBSTITUTIONS (indicated by '4' and '&')
- NUMERAL (indicated by '3')
- PUNCTUATION (indicated by '&')
- (YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

Entropy: ~28 BITS OF ENTROPY

Calculation: $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

Difficulty to Guess: EASY

Difficulty to Remember: HARD

Bottom Panel (correct horse battery staple):

- correct horse battery staple
- FOUR RANDOM COMMON WORDS

Entropy: ~44 BITS OF ENTROPY

Calculation: $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

Difficulty to Guess: HARD

Difficulty to Remember: YOU'VE ALREADY MEMORIZED IT

Conclusion: THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

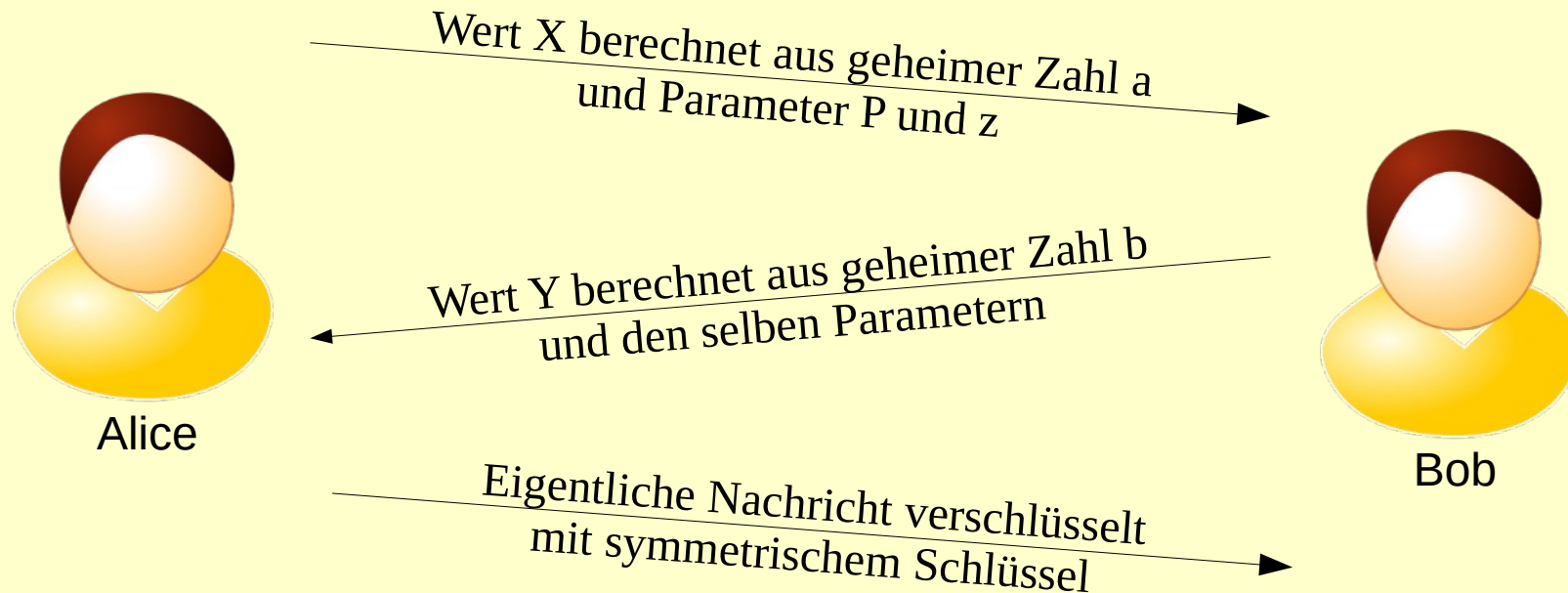
Quelle: XKCD.com,
CC-BY-NC-2.5



Asymmetrische Verschlüsselung

- Probleme des symmetrischen Verfahrens:
 - Wie wird der Schlüssel ausgetauscht?
 - Austausch zwischen mehreren Parteien (vgl. WikiLeaks-Leak)?

