

Digitale Verhütung

Thomas Keller - Chaostreff Leipzig - www.c3le.de



Creative Commons Namensnennung-Keine kommerzielle Nutzung 2.0 Deutschland Lizenz

Überblick

- Vorstellung
- Ziel der heutigen Veranstaltung
- Es gibt keine absolute Sicherheit!
- Technisches Grundwissen

Überblick II

- Digitale Verhütung
- Fragerunde
- Praxis-Workshop

Vorstellung

Zur Person

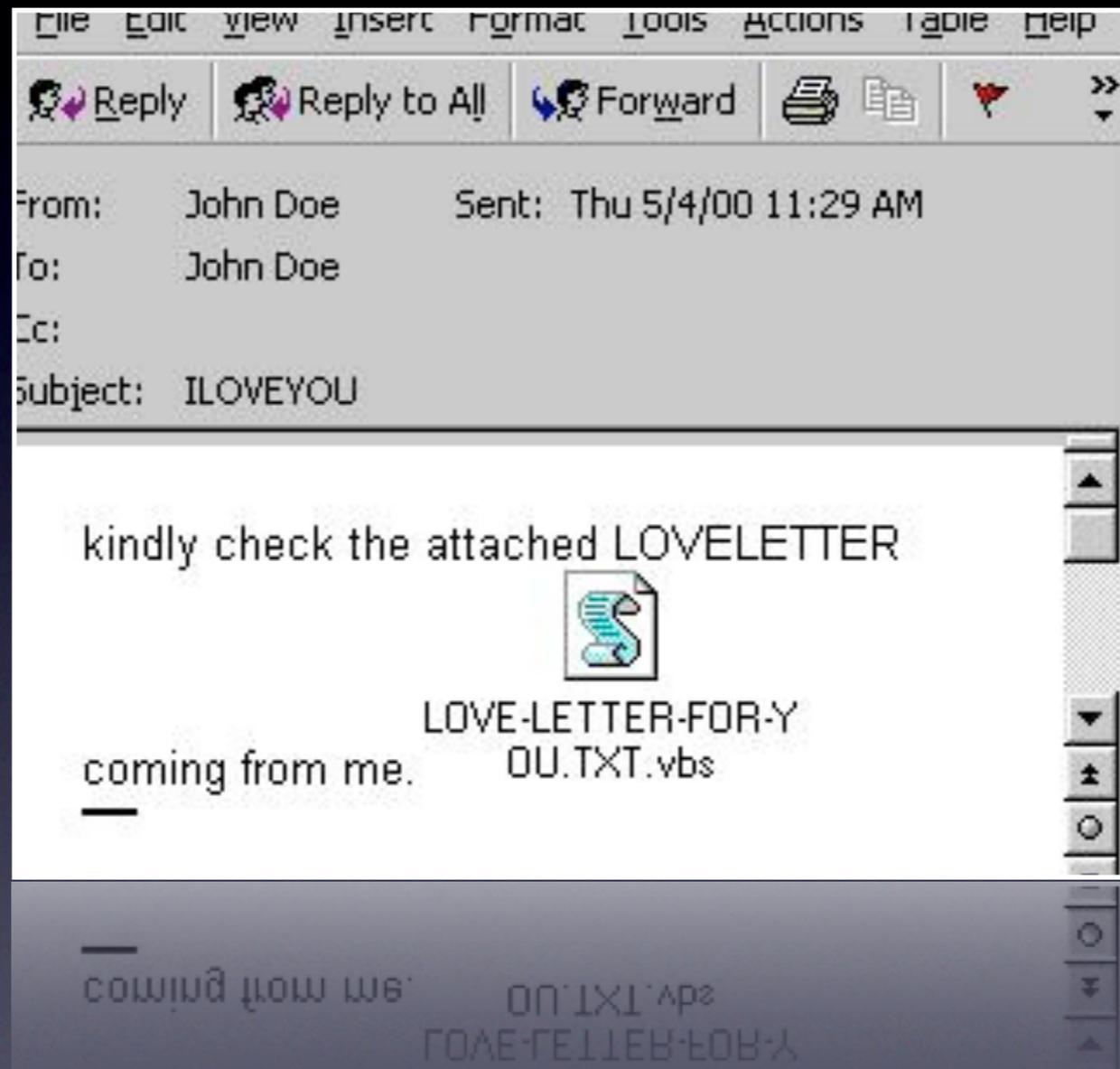
- 26 Jahre alt, verheiratet, ein kleiner Sohn
- Softwareentwickler in Leipziger Firma
- Open Source-Entwickler und Verfechter von freier Software und freiem Informationsaustausch
- aktiv im Chaostreff Leipzig und der Leipziger Ortsgruppe des Arbeitskreises Vorratsdatenspeicherung

Ziel der heutigen Veranstaltung

- Bewusstsein für Umgang mit den eigenen digitalen Daten, dem eigenen digitalen Leben schaffen
- Werkzeuge, Verhaltensweisen und Kenntnisse erlangen, um sich vor digitalen Betrügereien zu schützen
- Sicher und anonym kommunizieren

Es gibt keine absolute
Sicherheit!

