FP-Block

usable web privacy

by controlling browser fingerprinting

Joint work with Sjouke Mauw (UL), Christof Ferreira Torres (UL)

Open Universiteit

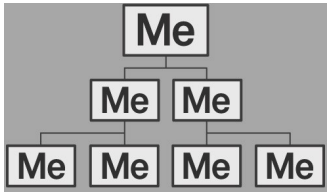
www.ou.nl

OUtline

- Part 1:
  introduction

- Part 2:
  thwarting 3rd party fingerprint-based web-tracking

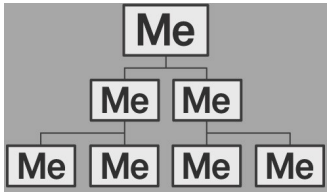
Introducing myself



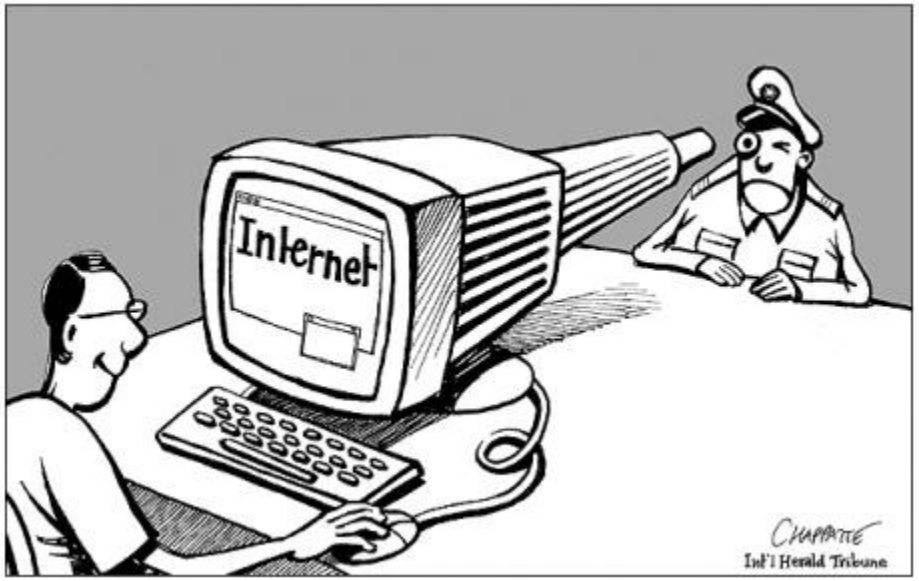
- PhD thesis on Fair Sharing and Vote Privacy (UL & TU/e)
- Voting @ University of Surrey
- Privacy in mobile/web @ University of Luxembourg
- Hybrid mixnet @ TU Darmstadt
- Interests:
  - vote privacy
  - healthcare privacy, e-health
  - auction verifiability & privacy
  - formalising privacy
  - practical security

Open Universiteit
www.ou.nl

Introducing myself



- PhD thesis on Fair Sharing and Vote Privacy (UL & TU/e)
- Voting @ University of Surrey
- Privacy in mobile/web @ University of Luxembourg
- Hybrid mixnet @ TU Darmstadt
- Interests:
  - vote priv
  - healthca
  - auction v
  - formalisi
  - practical

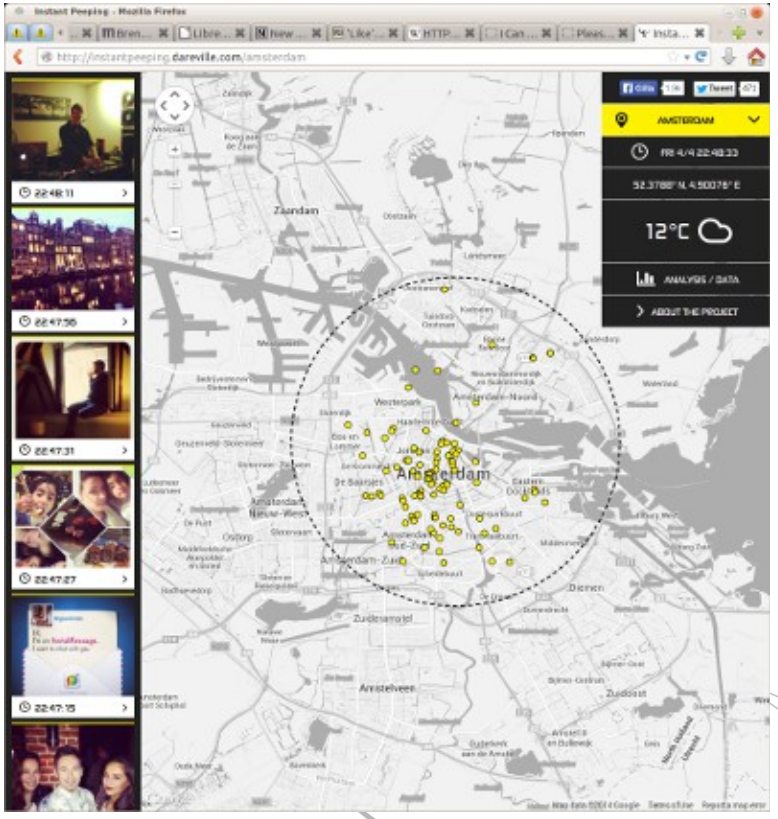


Open Universiteit
www.ou.nl

We are terrible at privacy

Open Universiteit
www.ou.nl

We are terrible at privacy



Open Universiteit
www.ou.nl

We are terrible at privacy

Open Universiteit
www.ou.nl

We are terrible at privacy

Open Universiteit
www.ou.nl

We really don't get privacy

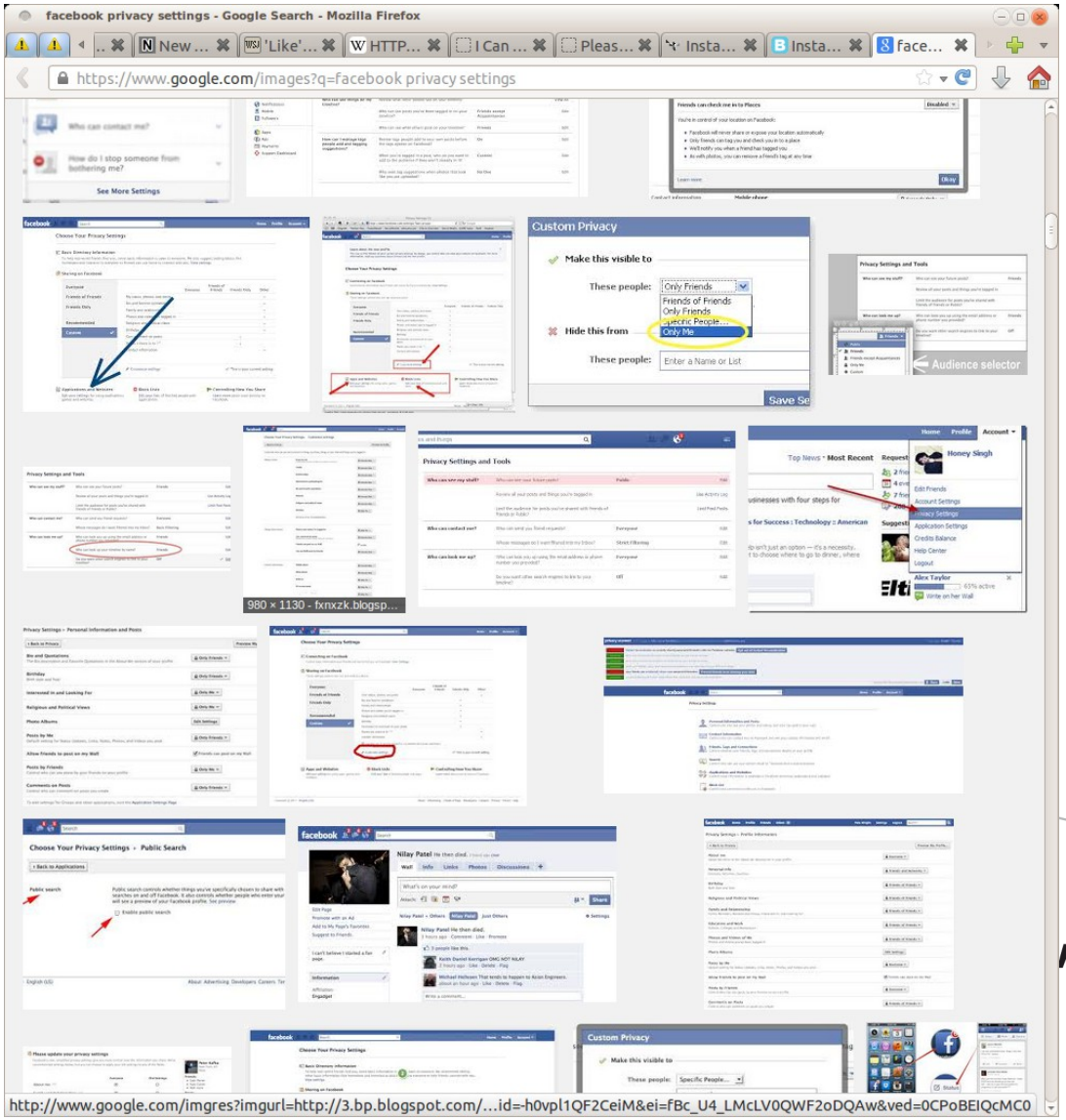
Open Universiteit
www.ou.nl

We really don't get privacy

Note: account number can suffice for withdrawal

In our defence: privacy is hard...

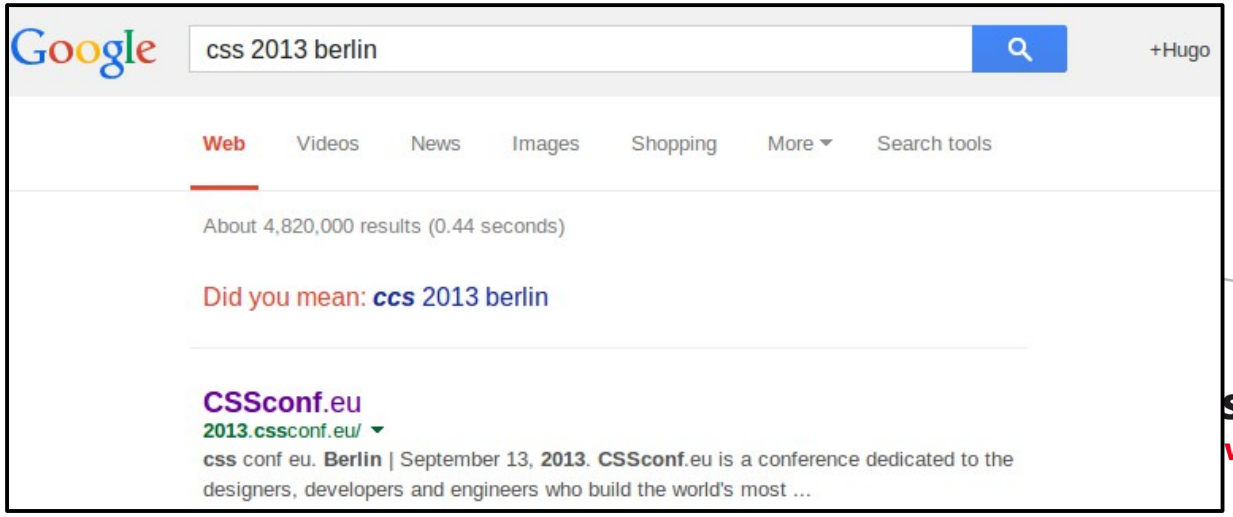
In our defence: privacy is hard...



… really hard...

TECH | 2/16/2012 @ 11:02AM | 2,398,698 views

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



siteit
w.ou.nl

… really, really hard.

*“Another thing which is just an observation, when I was working on the **blocking of the social plugins**, I always used the*  *website to test my implementation. Today **Facebook suggested** me on my phone the **group of***  *.”*

– anonymous UL Bachelor student / coauthor

Open Universiteit
www.ou.nl

Reasoning about privacy

Open Universiteit
www.ou.nl

Reasoning about privacy

- Privacy is wrt. someone

Open Universiteit
www.ou.nl

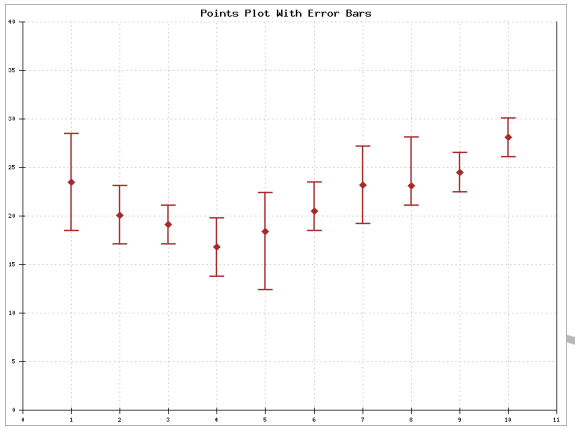
Reasoning about privacy

- Privacy is wrt. someone
- Two sides:
  - (in)distinguishability

Open Universiteit
www.ou.nl

Reasoning about privacy

- Privacy is wrt. someone
- Two sides:
  - (in)distinguishability
  - (un)certainty

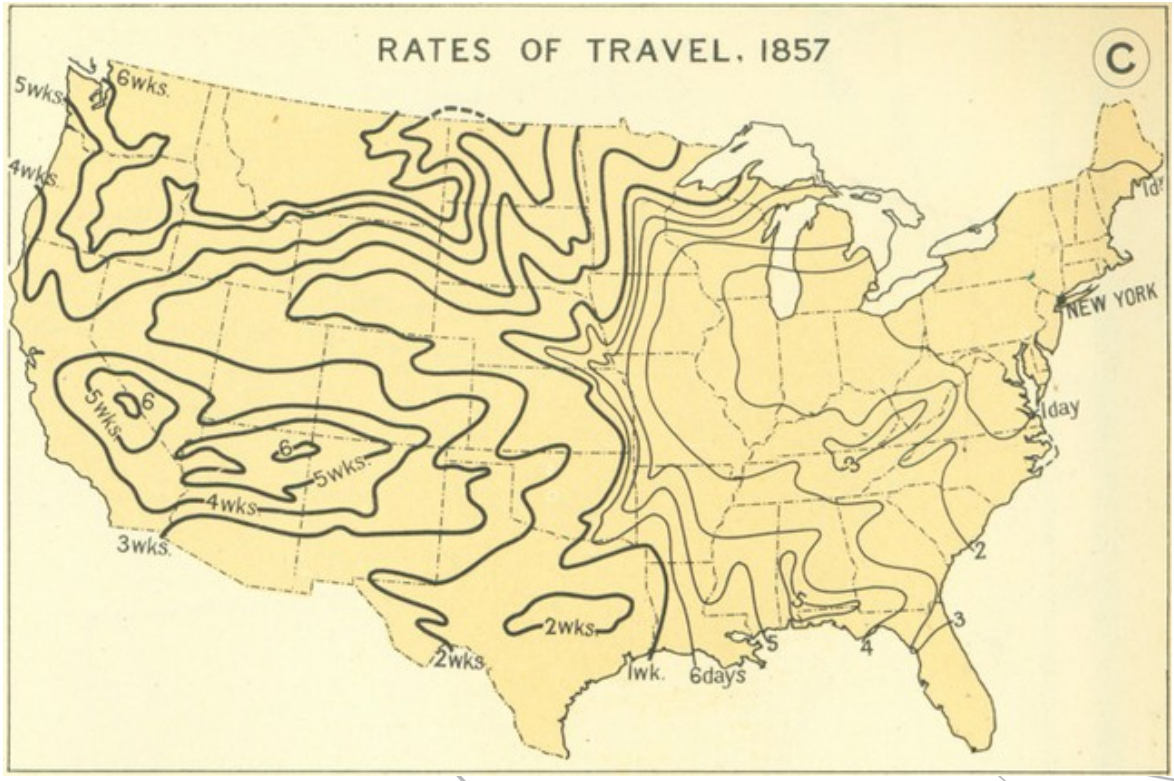


Open Universiteit
www.ou.nl

Did privacy become harder?