Diffie-Hellman (D-H) (vereinfachte Darstellung)



Der gemeinsame geheime Schlüssel kann von beiden Parteien berechnet werden, ohne dass er übertragen werden muss. Ein passiver Abhörer kann den Schlüssel nicht berechnen. Dieses Verfahren ist aber anfällig für Man-in-the-Middle.



Asymmetrische Verschlüsselung

- Vorteile:
 - Kein geheimer Übertragungskanal erforderlich.
 - Jede Partei hat ihren eigenen Schlüssel, kein geteiltes Schlüsselmateriale (vgl. WikiLeaks-Problematik).

- Nachteile:
 - Rechenintensiver, längere Schlüssel erforderlich.

Symmetrisch	Asymmetrisch RSA	Asymmetrisch ECC
112 Bit	2048 Bit	224 Bit
256 Bit	15360 Bit	521 Bit

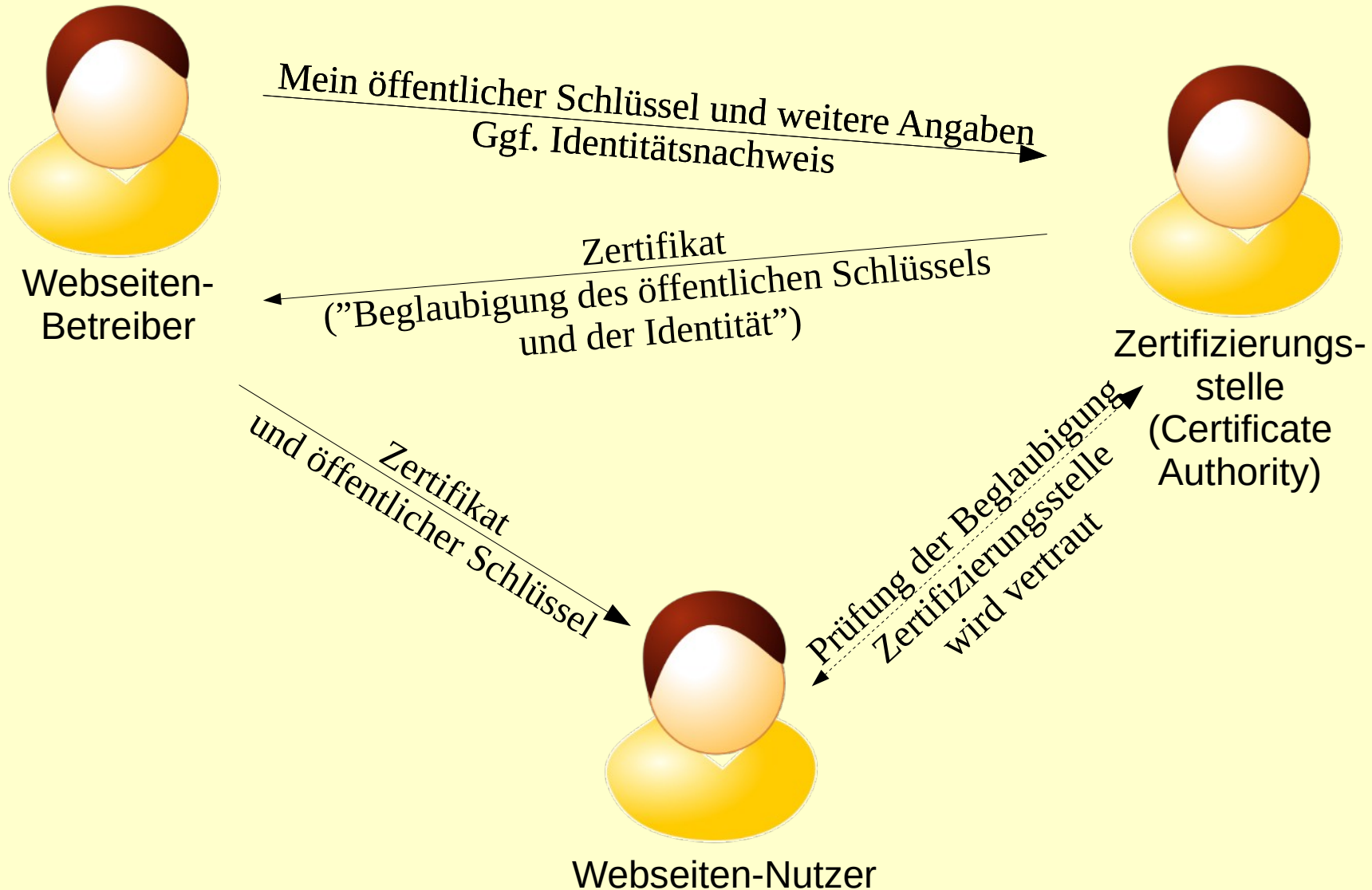
- Entdeckung neuer mathematischer Methoden kann Sicherheit des Verfahrens gefährden.
- Woher weiß man, dass man den richtigen öffentlichen Schlüssel zu einem bestimmten Empfänger hat?