- moderne Kommunikationstechnologie verspricht unbegrenzte Möglichkeiten
- Nutzer gehen meist zu unbedarft mit ihren Daten um
- Anonymität wird zunehmend Luxus
- “Das größte Sicherheitsproblem sitzt meist vor dem Monitor..”



ILOVEYOU-Wurm (2000)

- E-Mail-Wurm mit „sozialer“ Komponente
- Verbreitung per E-Mail (Adressbuch) und Internet Relay Chat (IRC)
- Wurm löscht / überschreibt Dateien
- geschätzter Schaden: 5.5 Mrd USD (2000)
- u.a. geschädigte Firmen: NASA, Pentagon, Ford...

Quelle: <http://www.m-boehmer.de/pdf/FROM-MANILA-WITH-LOVE.pdf>

Was lernen wir daraus?

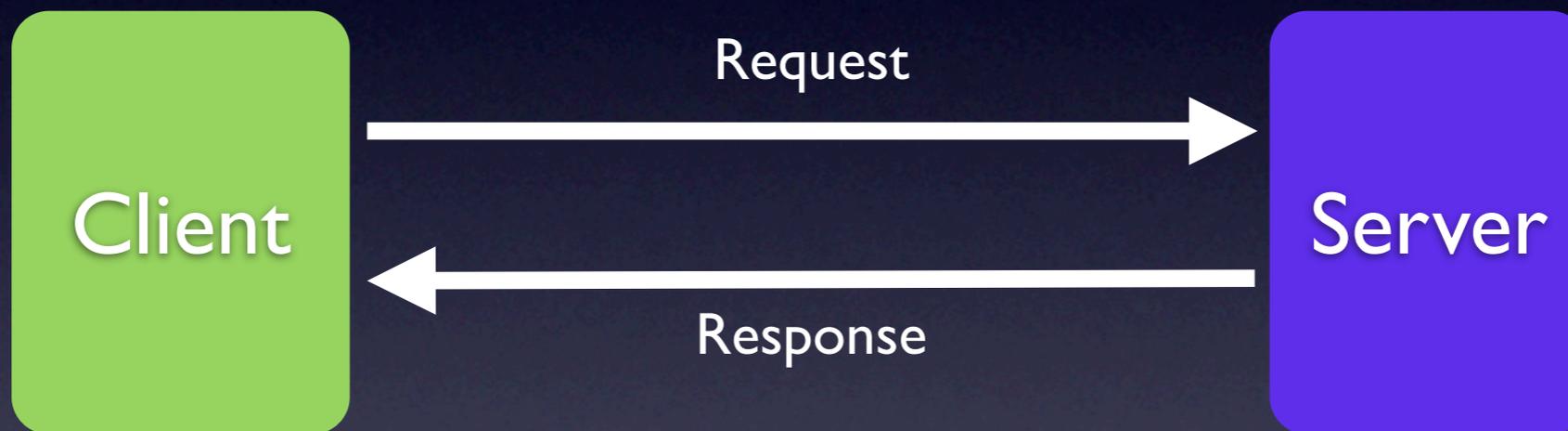
- Vertraue keinen E-Mails oder Webseiten mit fragwürdigen Inhalten!
- Wie würde man im realen Leben auf solche Angebote reagieren?
- Gesunden Menschenverstand einschalten!

Technisches Grundwissen

Client-Server-Modell

- Grundlage der meisten Kommunikationsdienste (WWW, E-Mail, FTP, ...)
- Client sendet Anfrage (Request) für einen Dienst auf einem bestimmten Port (Kanal)
- Dienst auf Server sendet Antwort (Response)
- Pull-Prinzip (wichtig!)