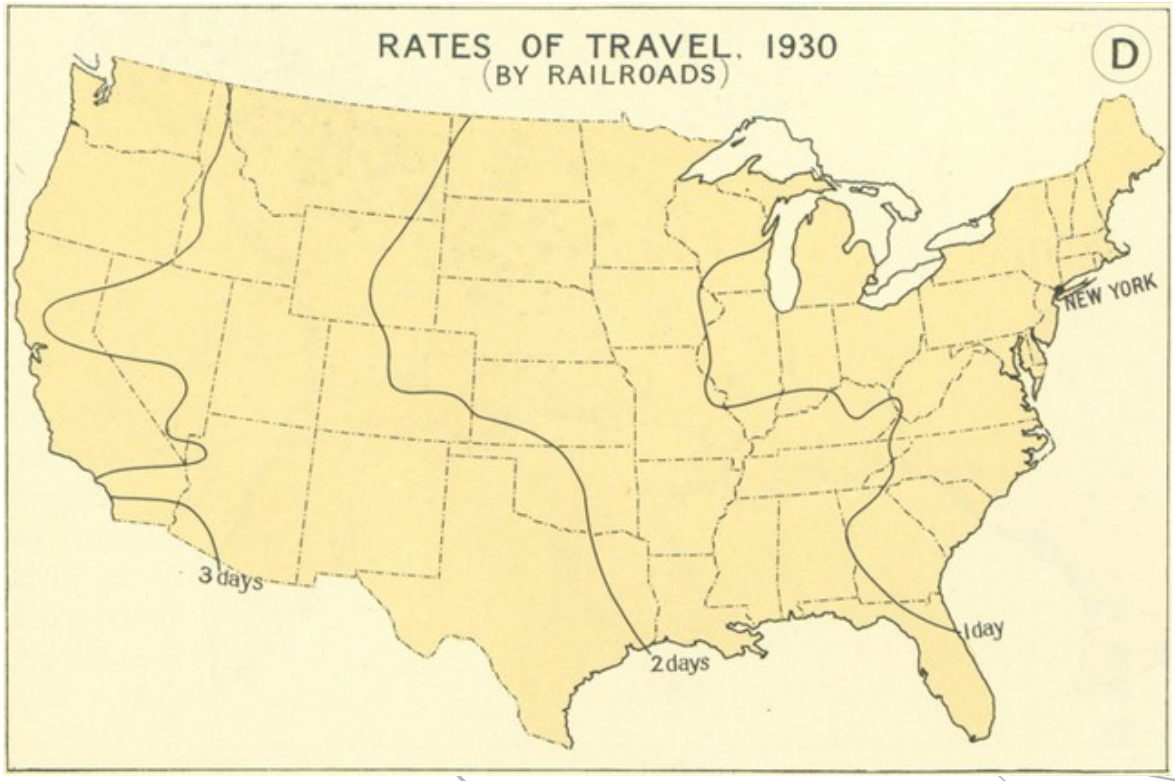
Open Universiteit
www.ou.nl

Did privacy become harder?



Open Universiteit
www.ou.nl

Did privacy become harder?



Open Universiteit
www.ou.nl

Did privacy become harder?

Open Universiteit
www.ou.nl

My research interests in a nutshell

Open Universiteit
www.ou.nl

My research interests in a nutshell

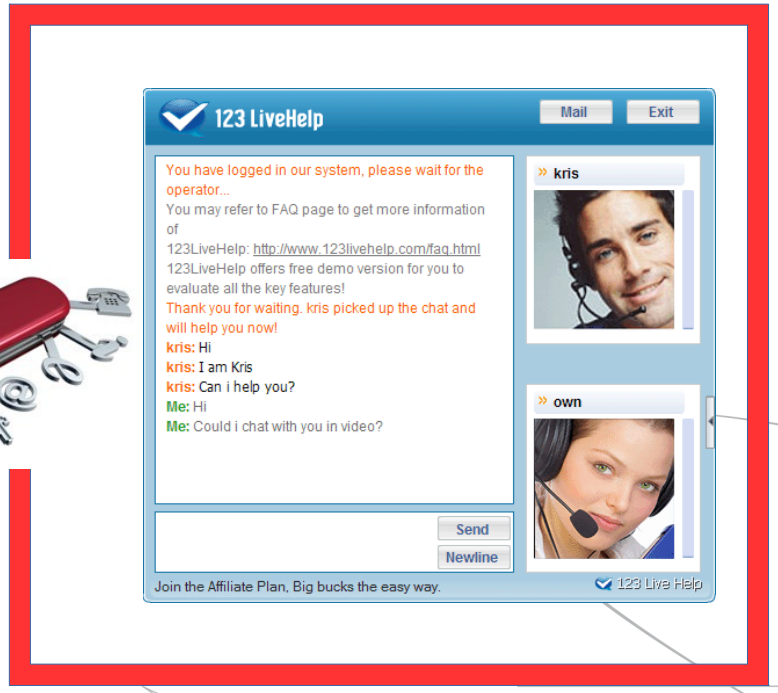
Open Universiteit
www.ou.nl

My research interests in a nutshell

Open Universiteit
www.ou.nl

My research interests in a nutshell

≈



Open Universiteit
www.ou.nl

FP-Block

usable web privacy
by controlling browser fingerprinting

Open Universiteit
www.ou.nl

OUtline

- What is tracking
- What is FP-based tracking
- Literature + countermeasures
- Web identities
- Fingerprint surface / Fingerprint vectors
- FP-Block

Open Universiteit
www.ou.nl

Reasons to track

- Find site errors / problems
- Count visitors, not pageviews
- Detect suspicious logins
- Targeted advertising

- Goal: track **a user**

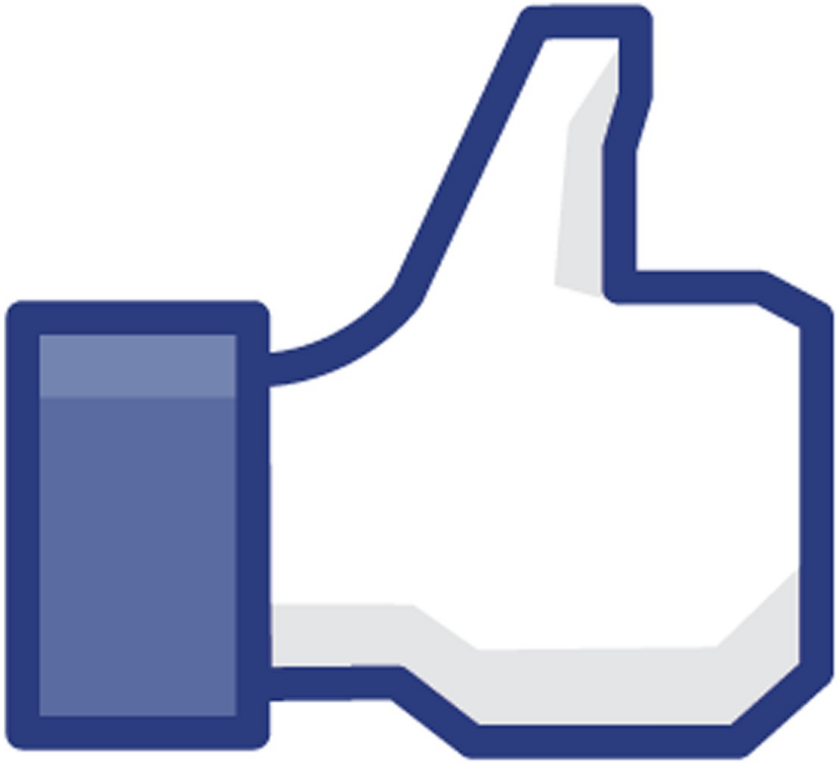
Web tracking

Tracking is good!

- Fraud prevention
- Improving web site usability
  - Finding common browsing “errors”
  - Related items of interest
  - ...

Open Universiteit
www.ou.nl

Embedded tracking, however...



ersiteit
www.ou.nl

Embedded tracking, however...

- Buttons everywhere

Embedded tracking, however...

- Buttons everywhere
- JS code loaded from social network
  - Request will send cookie
  - Response can set / update cookie

Embedded tracking, however...

- Buttons everywhere
- JS code loaded from social network
  - Request will send cookie
  - Response can set / update cookie
- Facebook can track people not on FB [Roos11]

Embedded tracking, however...

- Buttons everywhere

- JS code loaded from social network
  - Request will send cookie
  - Response can set / update cookie

- Facebook can track people not on FB [Roos11]
- Google is worse (AdSense, Analytics)

Embedded content

1. Content delivery networks
2. Advertising
3. Analytics and tracking
4. Embedded media
5. Social plugins
6. Payment
7. Libraries
8. ….

Open Universiteit
www.ou.nl

Embedded content

1. Content delivery networks
2. Advertising
3. Analytics and tracking
4. Embedded media
5. Social plugins
6. Payment
7. Libraries
8. ….

	Top 10k	Top 1mil
1. Akamai	17%	11%
2. Doubleclick	10%	20%
3. Google Analytics	19%	44%
4. YouTube	26%	47%
5. Facebook Like*	20%	16%
6. PayPal button	33%	44%
7. JQuery	18%	20%

Open Universiteit
www.ou.nl

Embedded content

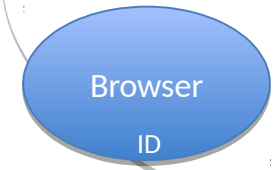
1. Content delivery networks
2. Advertising
3. Analytics and tracking
4. Embedded media
5. Social plugins
6. Payment
7. Libraries
8. ….

	Top 10k	Top 1mil
1. Akamai	17%	11%
2. Doubleclick	10%	20%
3. Google Analytics	19%	44%
4. YouTube	26%	47%
5. Facebook Like*	20%	16%
6. PayPal button	33%	44%
7. JQuery	18%	20%

* aggregated numbers from builtwith.com.
numbers by similartech.com are higher.