Asymmetrische Verschlüsselung

- Entscheidend für die Sicherheit asymmetrischer Verschlüsselungsverfahren ist die Korrektheit des öffentlichen Schlüssels!
- Verifikationsmethoden:
 - Abgleich des „Fingerabdrucks“ über einen nicht manipulierbaren Kommunikationskanal.
 - Web-of-Trust (z.B. PGP).
 - Zertifizierungsstellen (z.B. SSL-Zertifikate von Webseiten).

Zertifizierungsstellen (vereinfachte Prinzipdarstellung)

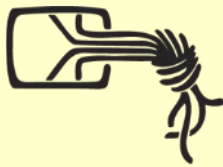


Asymmetrische Verschlüsselung

Kernprobleme in der Praxis



- Faktor „Mensch“
 - Stimmt die „Beglaubigung“ nicht oder ist die Zertifizierungsstelle unbekannt, wird der Benutzer gefragt, ob er trotzdem auf die Webseite möchte.
- Menge und Qualität der Zertifizierungsstellen
 - Aktuelle Browser kennen und vertrauen ca. 50 verschiedenen Zertifizierungsstellen in verschiedenen Ländern. Die schwächste bestimmt die Sicherheit des Gesamtsystems.
 - „Extended Validation“ SSL-Zertifikate lösen das Problem nur teilweise.
- Als Resultat ist in der Praxis die Sicherheit der SSL-Verschlüsselung anzuzweifeln.