Client-Server-Modell



Wegfindung im Netz

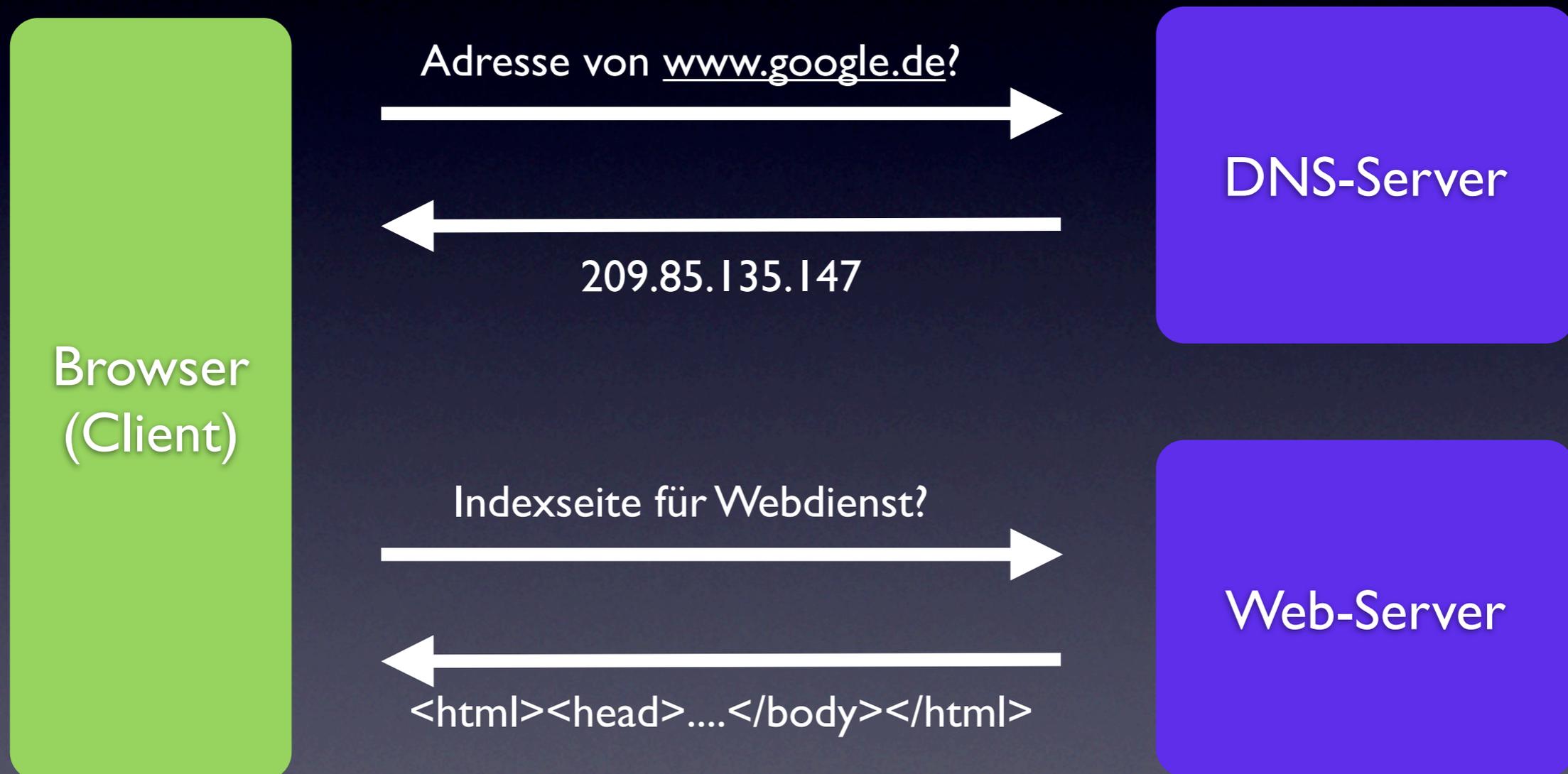
- Rechner identifizieren sich über eindeutige Nummern, sogenannte IP-Adressen (IP = Internet Protocol), bspw. 209.85.135.147
- Das Domain Name System (DNS) weist den IP-Adressen (=den Rechnern) Namen zu (nicht mehr zwangsläufig eindeutig)

Was passiert beim Laden einer Webseite?

- Benutzer gibt Webadresse (bspw. www.google.de) in Browser (Client) ein
- Browser fragt nächstgelegenen DNS-Server „gib mir die IP-Adresse von www.google.de“
- DNS-Server antwortet mit „209.85.135.147“

- Browser verbindet sich mit dem Rechner hinter der IP „209.85.135.147“ (Server) und dem WWW-Dienst auf Port 80
- Browser sendet in diesen Port die Anfrage „gib mir die Indexseite dieses Webserver“
- Server antwortet mit dem HTML-Text der Indexseite
- Browser stellt Webseite lokal dar

Nochmal schematisch



Und wie stehts um die Sicherheit?