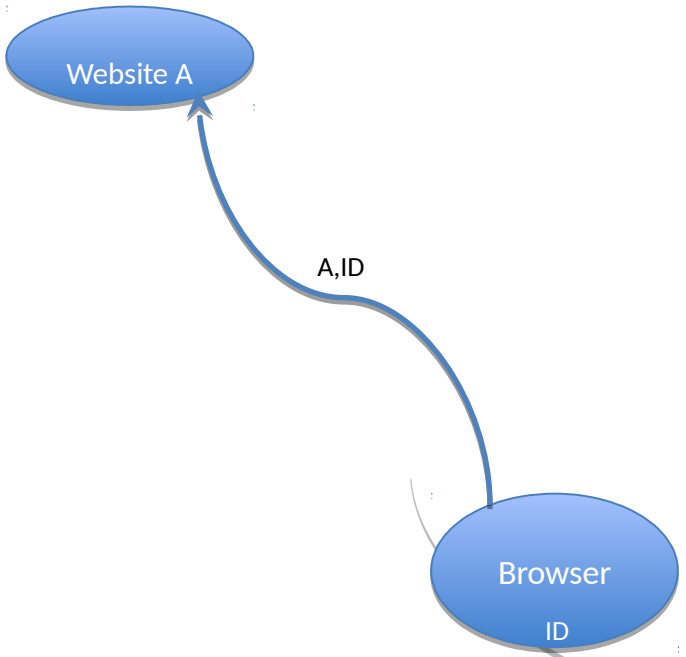
Open Universiteit
www.ou.nl

Tracking via embedded content



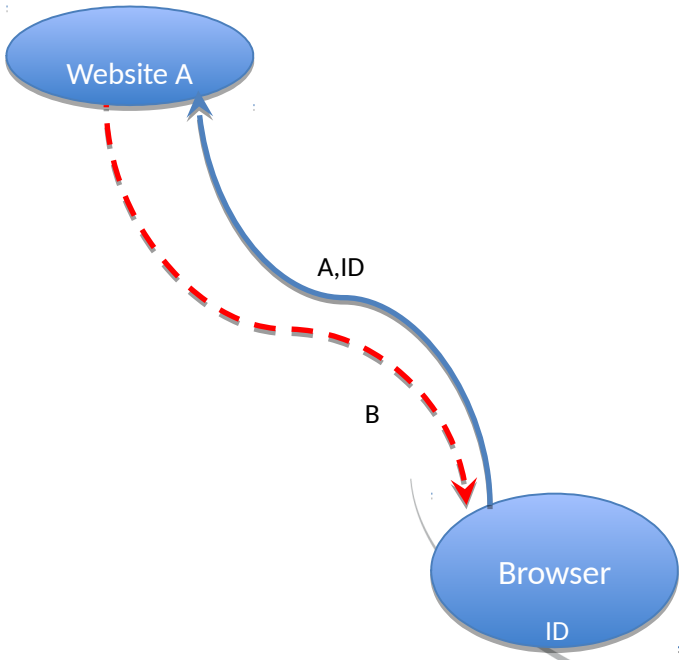
Open Universiteit
www.ou.nl

Tracking via embedded content



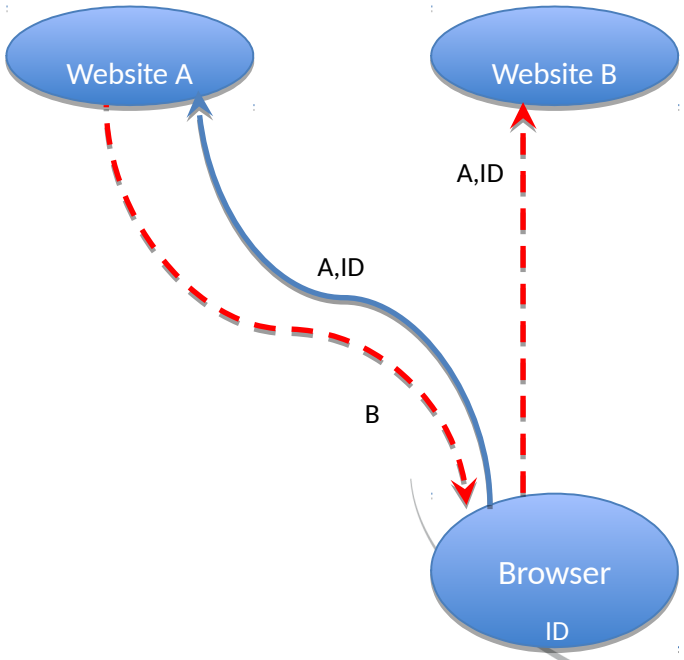
Open Universiteit
www.ou.nl

Tracking via embedded content



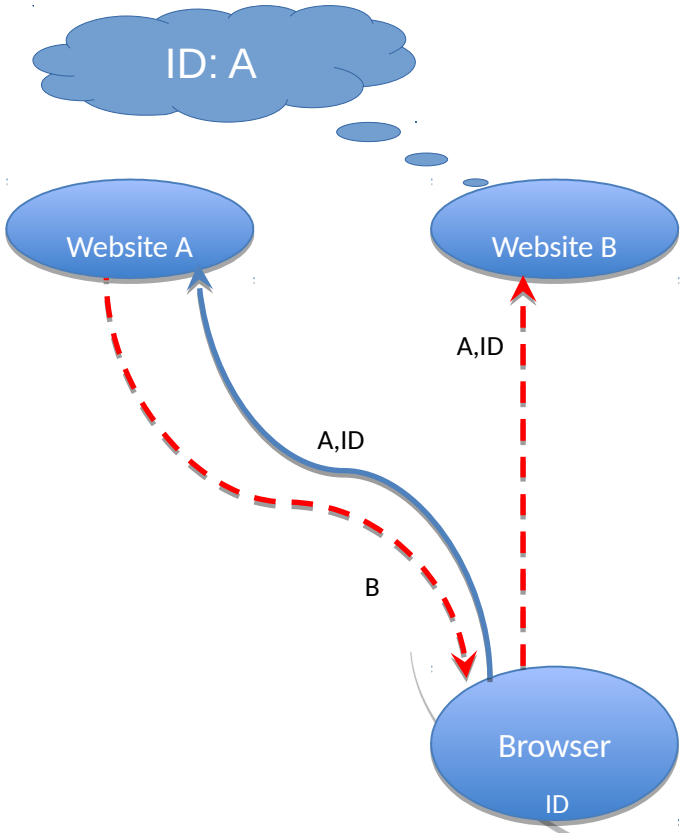
Open Universiteit
www.ou.nl

Tracking via embedded content



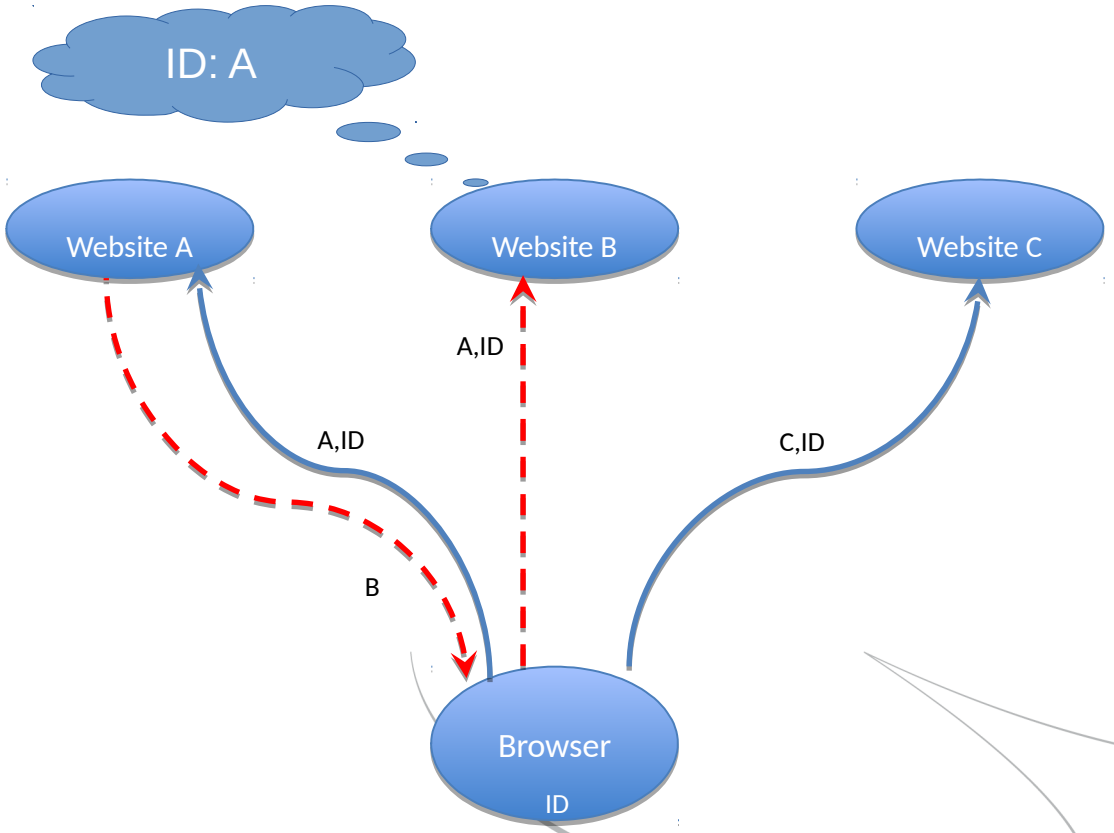
Open Universiteit
www.ou.nl

Tracking via embedded content



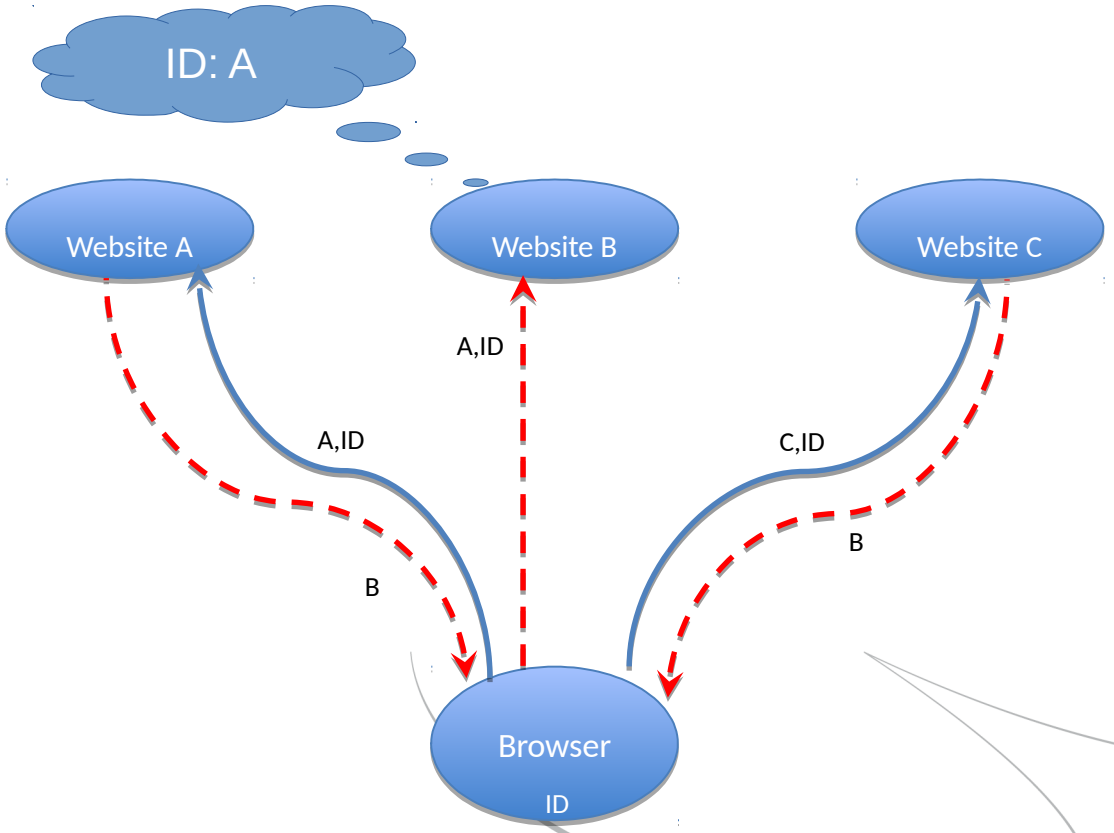
Open Universiteit
www.ou.nl

Tracking via embedded content



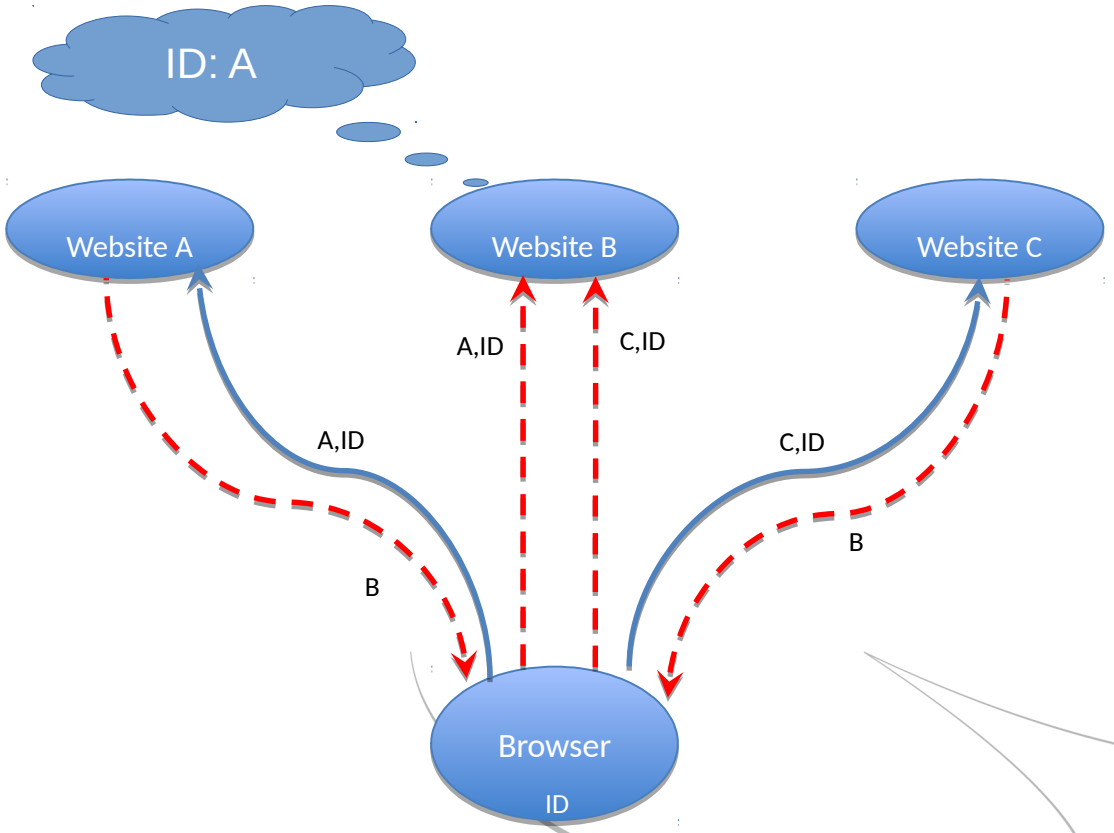
Open Universiteit
www.ou.nl

Tracking via embedded content



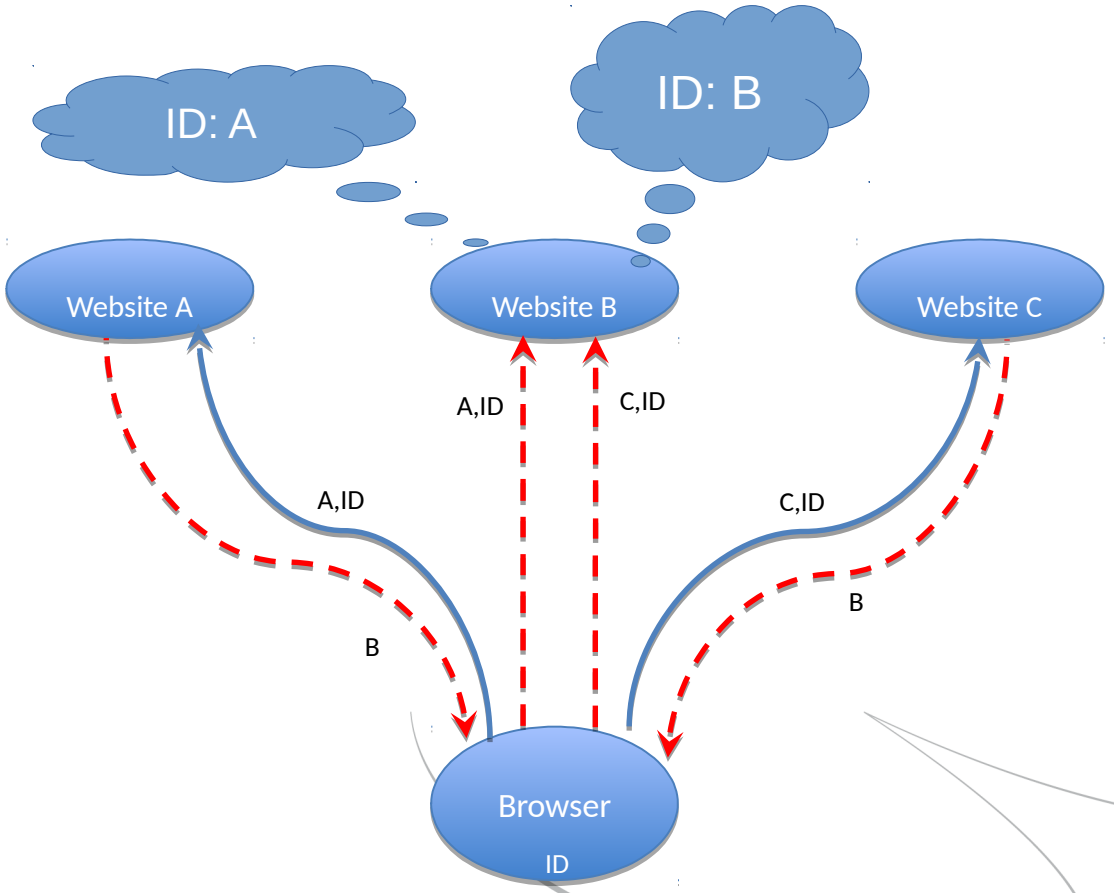
Open Universiteit
www.ou.nl

Tracking via embedded content



Open Universiteit
www.ou.nl

Tracking via embedded content



Open Universiteit
www.ou.nl

How to track

- Client-side
  - Cookies / evercookies / zombiecookies / ...
  - History exploit / CSS tricks / ...
  - Active fingerprinting
- Server-side only
  - Web bugs
  - Passive fingerprinting

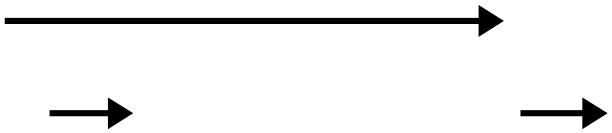
Why fingerprinting?

- Cookies: client-side storage.
- Fingerprinting:
  - Passive: infer info from server side.
  - Active: gather info from client side on-the-fly.

- Actually in use?
  - [S&P13, CCS13]: some, but not much... yet.

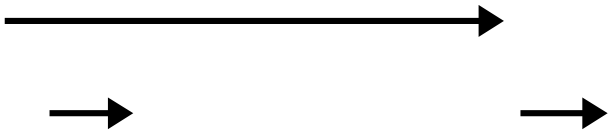
Related work

Panopticlick [PETS10]



Panopticlick [PETS10]

- Effectiveness of fingerprinting



Open Universiteit
www.ou.nl

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS → better results
  - Mobile → less plugins → better results

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS → better results
  - Mobile → less plugins → better results
- Fingerprints change...

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS → better results
  - Mobile → less plugins → better results
- Fingerprints change...
- ...predecessor found in 65% (99.1% correct)

Open Universiteit
www.ou.nl

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS → better results
  - Mobile → less plugins → better results
- Fingerprints change...
- ...predecessor found in 65% (99.1% correct)
- Revealing: order of fonts, order of plugins

Open Universiteit
www.ou.nl

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS ⟶ better results
  - Mobile ⟶ less plugins ⟶ better results
- Fingerprints change...
- ...predecessor found in 65% (99.1% correct)
- Revealing: order of fonts, order of plugins
- Defensive paradox

Open Universiteit
www.ou.nl

Panopticlick (2)

Test	Entropy (bits)
user-agent header	10.00
plugins	15.40
fontlist	13.90
screen resolution	4.83
supercookie test	2.12
http accept headers	6.09
timezone	3.04
cookies enabled?	0.35

Panopticlick (2)

Test	Entropy (bits)	
user-agent header	10.00	←
plugins	15.40	←
fontlist	13.90	←
screen resolution	4.83	
supercookie test	2.12	
http accept headers	6.09	
timezone	3.04	
cookies enabled?	0.35	

Open Universiteit

Panopticlick (2)

Test	Entropy (bits)	
user-agent header	10.00	←
plugins	15.40	←
fontlist	13.90	←
screen resolution	4.83	
supercookie test	2.12	
http accept headers	6.09	
timezone	3.04	
cookies enabled?	0.35	

Open Universiteit

Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)

More ways to fingerprint

More ways to fingerprint

[W2SP11] – fingerprinting JavaScript implementations
Hooray for the speedwars!

More ways to fingerprint

[W2SP11] – fingerprinting JavaScript implementations
Hooray for the speedwars!

[W2SP12] – fingerprinting HTML5 font rendering
All Arials are equal... except most aren't.

More ways to fingerprint

[W2SP11] – fingerprinting JavaScript implementations
Hooray for the speedwars!

[W2SP12] – fingerprinting HTML5 font rendering
All Arials are equal... except most aren't.

[W2SP13] – fingerprinting JS engine errors.
“Foutje, bedankt.”

More ways to fingerprint

[W2SP11] – fingerprinting JavaScript implementations
Hooray for the speedwars!

[W2SP12] – fingerprinting HTML5 font rendering
All Arials are equal... except most aren't.

[W2SP13] – fingerprinting JS engine errors.
“Foutje, bedankt.”

Clock skew can be passively detected, proxies don't help.

Fighting fingerprinting

Fighting fingerprinting

- Do Not Track header? [NSDI12]: **X**

Open Universiteit
www.ou.nl

Fighting fingerprinting

- Do Not Track header? [NSDI12]: **X**
- Blacklisting fingerprinters? [W2SP11]: **X**

Open Universiteit
www.ou.nl

Fighting fingerprinting

- Do Not Track header? [NSDI12]: **X**
- Blacklisting fingerprinters? [W2SP11]: **X**
- FireGloves [NordSec11]? [CCS13]: **X**
- Tor Browser? [CCS13]: **X**

Open Universiteit
www.ou.nl

Fighting fingerprinting

- Do Not Track header? [NSDI12]: **X**
- Blacklisting fingerprinters? [W2SP11]: **X**
- FireGloves [NordSec11]? [CCS13]: **X**
- Tor Browser? [CCS13]: **X**

- Again: defensive paradox.

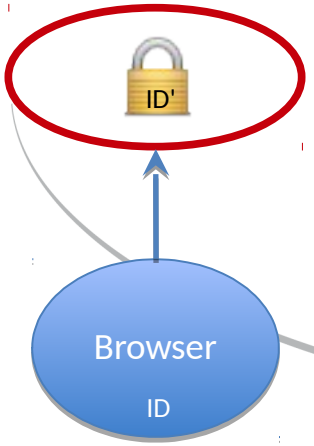
Open Universiteit
www.ou.nl

Privacy plugins

. . .