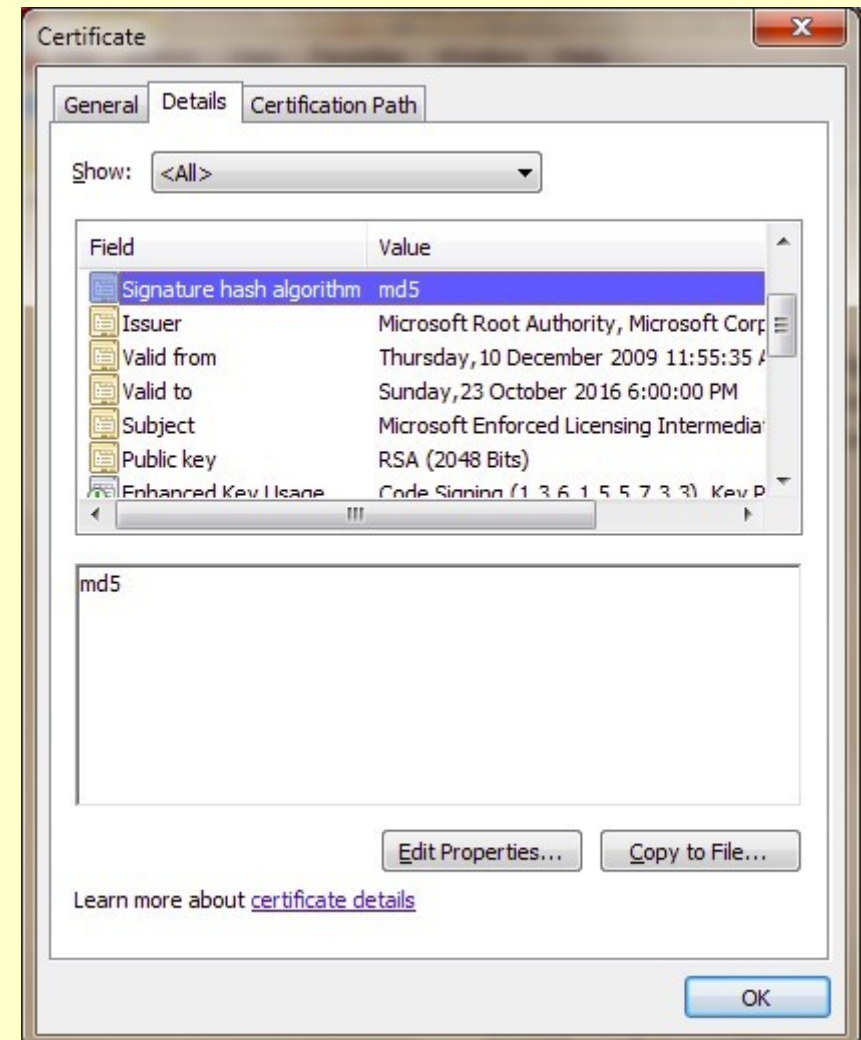
Der Fall „DigiNotar“

- Am 28. August 2011 berichtet ein Iraner von einem gültigen Zertifikat für die Google-Server, das aber nicht zu Google gehört. Es wird vermutet, dass die iranische Regierung das Zertifikat benutzt, um Google-Nutzer (z.B. Gmail) zu überwachen.
- Es stellt sich heraus, dass das Zertifikat bereits am 10. Juli durch die Zertifizierungsstelle „DigiNotar“ in den Niederlanden ausgestellt wurde.
- Am 30. August verkündet „DigiNotar“, dass das Zertifikat aus einem „Hackereinbruch“ stamme, der am 19. Juli festgestellt wurde.
- Es tauchen weitere Zertifikate auf, die zum Teil ab dem 20. Juli erstellt wurden, u.a. für den Anonymisierungsdienst Tor.
- Über 500 Zertifikate werden zurückgezogen, u.a. für Webseiten von Geheimdiensten.
- Anfang September übernimmt die niederländische Regierung die Kontrolle über „DigiNotar“, das auch die staatliche Zertifizierungsstelle betreibt.
- Weitere Zertifizierungsstellen stellen Einbrüche bei sich fest.
- Am 19. September meldet „DigiNotar“ Insolvenz an.



„Flame“ (aka sKyWiper)

- Computerwurm, entdeckt im Mai 2012.
 - diente vermutlich zur Spionage im Mittleren Osten
 - Verbreitung über USB Sticks und Netzwerk
 - kann Audio- und Bildschirmaufzeichnungen machen, Tastatureingaben, Netzwerkverkehr und Skype abhören
 - bereits seit mindestens Februar 2010 aktiv
 - erkennt Virens Scanner und wechselt zu „unverdächtigem“ Verhalten
 - **nutzte eine MD5-Hash Kollision, um eine digitale Signatur von Microsoft nachzustellen**



Autor: Socrates2008; Lizenz: CC BY-SA 3.0



OTR-Verschlüsselung

- OTR - „Off-the-Record“
 - relativ neues Verschlüsselungsverfahren für Messaging
 - Encryption, Authentication, Deniability, Perfect Forward Secrecy



Kontakt

Chaos Computer Club München e.V.

info@muc.ccc.de

<http://muc.ccc.de>

Schleißheimer Str. 41

(Postadresse Hessstr. 90)

80797 München