- Im idealisierten Modell von eben war das nicht vorgesehen
- Über 90% der Internetkommunikation erfolgt nicht anonymisiert und ungesichert
- Eine direkte, anonyme und gesicherte Kommunikationsverbindung zwischen Client und Server ist die Ausnahme (Proxys, Router, ...)

```
Terminal — ssh — 100x24
h; U; PPC Mac OS X 10.5; en-US; rv:1.9b5) Gecko/2008032619 Firefox/3.0b5"
90.194.46.112 - - [15/May/2008:15:39:43 -0400] "GET /show_style.php?opt=header&d=10 HTTP/1.1" 200 33
294 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.1)"
209.152.109.224 - - [15/May/2008:15:39:43 -0400] "GET /show_alb.php?d=29226 HTTP/1.1" 200 22045 "htt
p://www.google.com/search?hl=en&q=opaque+brotherhood+lyrics" "Mozilla/4.0 (compatible; MSIE 7.0; Win
dows NT 6.0; WOW64; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506; Media Center PC 5.0)"
209.152.109.224 - - [15/May/2008:15:39:43 -0400] "GET /javascript.js HTTP/1.1" 200 10250 "http://www
.musicmademe.com/show_alb.php?d=29226" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; WOW64; SL
CC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506; Media Center PC 5.0)"
209.152.109.224 - - [15/May/2008:15:39:43 -0400] "GET /templates/1/styles.css HTTP/1.1" 200 10231 "h
ttp://www.musicmademe.com/show_alb.php?d=29226" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0;
WOW64; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506; Media Center PC 5.0)"
209.152.109.224 - - [15/May/2008:15:39:44 -0400] "GET /classes/lightbox/prototype.js HTTP/1.1" 200 4
9387 "http://www.musicmademe.com/show_alb.php?d=29226" "Mozilla/4.0 (compatible; MSIE 7.0; Windows N
T 6.0; WOW64; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506; Media Center PC 5.0)"
74.6.19.90 - - [15/May/2008:15:39:44 -0400] "GET /show_art.php?d=2804 HTTP/1.0" 200 21805 "-" "Mozil
la/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)"
209.152.109.224 - - [15/May/2008:15:39:44 -0400] "GET /classes/lightbox/scriptaculous.js?load=effect
s HTTP/1.1" 200 2196 "http://www.musicmademe.com/show_alb.php?d=29226" "Mozilla/4.0 (compatible; MSI
E 7.0; Windows NT 6.0; WOW64; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506; Media Center PC 5.0)"
209.152.109.224 - - [15/May/2008:15:39:45 -0400] "GET /classes/lightbox/effects.js HTTP/1.1" 200 328
72 "http://www.musicmademe.com/show_alb.php?d=29226" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
6.0; WOW64; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506; Media Center PC 5.0)"

```

Spurensuche

Spurensuche II

- Internetprovider merkt sich bei Einwahl IP
- Server zeichnen Verbindungsdaten auf:
 - IP-Adresse
 - Datum und Uhrzeit des Zugriffs
 - Ursprungsadresse (Referer)
 - ...

Spurensuche III

- Benutzer gibt Daten Webdiensten preis
 - Web 2.0: Blogs, Foren, Twitter
 - „Datenkraken“: Amazon, Google
- Durch geschicktes Data Mining können so Profile erstellt werden
- Das Internet vergisst nichts... schon einmal nach dem eigenen Namen gegoogelt?

Ungeschützte Kommunikation

- Rolf schreibt eine Postkarte mit Urlaubsgrüßen aus der Türkei und schickt sie an seine Oma Susi in Dresden
- Nach dem Urlaub wieder zu Hause angekommen, kümmert sich Rolf um die Abrechnung seines letzten eBay-Verkaufs und übermittelt den Höchstbietenden per E-Mail die Bankdaten seines Girokontos

Was sollte uns hier übel aufstoßen?