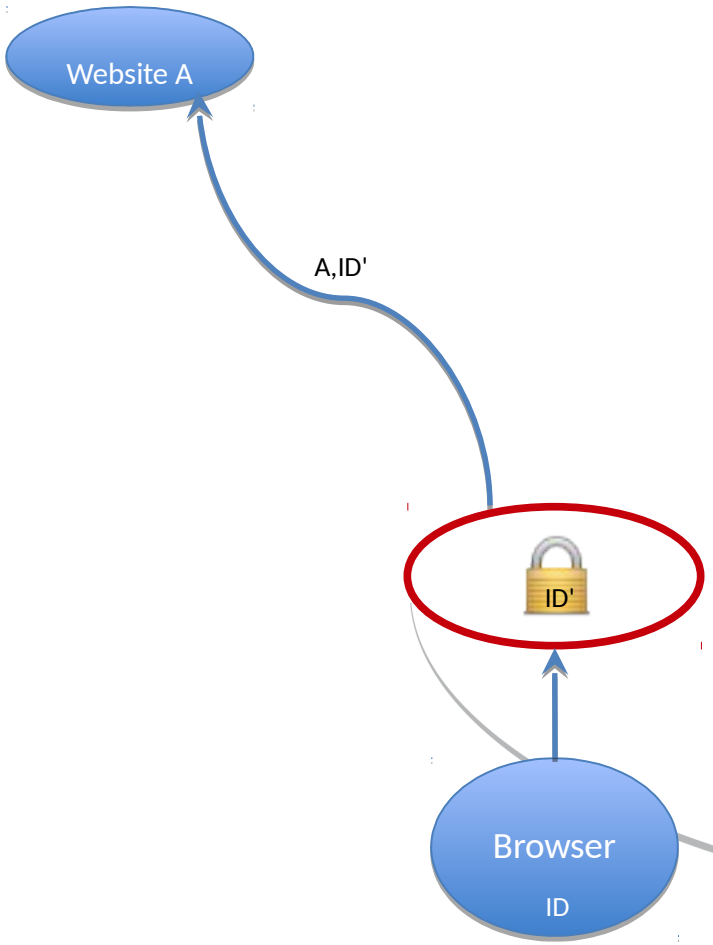
ersiteit
www.ou.nl

Typical countermeasures



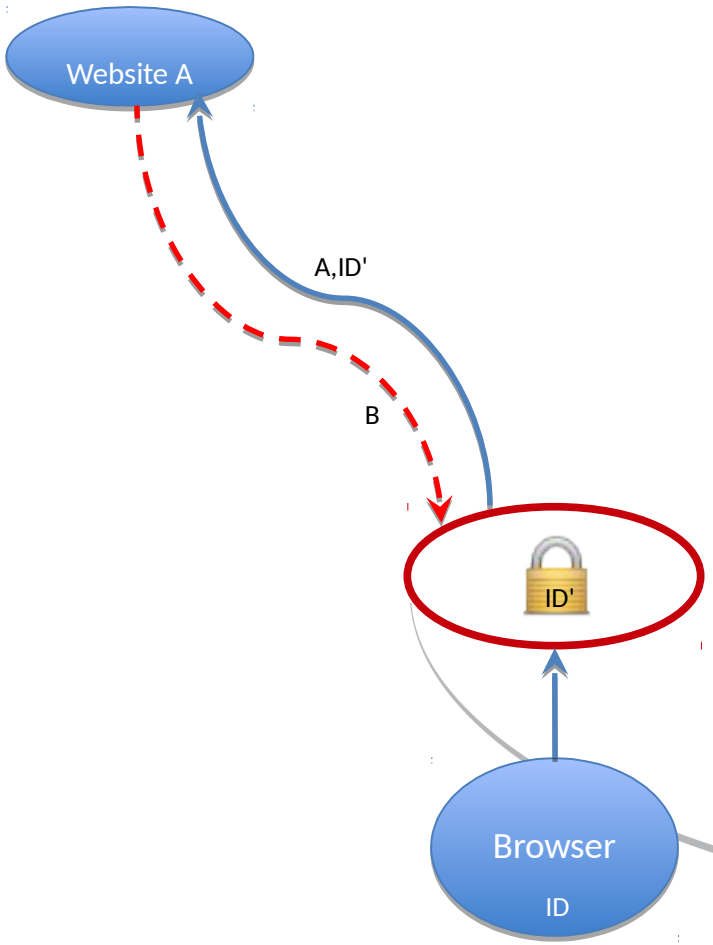
Open Universiteit
www.ou.nl

Typical countermeasures



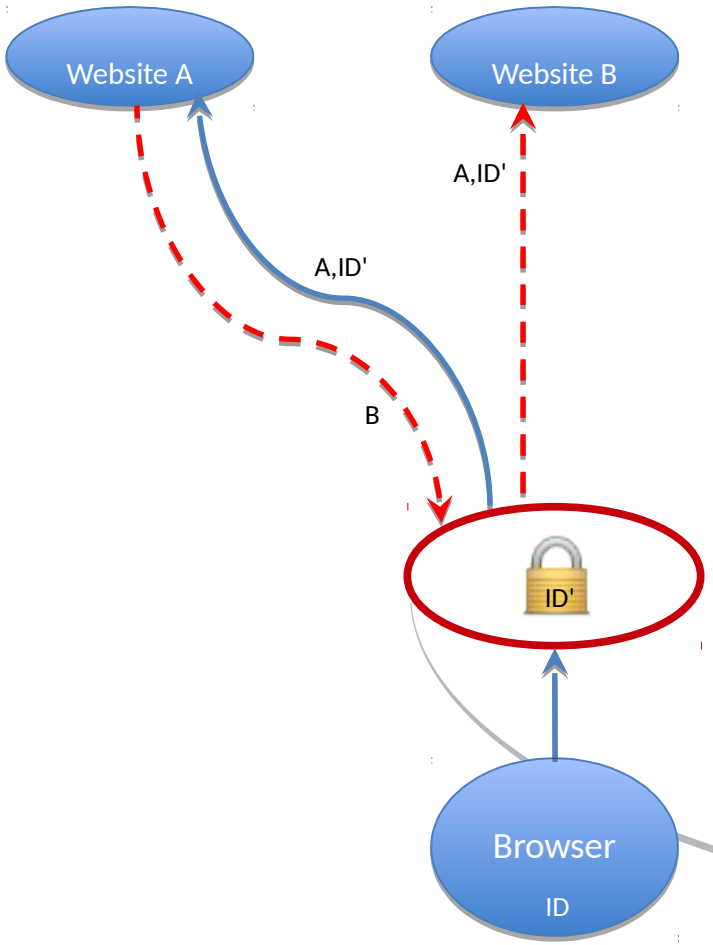
Open Universiteit
www.ou.nl

Typical countermeasures



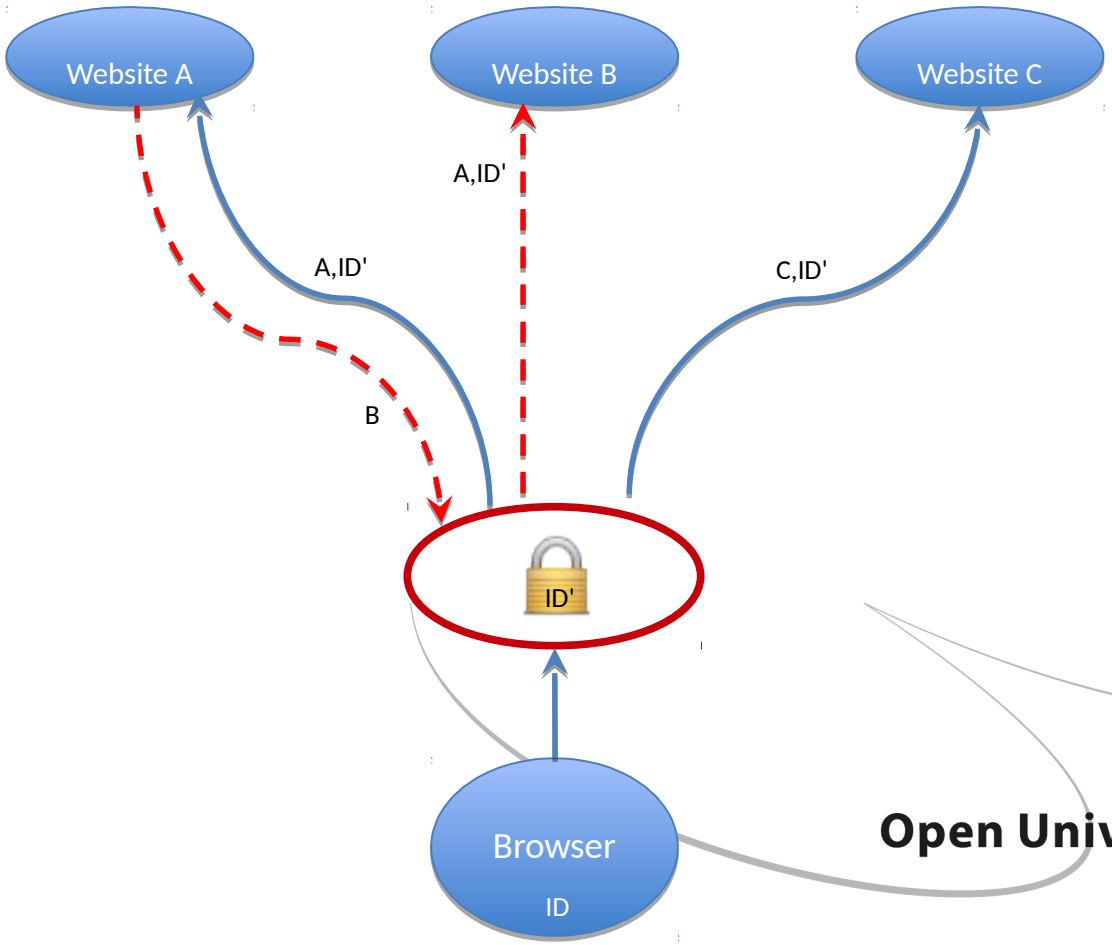
Open Universiteit
www.ou.nl

Typical countermeasures



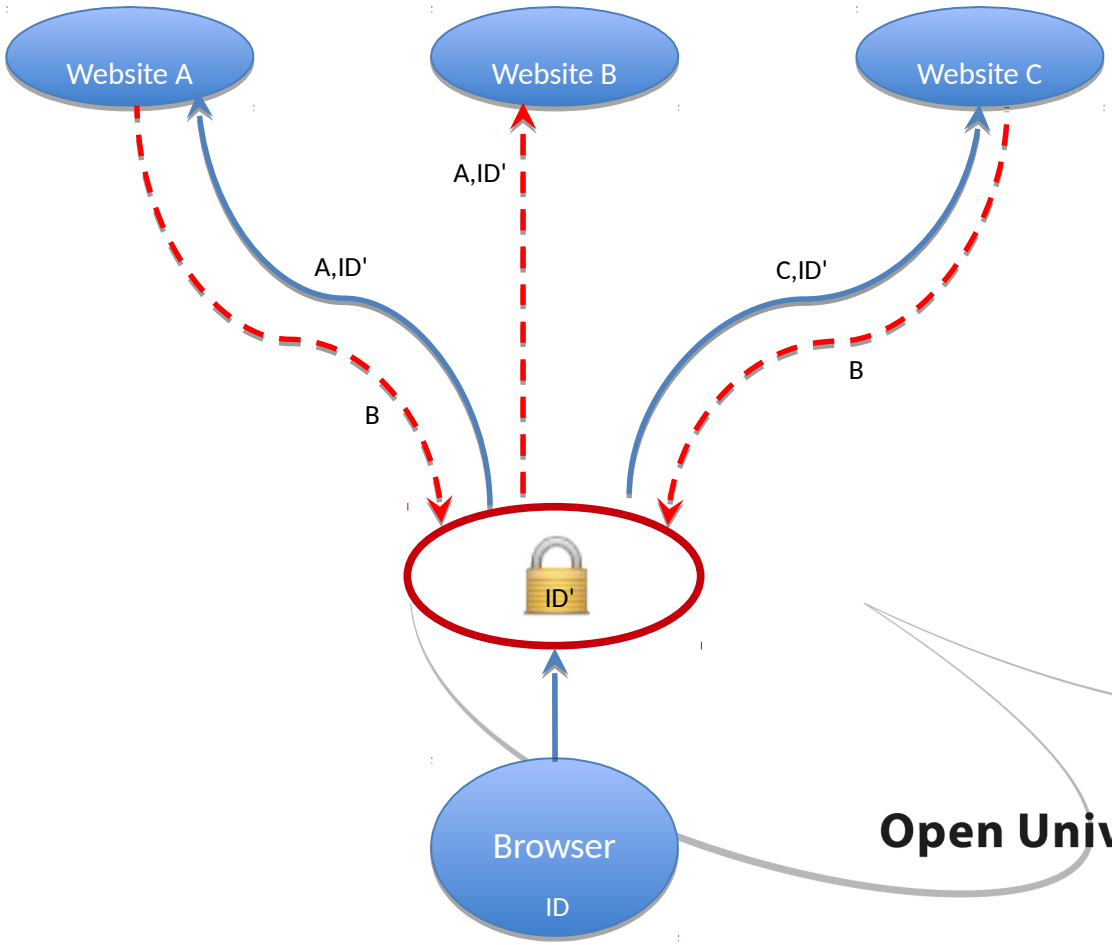
Open Universiteit
www.ou.nl

Typical countermeasures



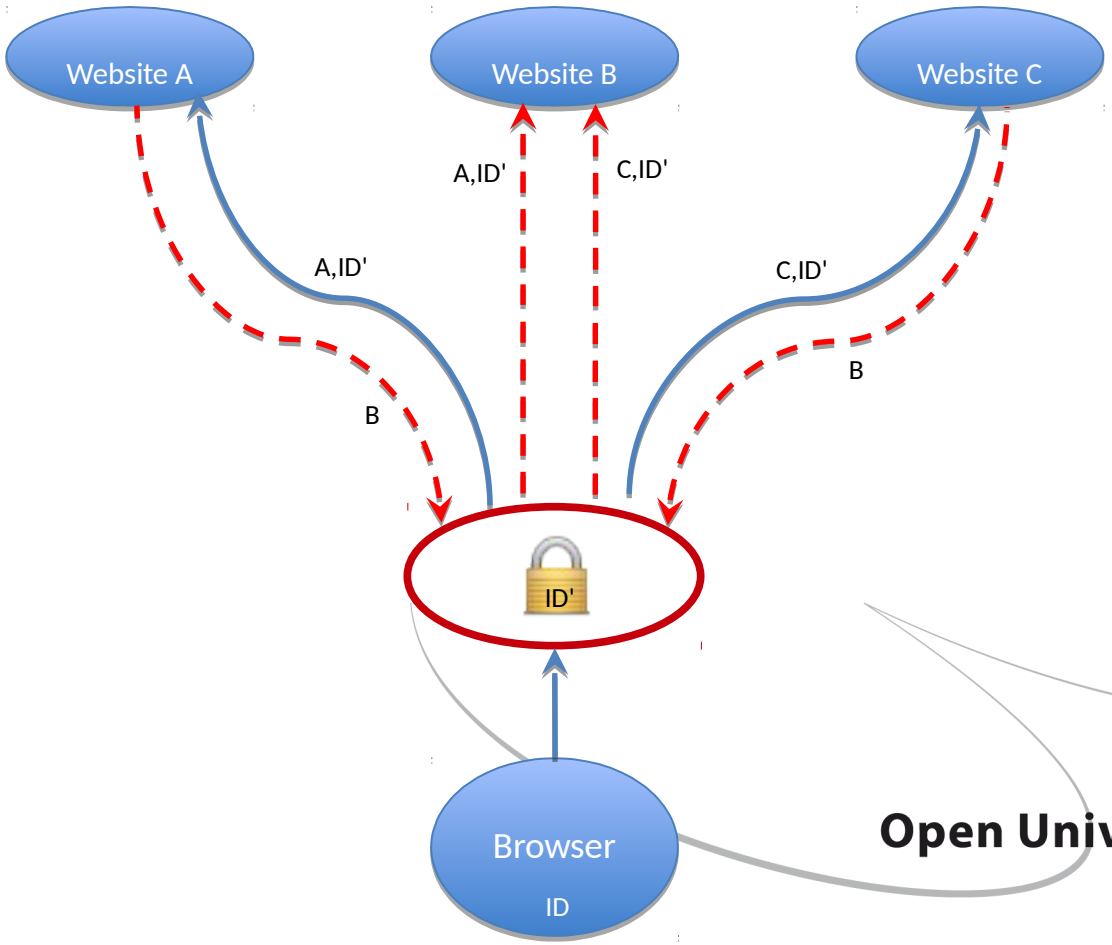
Open Universiteit
www.ou.nl

Typical countermeasures



Open Universiteit
www.ou.nl

Typical countermeasures



Open Universiteit
www.ou.nl

Overcoming the defensive paradox

The defense can be detected …

... which makes you more unique.