- Würde Rolf die Bankdaten seines Girokontos dem Höchstbietenden auch per Postkarte mitteilen...?
- Unverschlüsselte E-Mails sind wie Postkarten: Von **jedem** lesbar
(Chef, Internetanbieter, Nachbar von unten)

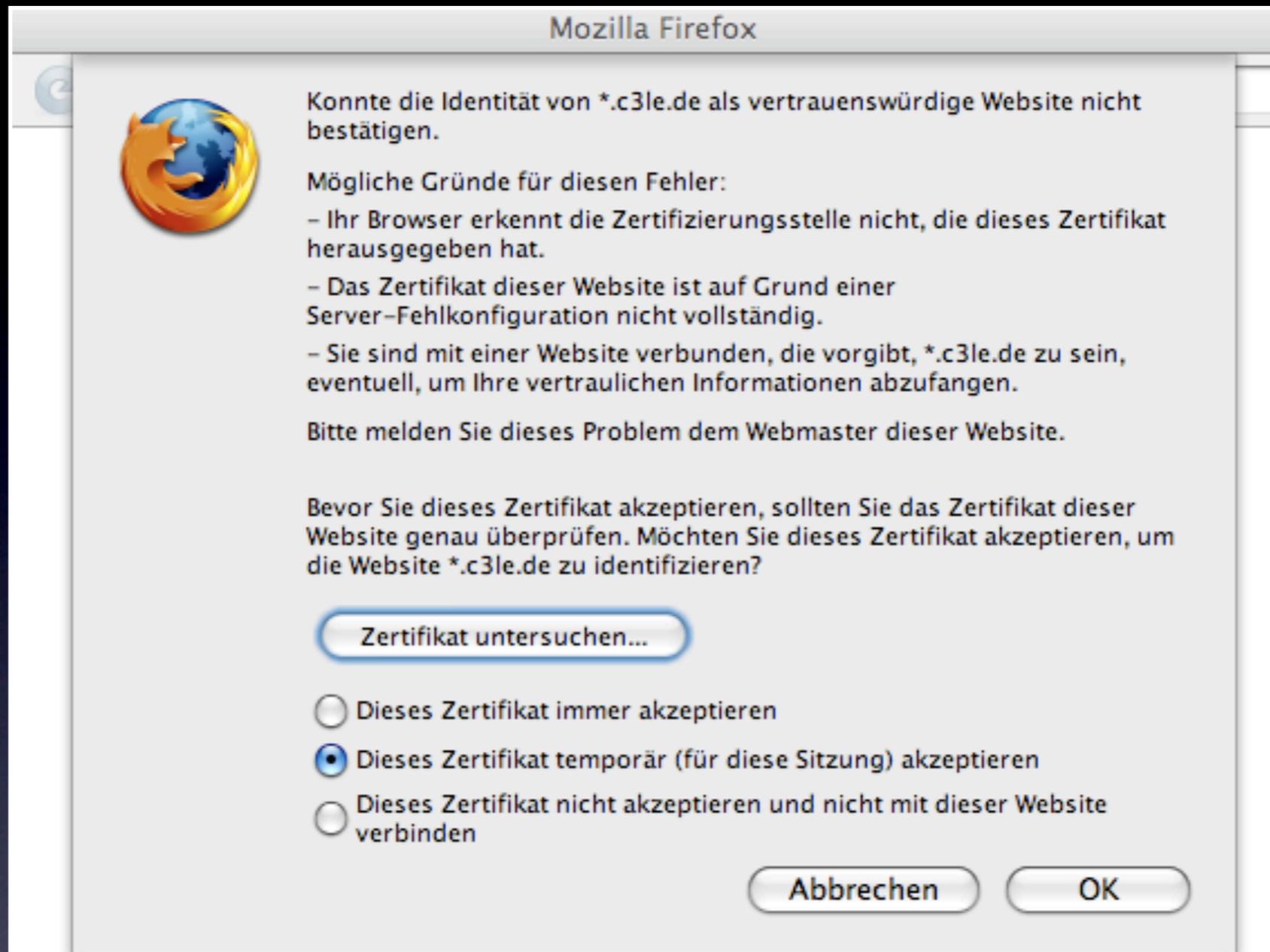
Digitale Verhütung

Sicher im Web

- Identitätsklau vor allem durch Phishing (engl. to fish = fischen) auf dem Vormarsch
- Kriminelle schicken E-Mails, die offizielle Institutionen (Banken, Versicherungen, Auktionsplattformen, etc.) vorgaukeln
- E-Mails enthalten Links auf gefälschte Webseiten, die persönliche Daten (vor allem Konto- bzw. Kreditkartendaten) „abfischen“

Wie kann man sich schützen?

- Banken, Versicherungen, etc. fordern niemals per E-Mail zur Eingabe von Logins, PINs oder TANs auf!
- Rücksprache mit der Bank halten!
- Weblink zur Bank immer über Lesezeichen!
- Auf SSL-Schutz achten...