Open Universiteit
www.ou.nl

Overcoming the defensive paradox

The defense can be detected …

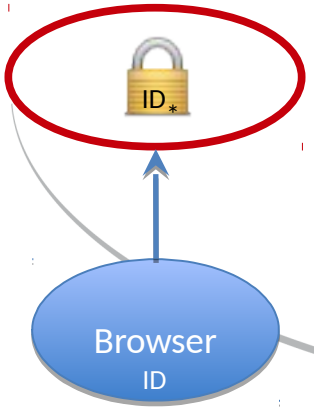
... which makes you more unique.

How to overcome?

- Leverage this uniqueness;
- Allow local tracking.

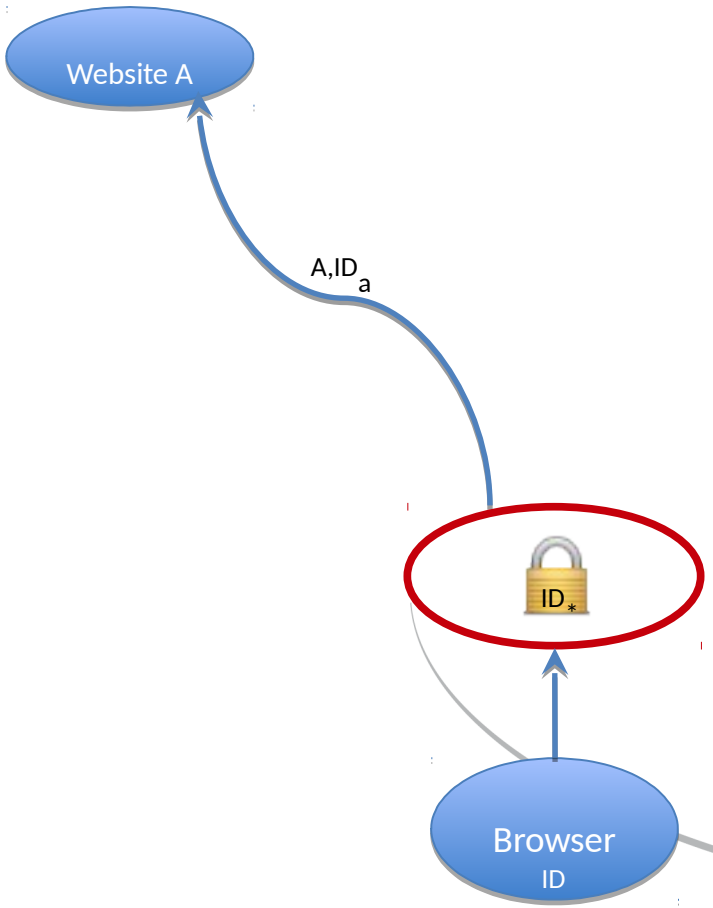
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



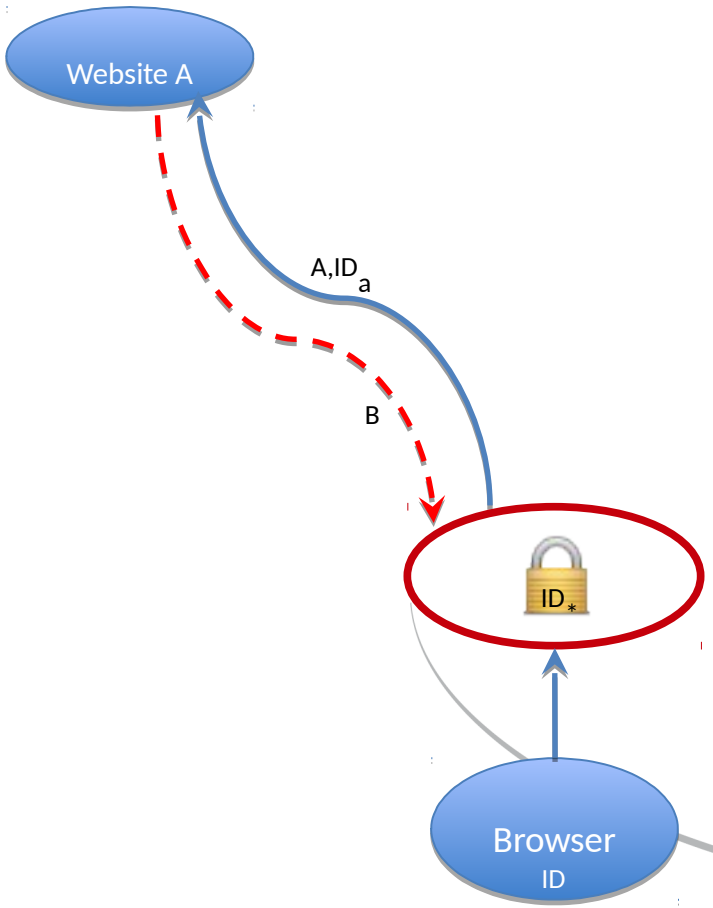
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



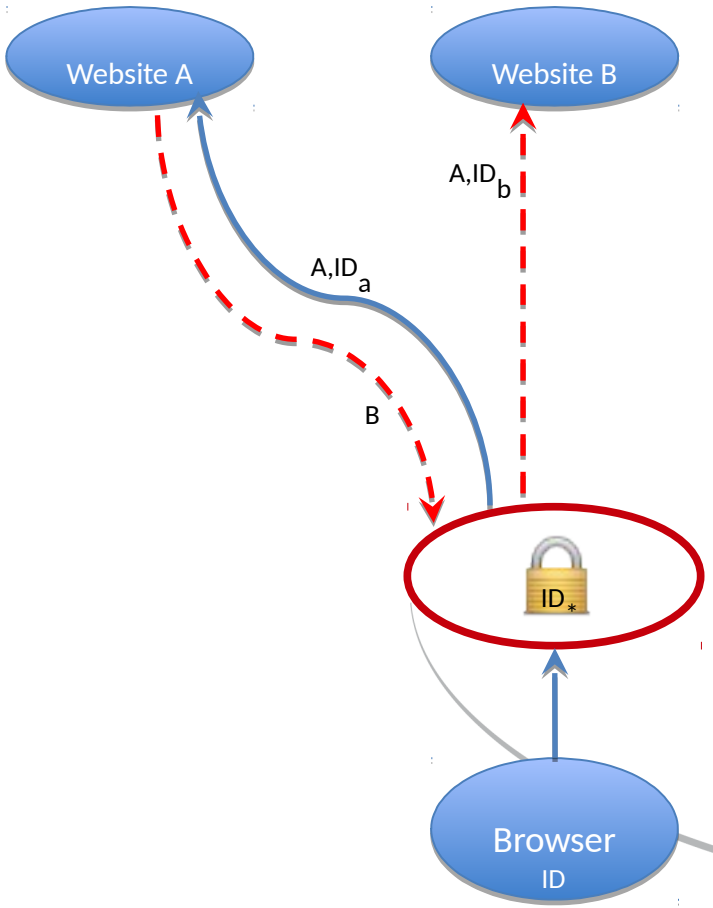
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



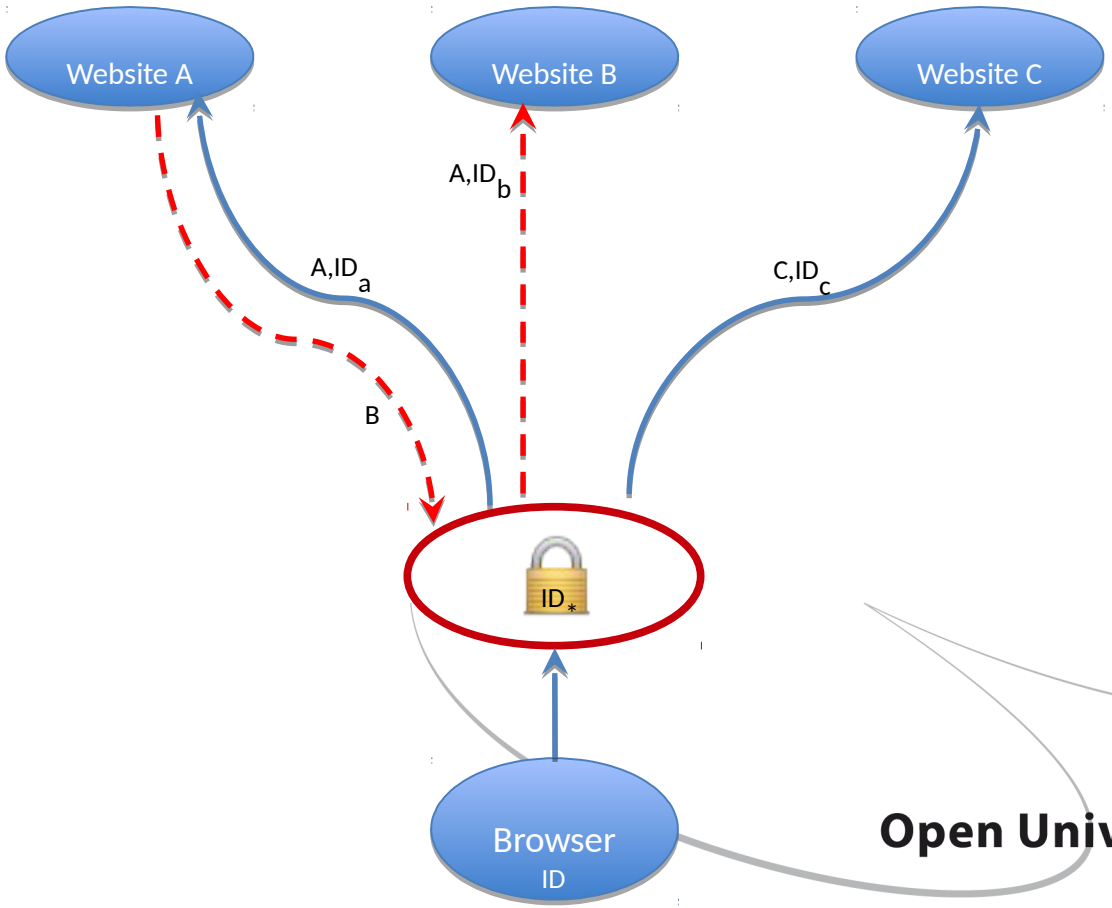
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



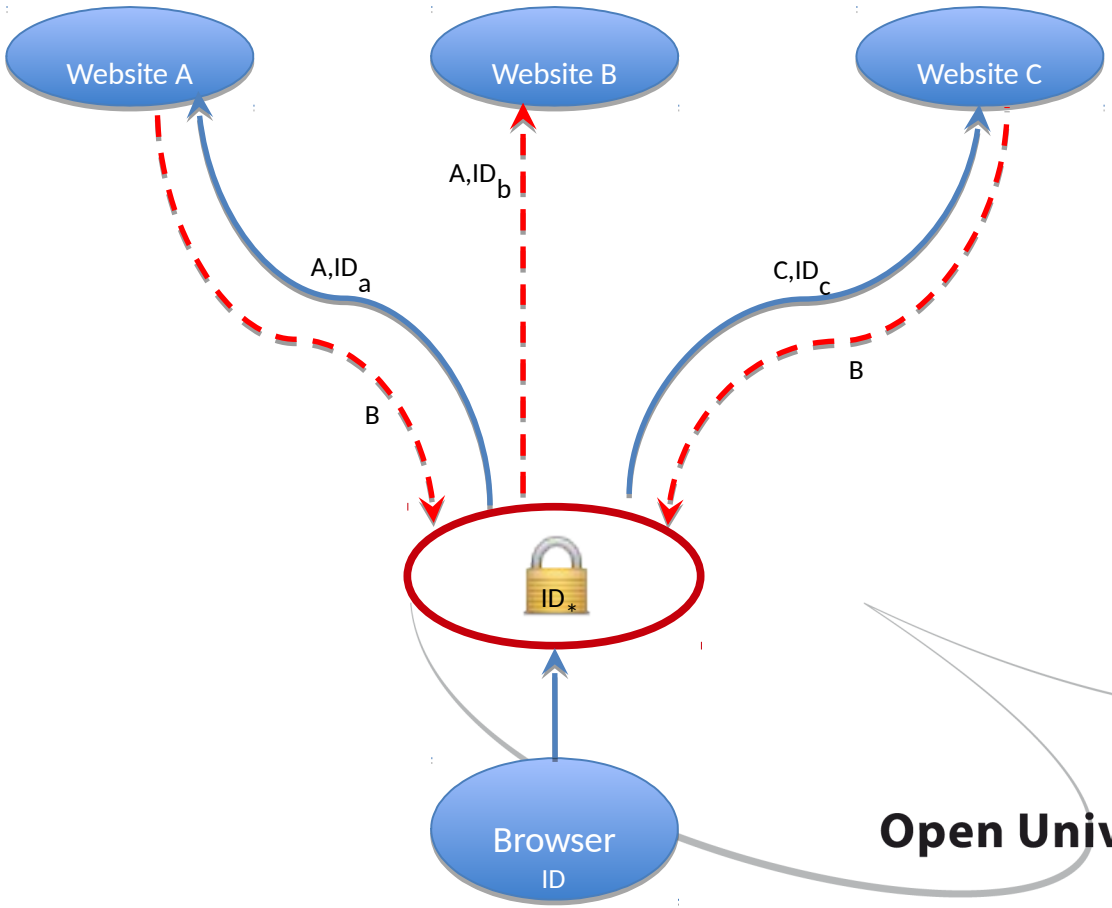
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



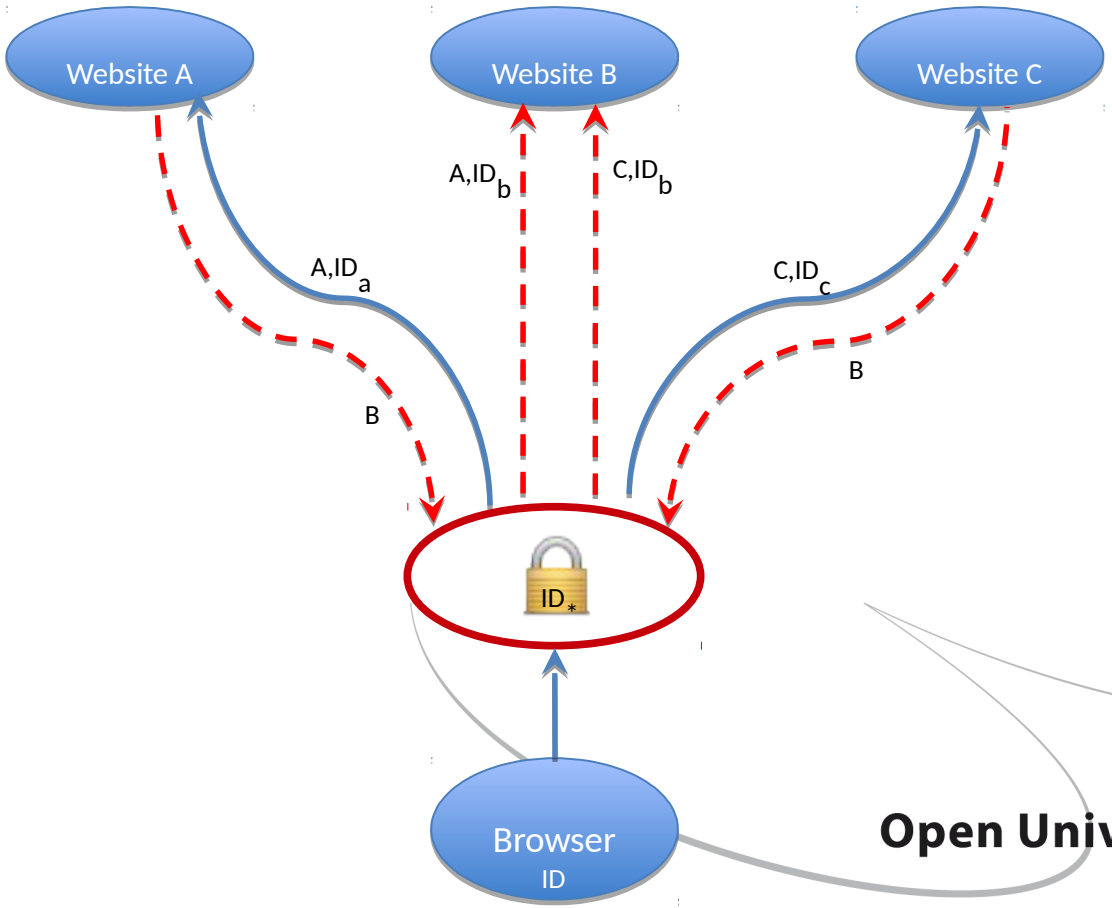
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



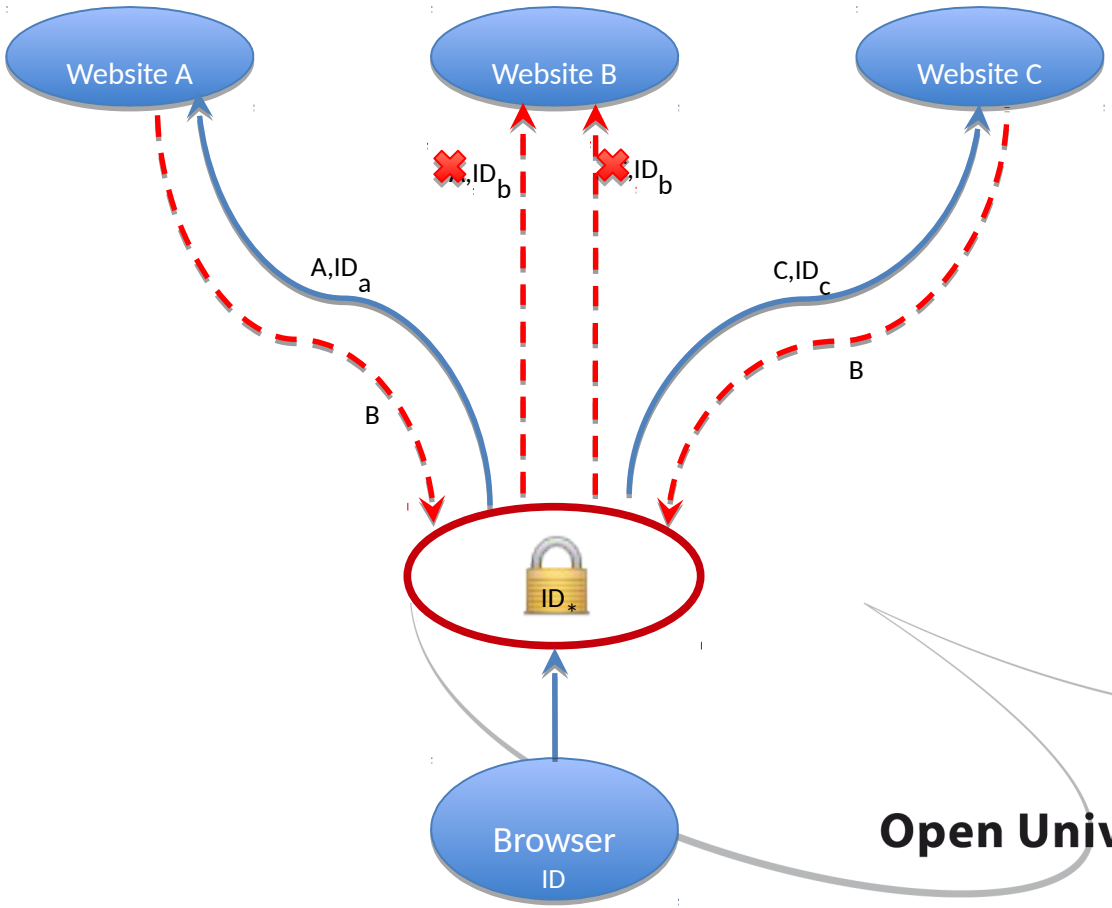
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



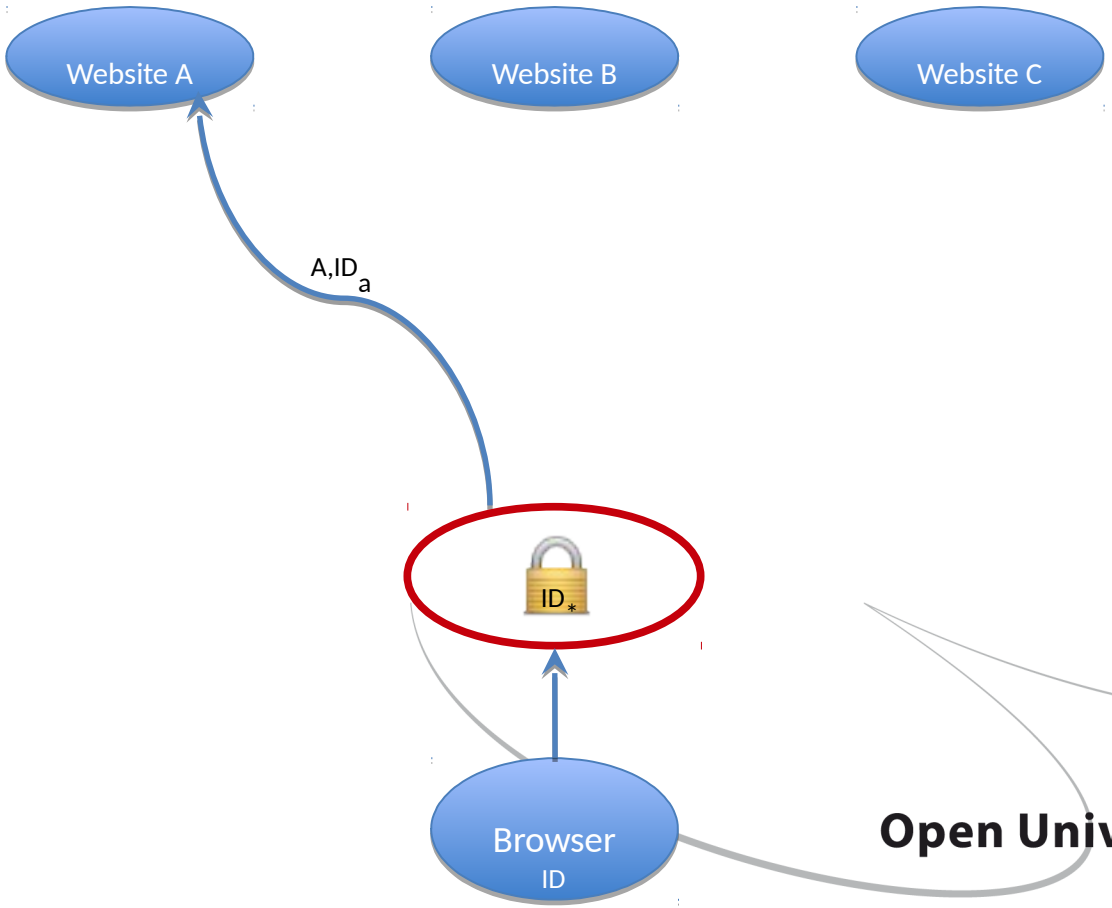
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



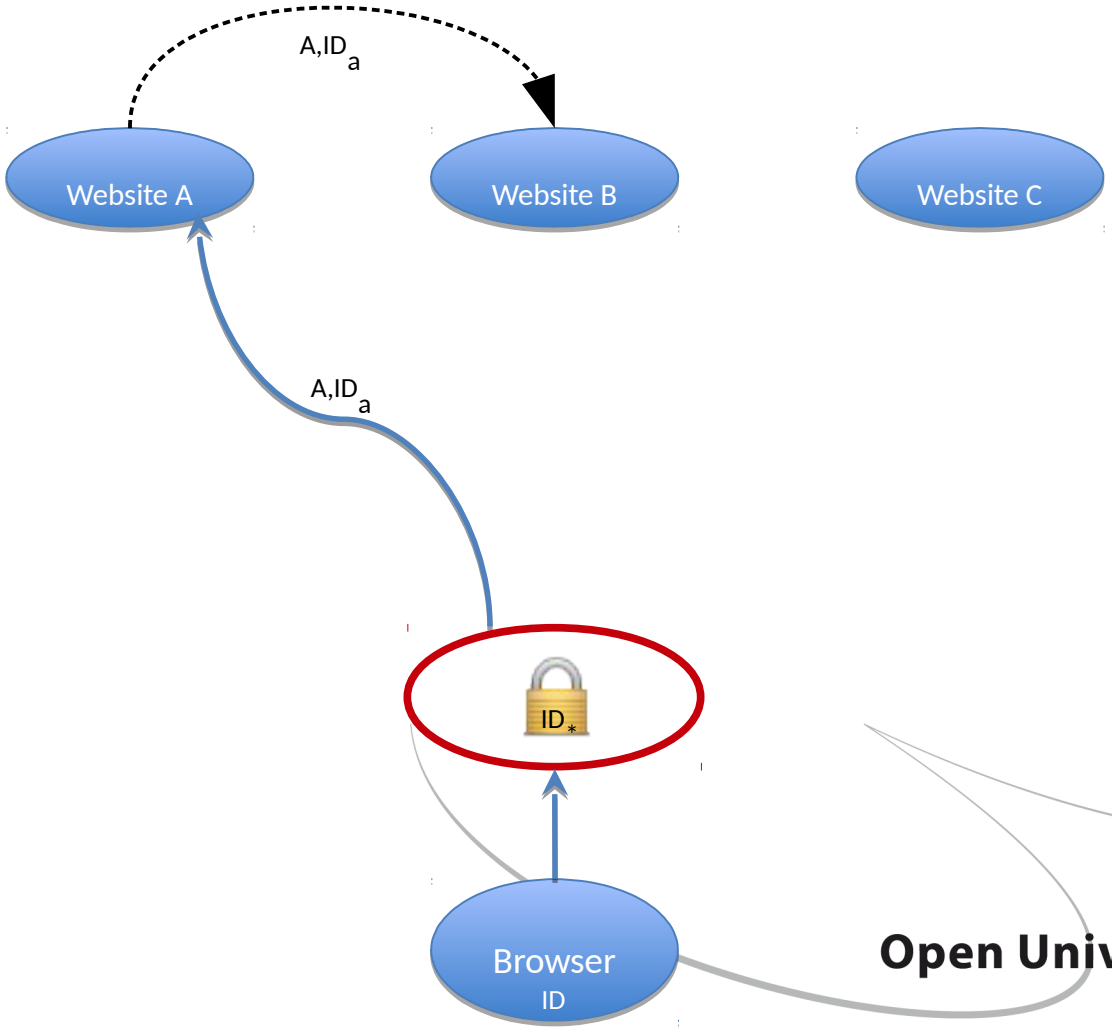
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