Sicherheitsabfrage im Firefox

SSL-Zertifikate

- ein SSL-Zertifikat ist ein Dokument, welches die Echtheit einer Website durch eine dritte, vertrauenswürdige Instanz bestätigt („signiert“ bzw. „unterzeichnet“)
- gültige SSL-Zertifikate werden in modernen Browsern meist durch eine gelbe bzw. grüne Adresszeile angezeigt
- ungültige / fehlerhafte Zertifikate geben Warnmeldungen aus

SSL-Zertifikate II

- wann ist ein Zertifikat ungültig?
 - Ablaufdatum erreicht
 - Domainnamen stimmen nicht überein
 - Instanz, die das Zertifikat unterschrieben hat, ist nicht bekannt oder nicht vertrauenswürdig...

Allgemein Details

Dieses Zertifikat konnte nicht verifiziert werden, da es abgelaufen ist.

Herausgegeben für

Allgemeiner Name (CN)	plesk
Organisation (O)	SWsoft, Inc.
Organisationseinheit (OU)	Plesk
Seriennummer	44:C4:5C:48

Herausgegeben von

Allgemeiner Name (CN)	plesk
Organisation (O)	SWsoft, Inc.
Organisationseinheit (OU)	Plesk

Validität

Herausgegeben am	24.07.2006
Läuft ab am	24.07.2007

Fingerabdrücke

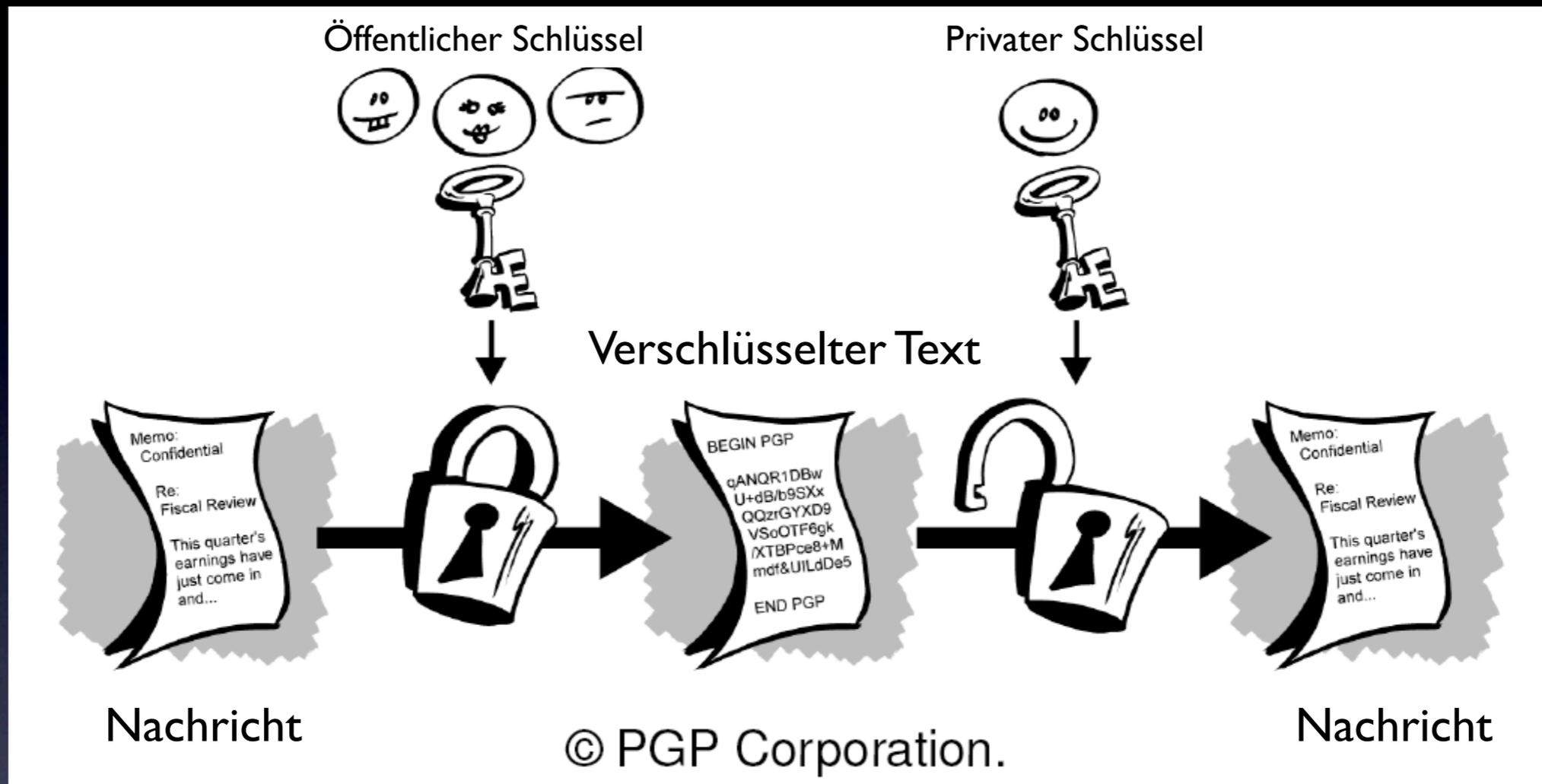
SHA1-Fingerprint	A3:EE:18:A6:11:DA:1E:95:6E:E1:43:80:81:6A:ED:40:F8:66:98:AE
MD5-Fingerprint	D9:35:9F:5F:3D:9A:5A:E5:26:EE:59:6A:72:3E:18:16