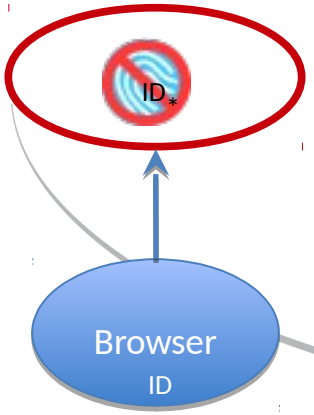
Open Universiteit
www.ou.nl

Option 1: constant fingerprint / site



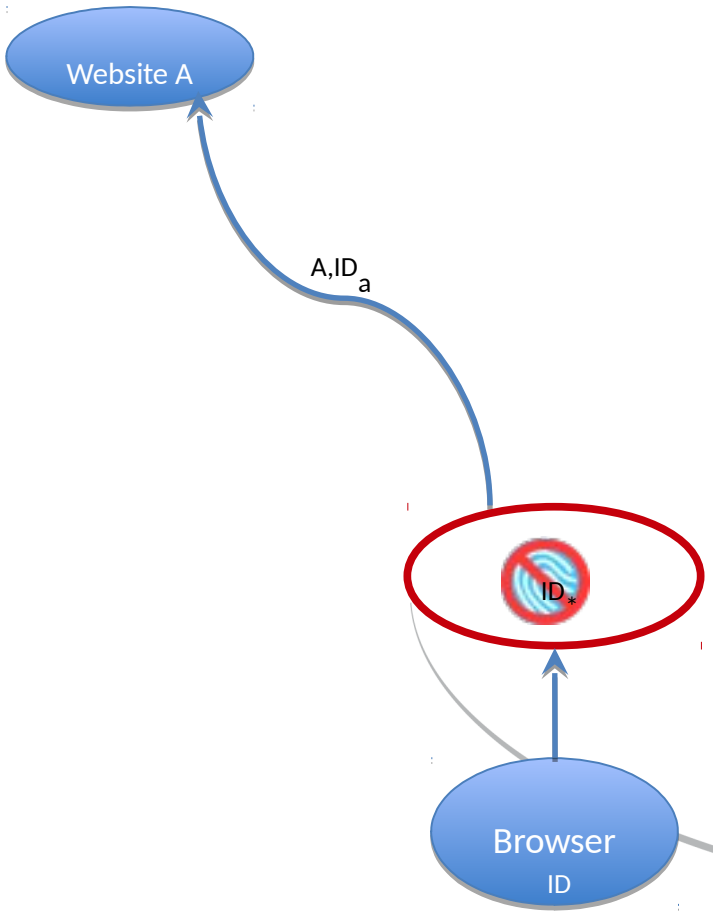
Open Universiteit
www.ou.nl

Option 2: separate web identities



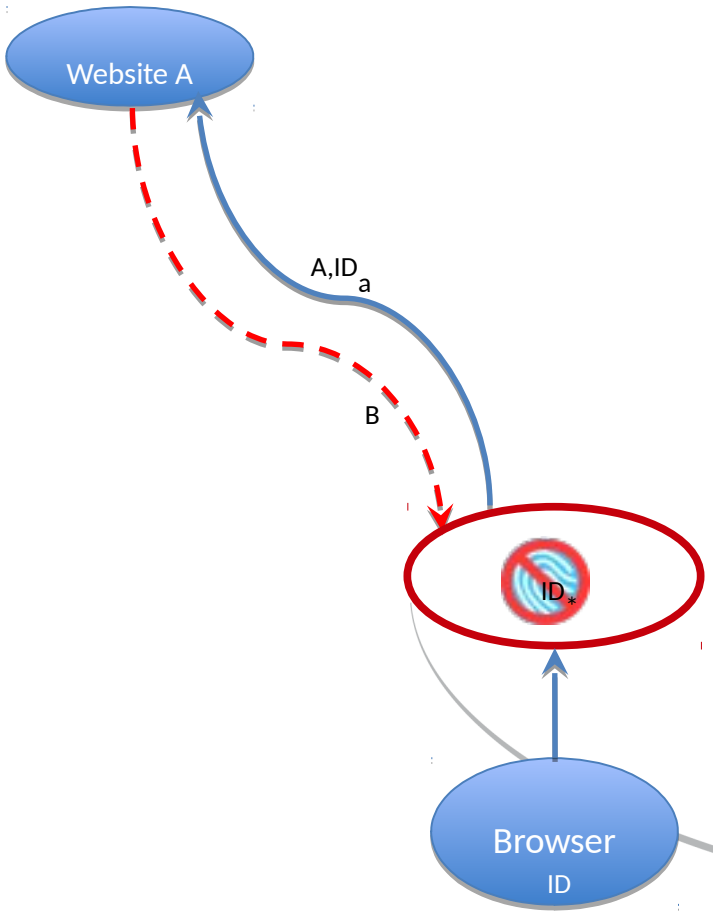
Open Universiteit
www.ou.nl

Option 2: separate web identities



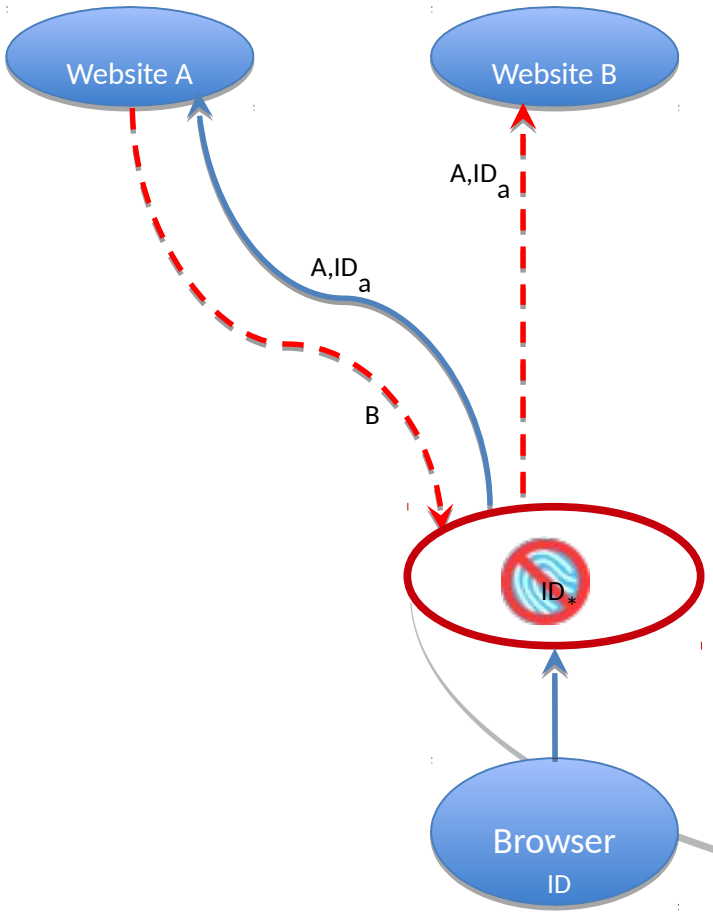
Open Universiteit
www.ou.nl

Option 2: separate web identities



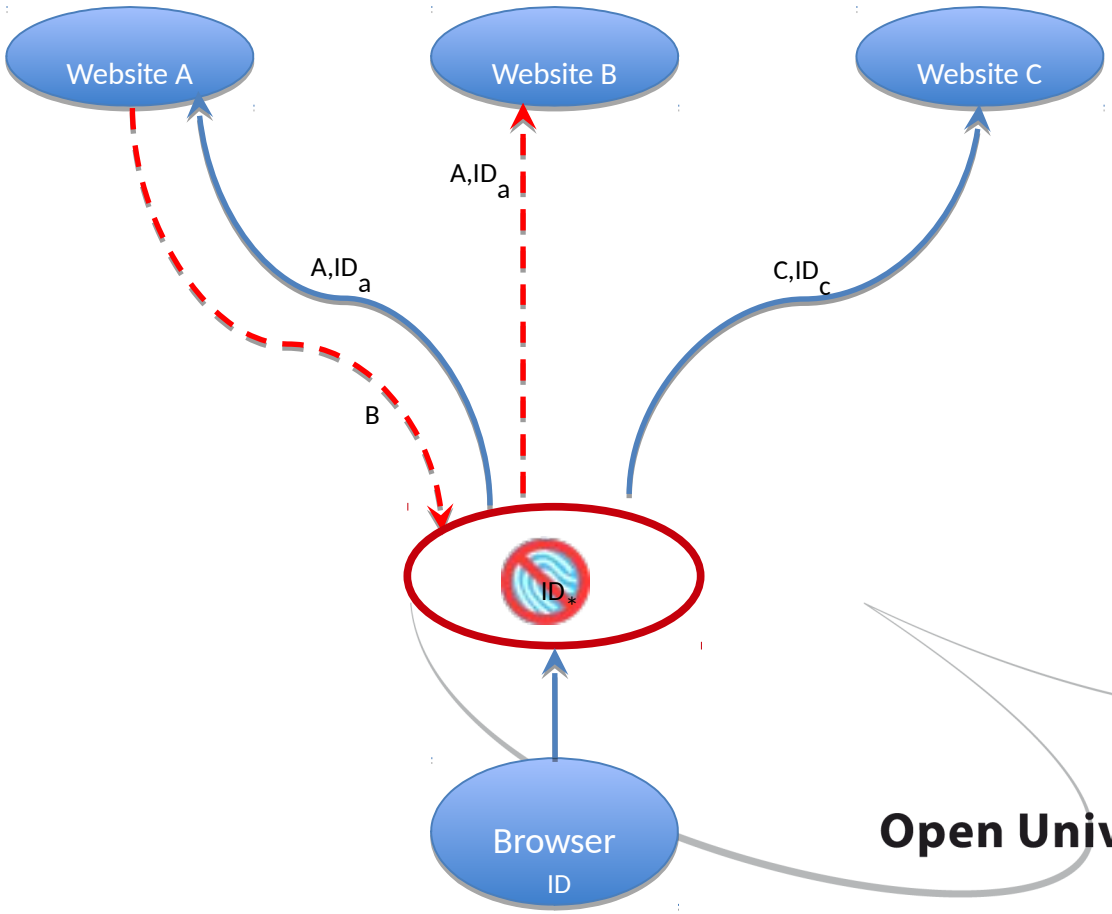
Open Universiteit
www.ou.nl

Option 2: separate web identities



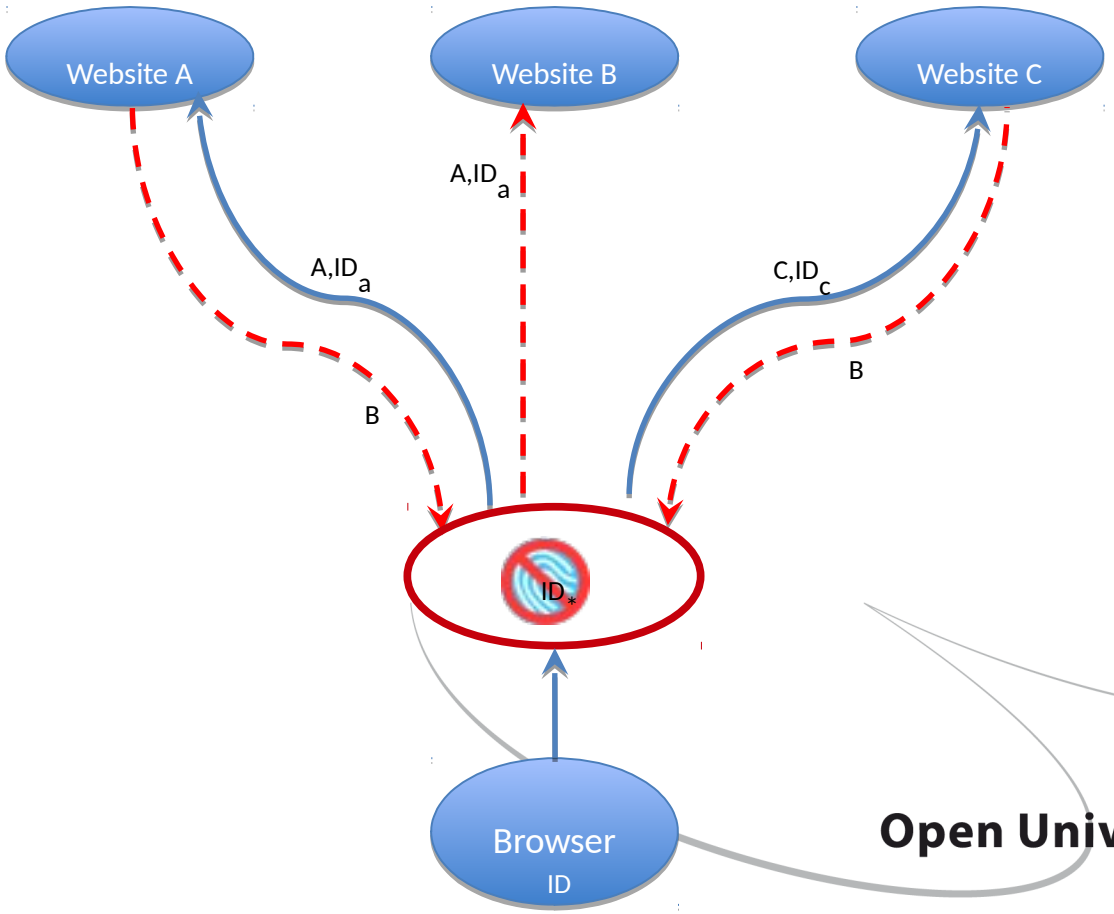
Open Universiteit
www.ou.nl

Option 2: separate web identities



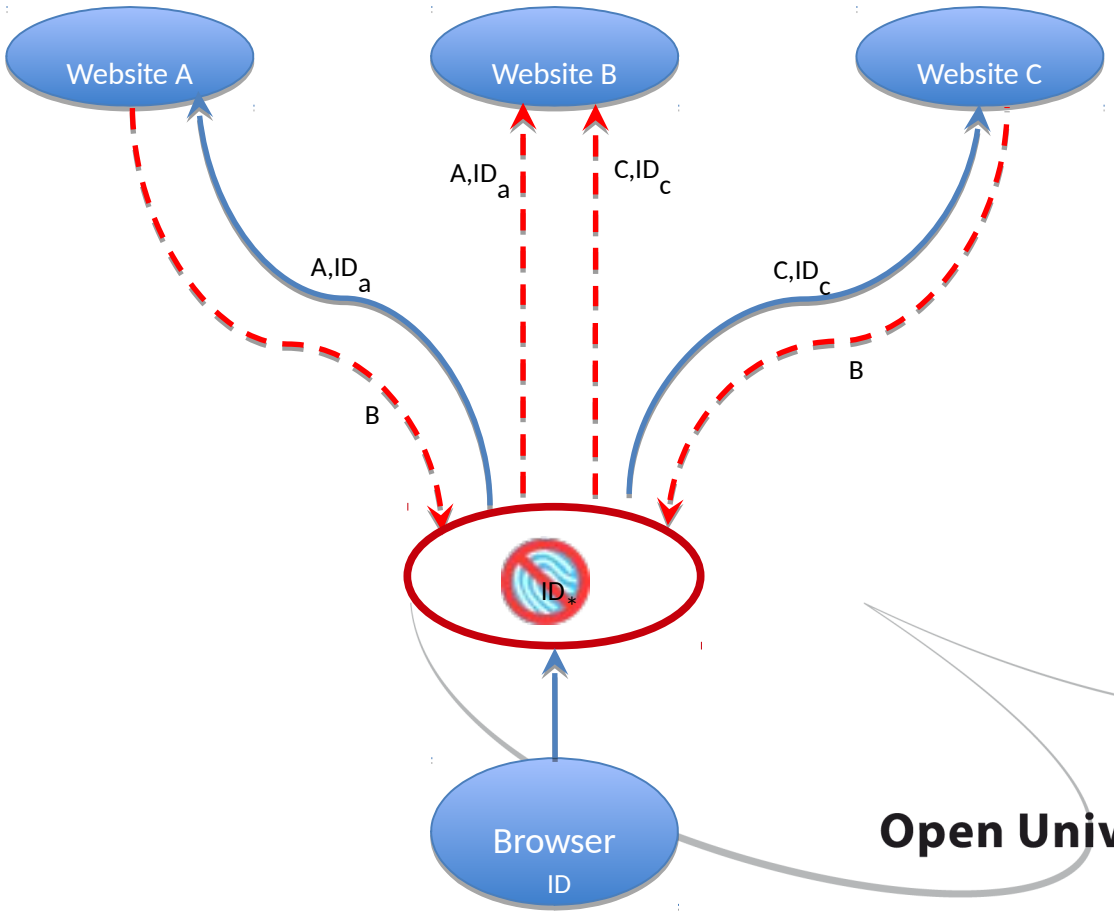
Open Universiteit
www.ou.nl

Option 2: separate web identities



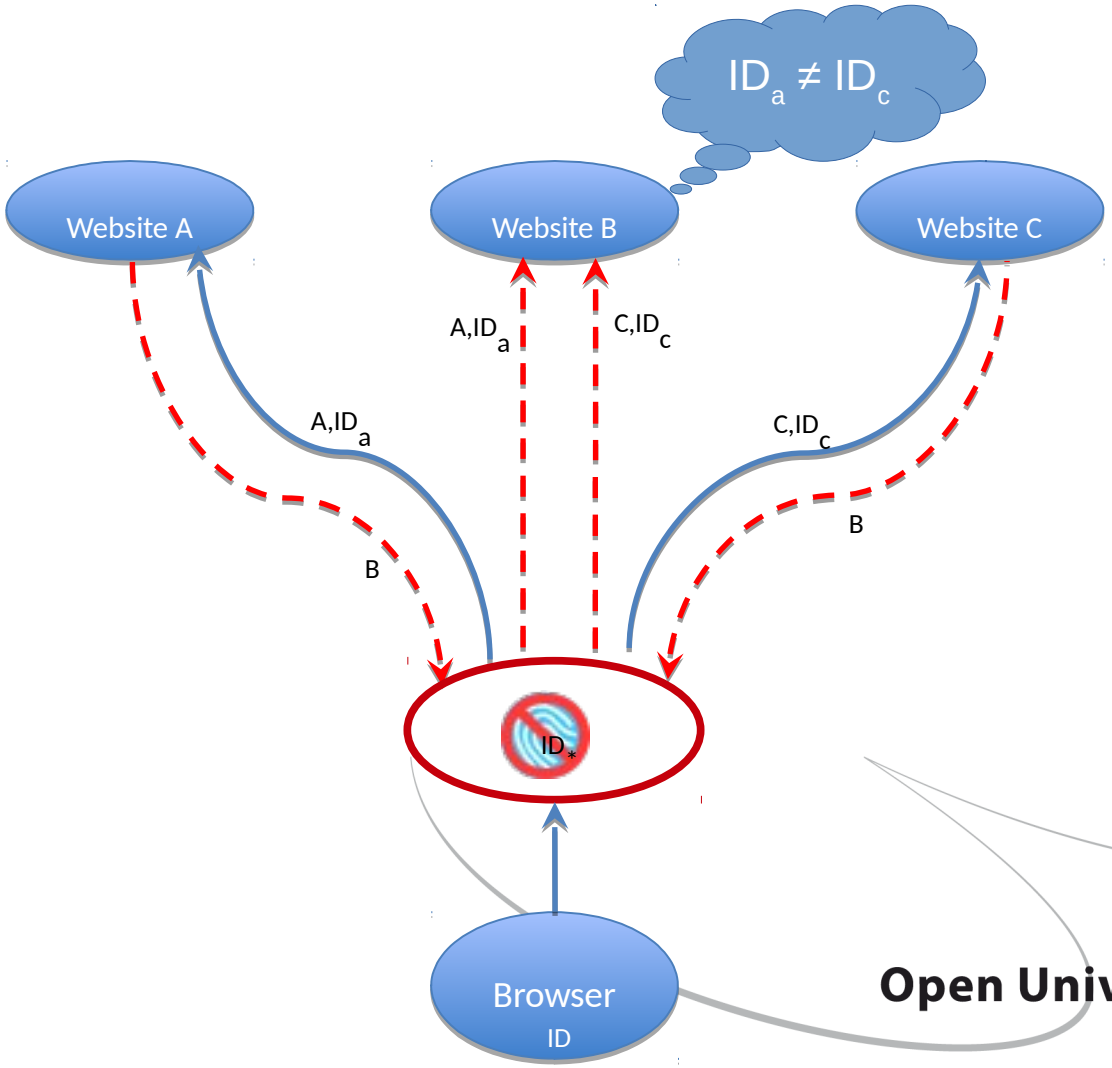
Open Universiteit
www.ou.nl

Option 2: separate web identities



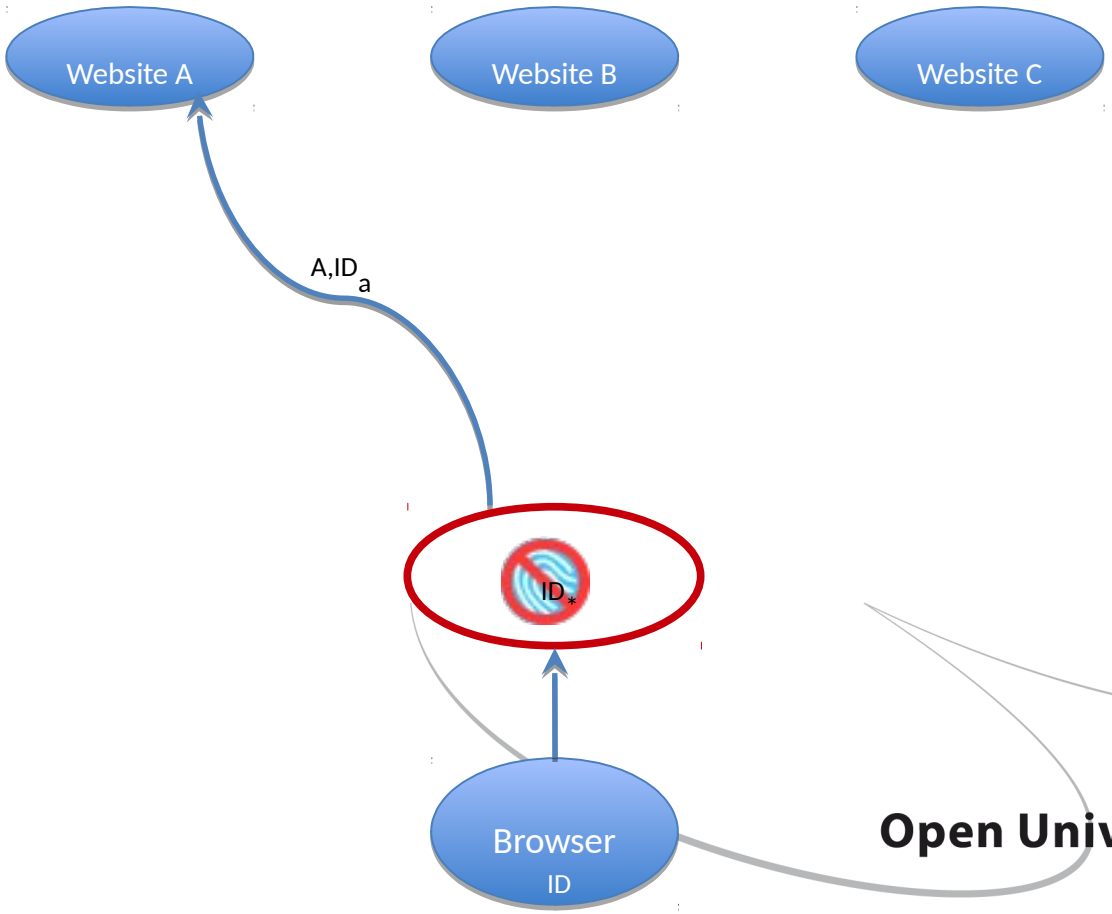
Open Universiteit
www.ou.nl

Option 2: separate web identities



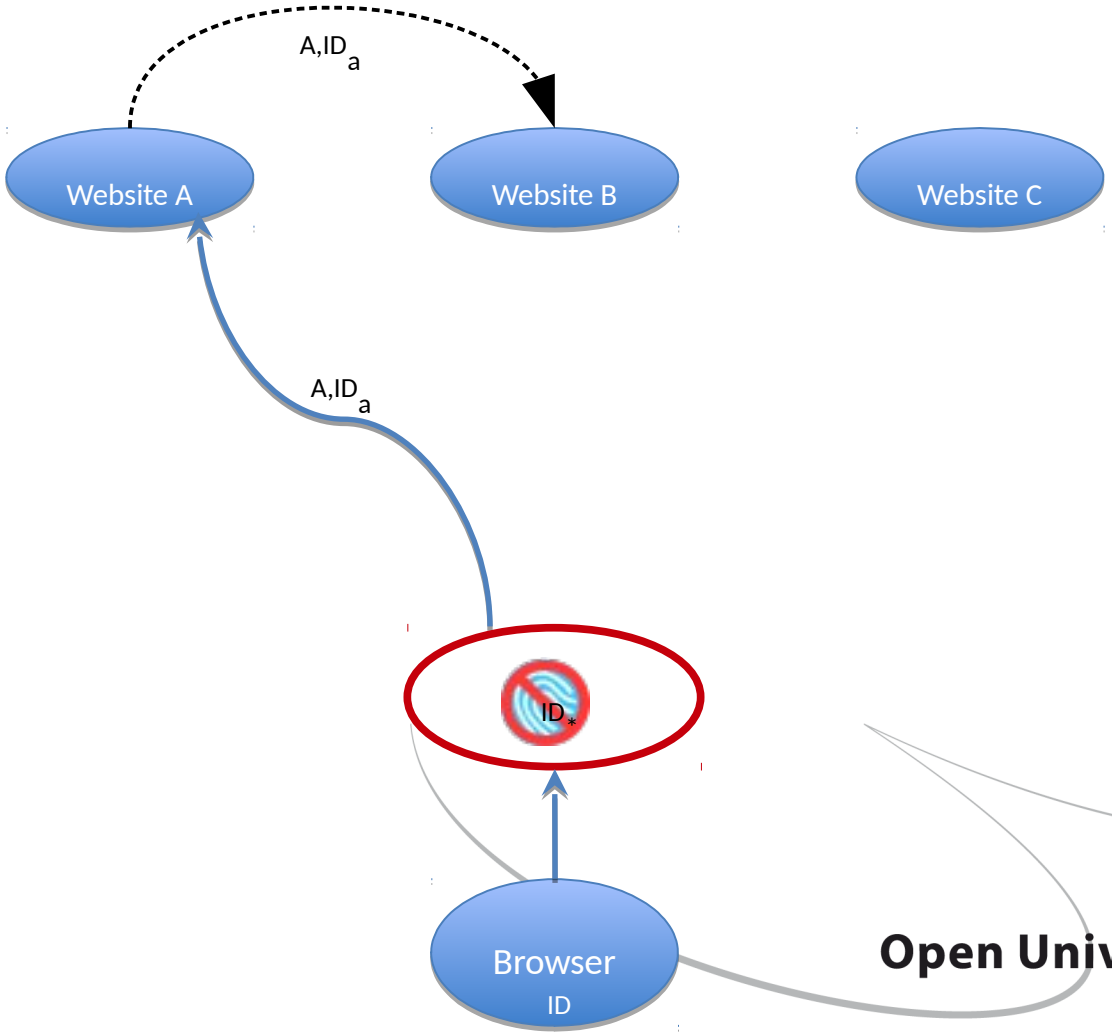
Open Universiteit
www.ou.nl

Option 2: separate web identities



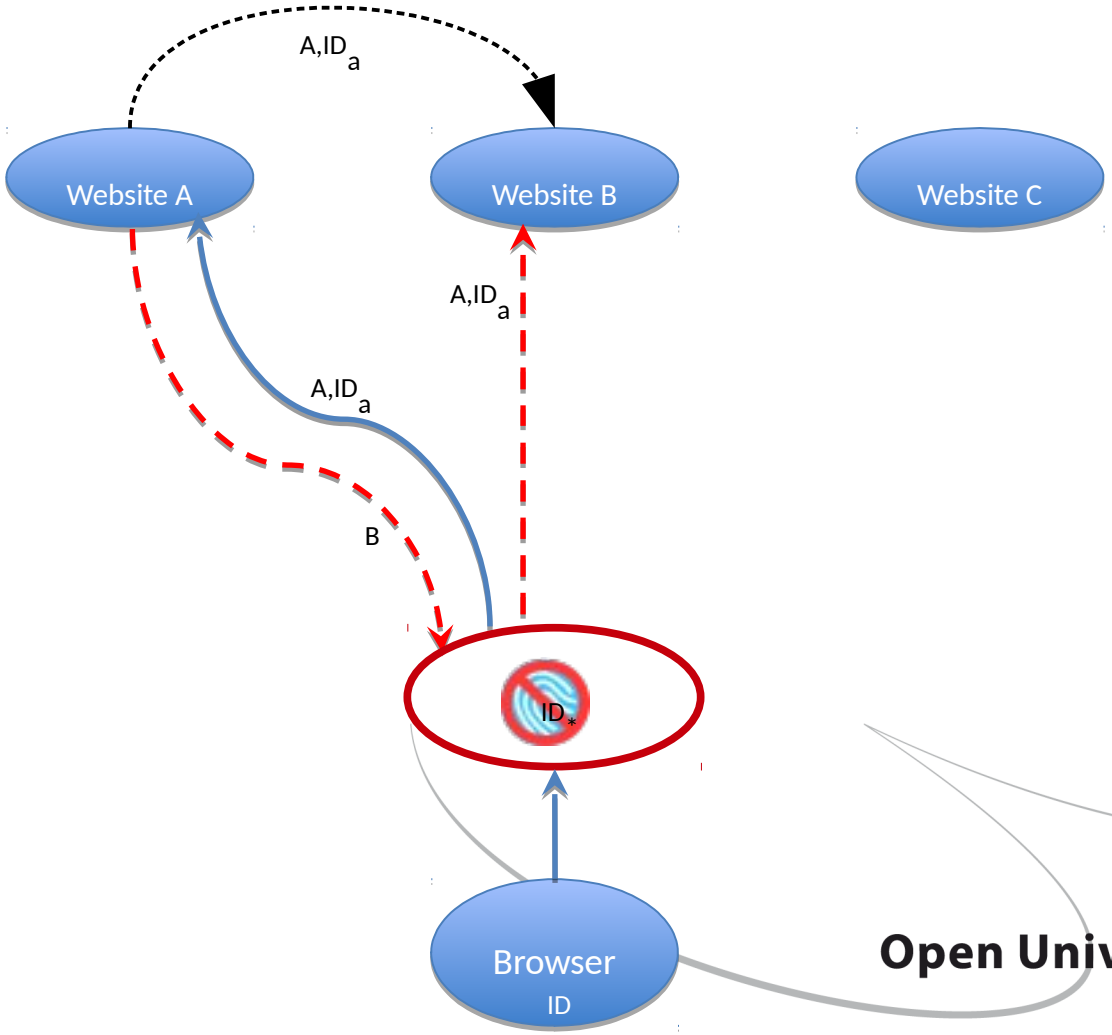
Open Universiteit
www.ou.nl

Option 2: separate web identities



Open Universiteit
www.ou.nl

Option 2: separate web identities



Open Universiteit
www.ou.nl

Determining the fingerprint surface

Theoretical argument:

If there is one computer used directly by everyone at the same time, then fingerprints might be indistinguishable.

Practice

- Different physical locations
- Different hardware
- Different software

complete coverage infeasible → determine fingerprint vectors

Fingerprinters

Non-profit:

- Panopticlick - academic study
- FingerPrintJS - open source

Commercial:

- AddThis - social media buttons
- BlueCava - advertisements
- Iovation - fraud prevention
- ThreatMetrix - fraud prevention

Open Universiteit
www.ou.nl

Fingerprint vectors

- √: this work
- √: [S&P13]
- –: [S&P13], but dropped

Attribute	Pan	BC	IO	TM	Add	FPjs
Plugin Enumeration	√	√	✓	√	✓	✓
Font Detection	√	√		√		
User-Agent	√	√	✓	√	✓	✓
HTTP Header Accept	√					
HTTP Header Accept-Charset	√					
HTTP Header Accept-Encoding	√					
HTTP Header Accept-Language	√					
Screen Resolution	√	√	√	√	✓	✓
Timezone	√	√	√	√	✓	✓
Browser Language		√	√	–	✓	✓
OS & Kernel Version		✓	✓	√	✓	✓
DOM Storage	√	✓	✓	✓	✓	✓
IE userData	√	✓				
Java Enabled	✓				✓	
DNT User Choice		–			✓	✓
Cookies Enabled	√		✓			
JS detect: Flash Enabled	√	√	√	√	✓	✓
ActiveX + CLSIDs	√	√		√	✓	✓
Date & Time		✓	√	✓	✓	
CPU		✓	✓		✓	✓
System/User Language		√	✓		✓	
OpenDatabase			✓		✓	✓
Canvas Fingerprinting					✓	✓
Mime-type Enumeration	√			√		
HTTP Proxy Detection			√	√		
IndexedDB					✓	✓
Math Constants		√			✓	
Windows Registry		√	√			
TCP/IP Parameters		√	√			
Google Gears Detection		√				
Flash Manufacturer				√		
MSIE Security Policy		√				
AJAX Implementation		√				
MSIE Product key			√			
Device Enumeration		√				
Device Identifiers			√			
IP address		√				
HTML Body Behavior						✓
Battery					✓	
WebGLRenderingContext					✓	

Proof-of-concept: FP-Block plugin

- Generates consistent fingerprint
- One fingerprint used per domain
- 23 attributes covered (Tor: 14, FireGloves: 8)
- Covers
  - HTTP (passive fingerprinting)
  - JavaScript (active fingerprinting)
- Additional coverage to ensure functionality
- Canvas fingerprint
  - detection [CCS14]
  - prevention (new)

Open Universiteit
www.ou.nl

Fingerprint coverage

Footnotes:

- Property can be checked passively, i.e., no client-side technology required.
- Property specific to Internet Explorer.
- Property is determined using a Windows DLL created by the fingerprinting company.
- Out of scope – FP-Block only targets HTTP and Javascript layers.
- Blocking or spoofing this attribute would break or limit important functionality.

Attribute	FG	Tor	PV	RAS	**FPB**
Plugin Enumeration	✓	✓	✓		✓
Font Detection	✓	✓	✓	✓	✓
User-Agent	✓	✓		✓	✓
HTTP Header Accept					
HTTP Header Accept-Charset		✓			
HTTP Header Accept-Encoding				✓	✓
HTTP Header Accept-Language		✓		✓	✓
Screen Resolution	✓	✓		✓	✓
Timezone	✓	✓		✓	✓
Browser Language	✓				✓
OS & Kernel Version	✓	✓		✓	✓
DOM Storage				✓	✓
IE userData					
Java Enabled					✓
DNT User Choice				✓	✓
Cookies Enabled					✓
JS detect: Flash Enabled					✓
ActiveX + CLSIDs					
Date & Time					
CPU				✓	✓
System/User Language					✓
OpenDatabase					✓
Canvas Fingerprinting		✓		✓	✓
Mime-type Enumeration	✓	✓	✓		✓
HTTP Proxy Detection					
IndexedDB					✓
Math Constants					
Windows Registry					
TCP/IP Parameters		✓			
Google Gears Detection					
Flash Manufacturer					
MSIE Security Policy					
AJAX Implementation					
MSIE Product key					
Device Enumeration					
Device Identifiers					
IP address		✓			
HTML Body Behavior					
Battery		✓			✓
WebGLRenderingContext		✓		✓	✓

Validation

- Controlled test setup
  - 2 domains
  - On each: page embedding file from other domain
  - Generate fingerprint with fingerprintJS

- Real-life test setup
  - BC, IO, TM, fingerprintJS, Panopticlick, AddThis

- Additional test: BlueCava ID request

Monitoring evolution of fingerprinters

Updates since September 2014:

- Panopticlick –
- **BlueCava** –
- **AddThis** –
- **Iovation** **complex**
- FingerPrintJS added screen orientation
- **ThreatMetrix** **major changes since 27 oct '14**

Open Universiteit
www.ou.nl

Conclusions

- Ubiquitous tracking is a reality
- Countermeasures fall short
- Local tracking is acceptable
  → overcomes defensive paradox

Results:

- Propose separation of web identities
- Determine fingerprint vectors
- Proof-of-concept implementation
- Validation against commercial fingerprinters

Thank you for your attention!

Open Universiteit
www.ou.nl

References (1)

[PETS10] P. Eckersley. **How unique is your web browser?** In *Proc. 10Th Privacy Enhancing Technologies Symposium (PETS'10)*, LNCS 6205, pp. 1-18. Springer, 2010.

[CCS13] G. Acar, M. Juarez, N. Nikiforakis, C. Diaz, S. Gürses, F. Piessens, B. Preneel. **FPDetective: dusting the web for fingerprinters**. In *Proc. 20Th Conference on Computer & Communications Security (CCS'13),* pp. 1129-1140. ACM.

[W2SP11] K. Mowery, D. Bogenreif, S. Yilek, H. Shacham. **Fingerprinting information in JavaScript implementations**. In *Proc. 2nd Web 2.0 Security and Privacy (W2SP'11)*.

[W2SP12] K. Mowery, H. Shacham. **Pixel Perfect: Fingerprinting Canvas in HTML5**. In *Proc. 3rd Web 2.0 Security and Privacy (W2SP'12)*.

[W2SP13] M. Mulazzani, P. Reschl, M. Huber, M. Leithner, S. Schrittwieser, E. Weippl. **Fast and reliable browser identification with Javascript engine fingerprinting**. In *Proc. 3rd Web 2.0 Security and Privacy (W2SP'13)*.

References (2)

[Roos11] A. Roosendaal. **Facebook Tracks and Traces Everyone: Like This!**. Tilburg Law School Research Paper No. 03/2011.

[S&P13] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens,G. Vigna. **Cookieless monster: Exploring the ecosystem of web-based device fingerprinting.** In *Proc. 34th Symposium on Security and Privacy (SP'13)*, pp. 541-555. IEEE, 2013.

[NordSec11] K. Boda, Á.M. Földes, G.Gy. Gulyás, S. Imre. **User Tracking on the Web via Cross-Browser Fingerprinting.** In *Proc. 16th Nordic Conference in Secure IT Systems (Nordsec 2011)*, Springer-Verlag, LNCS 7161, pp. 31-46, 2012.

[NSDI12] F. Roesner, T. Kohno, D. Wetherall. **Detecting and defending against third-party tracking on the web**. In *Proc. 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI'12)*, pages 155–168. USENIX, 2012.

Open Universiteit
www.ou.nl