Schließen

Zertifikat-Details

Was tun gegen Mithörer / -leser?

- nicht mehr (digital) kommunizieren?
- eigene Geheimsprache (Chiffre)
ausdenken, um mit meinem Gegenüber zu
kommunizieren - wenig praktikabel
- Tandem aus Verschlüsselung und
Anonymisierungsdiensten nutzen!



Prinzip der asymmetrischen Verschlüsselung

Prinzip der asymmetrischen Verschlüsselung

- Analogon: Briefkasten
- jeder Teilnehmer erzeugt einmalig ein Schlüsselpaar
- Schlüsselpaar besteht aus öffentlichem und privatem Schlüssel
- öffentliche Schlüssel werden untereinander ausgetauscht und authentifiziert
- privater Schlüssel wird geheimgehalten
- Anwendungen: SSL, PGP/GnuPG, u.v.a.

Quelle: http://www.christiankoch.de/c3le/2007-04-08_gnupg_druck.pdf

dead fish

http://www.kamouflage.info/browse.php?u=Oi8vd3d3LnRob21hc2t1bGxlcj5ia RSS Google

URL: http://www.thomaskeller.biz/blog/ Go [home] [clear cookies]

Options: Encode URL Encode Page (beta) Allow Cookies Remove Scripts Remove Images Remove Flash

 **dead fish** only dead fish swim with the stream

Home About me

Digital Standards Organization

May 13, 2008 - 17:46

Via the NoOOXML mailing list:

When one thinks of international human rights, one thinks of The Hague - home of the International Court of Justice and the International Criminal Court, and the situs of an increasing number of Tribunals chartered to redress the assaults on human dignity that inexcusably continue to plague this planet. It is therefore appropriate that The Hague has been chosen to witness yet another pronouncement in defense of human rights. That pronouncement has been titled The Hague Declaration by the new international group, called the Digital Standards Organization ("Digistan," for short), that crafted it. In this blog entry, I'll talk about what the Declaration is all about, and what it is intended to achieve.

(Source)

Go to www.digistan.org for more information and sign The Hague Declaration.

ISO failed horribly last time to achieve what Digistan now goes after, lets just hope they get the credibility and acceptance throughout the community and public they need to move on.

 Share This

Posted in  OOXML, Standards |  No Comments >

Search

Recent Posts

- <> Digital Standards Organization
- <> Hide Qt GUI applications from the Mac OS X dock and menu
- <> montone hackery
- <> Perverted Logic / Monotone Summit
- <> The full story what has happened in Norway

Campaigns I support

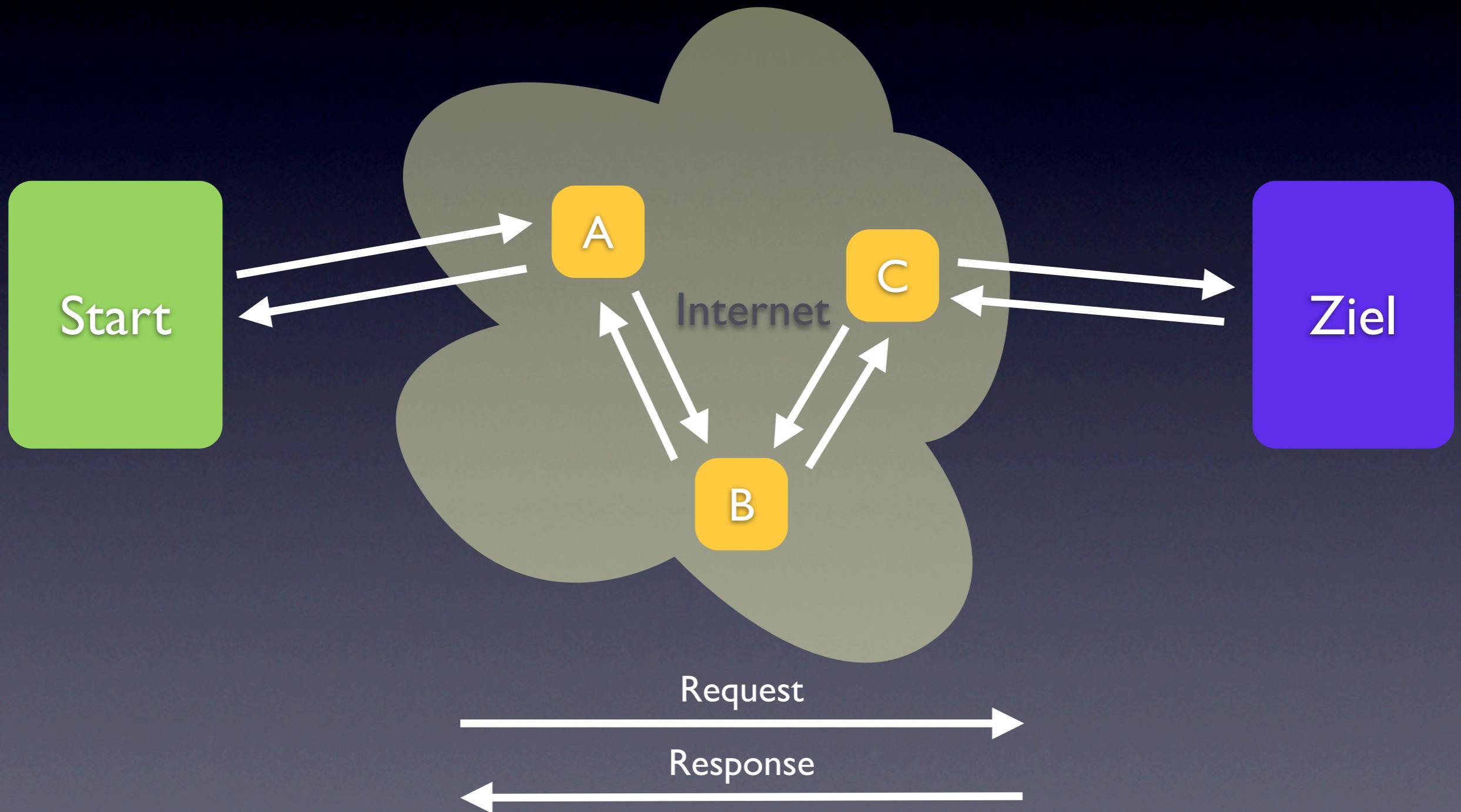


Anonymisierungsdienste

Anonymisierungsdienste

- Eben gesehen: einfacher Web-Proxy
- Aber: Problem ist nur verlagert:
 - Proxy speichert u. U. Verbindungsdaten
 - Einfache Web-Proxies nutzen normales Routing
- Deshalb: Anonymizer auf Mix-Basis...

Mix-Netzwerk



Mix-Netzwerk II

- Netzwerkverkehr wird über drei beliebige Knoten („Mixe“) A, B und C geleitet
- Zusammenhang zw. Start und Ziel aus Netzwerkstruktur nicht ablesbar:
 - A kennt nur Start und B
 - B kennt nur A und C
 - C kennt nur B und Ziel
- Übermittlung zw. den Mixen verschlüsselt

Mix-Netzwerk III

- Vorteil: maximale Anonymisierung, maximale Sicherheit
- Nachteil: langsamer Datendurchsatz (oftmals im ISDN-Bereich oder darunter), da kryptografisch aufwendig
- Anwendungen: TOR, JAP
 - Verschlüsselung des ges. Internetverkehrs
 - TOR: Plugins für Firefox und Thunderbird

Fazit

- anonyme Kommunikation ist Luxus und erfordert Anstrengungen (Konsumenzug?)
- gesundes Misstrauen ggü. fremden / „seltsam“ anmutenden Diensten ist hilfreich
- Verhältnismäßigkeit bewahren: Wer öffentliche Profile bei MySpace, XING und / oder StudiVZ hat, braucht sich keine Gedanken mehr über die Weitergabe seiner persönlichen Daten machen...

Fragerunde

Praxis-Workshop