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

Open Universiteit

www.ou.nl

First

Privacy does not need to be motivated.

Invasion of privacy needs to be motivated.

What this presentation is about

What this presentation is about

BBC

DIE ZEIT

NU.nl

Le Monde

EL PAÍS

What this presentation is about

What this presentation is about

What this presentation is about

Contributions

- Distinguish between local and cross-domain tracking
- Fingerprint privacy via separating web identities
- Proof-of-concept implementation
  - v1.0: http://esorics2015.sba-research.org/
  - Latest: https://github.com/ChristofTorres/FP-Block
- Determined common fingerprint vectors

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%

Embedded content

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

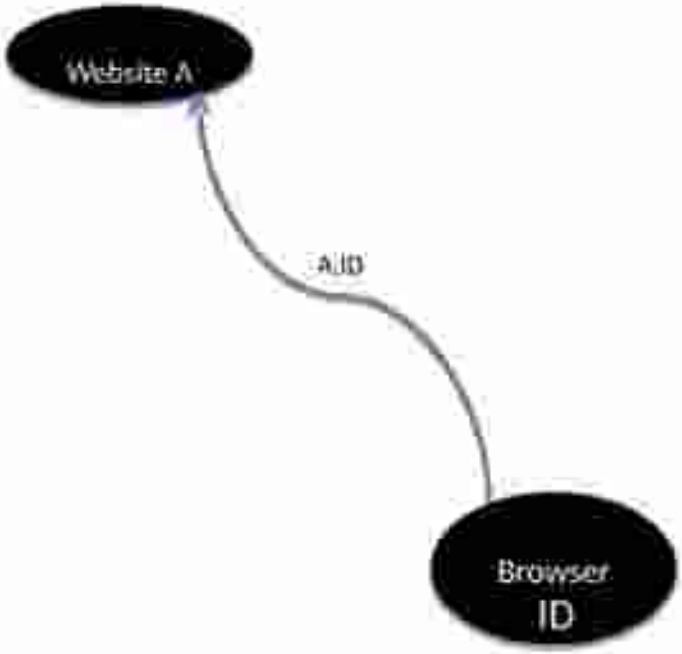
Embedded content

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

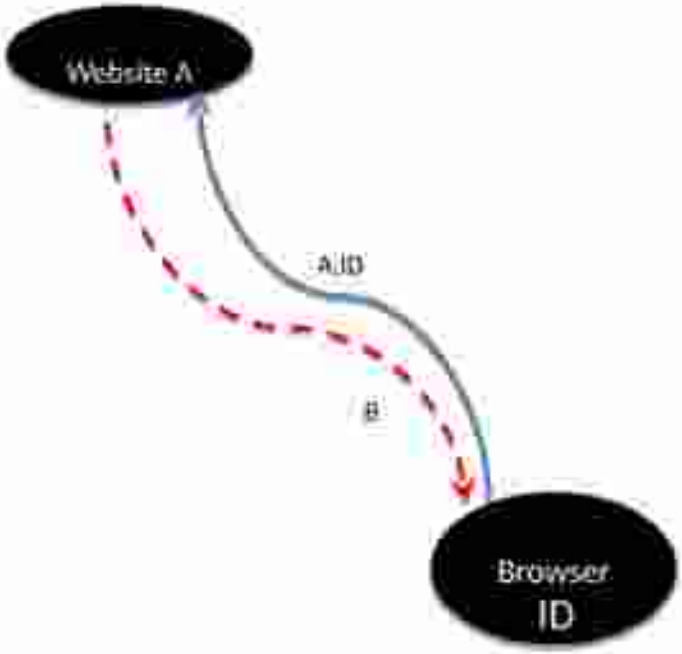
	Top 10k	Top 1mil
1. Akamai	17%	11%
2. Doubleclick	10%	20%
3. Google Analytics	19%	44%
4. YouTube	26%	47%
5. Facebook Like*	20%	16%
6. PayPal button	33%	44%
7. JQuery	18%	20%

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

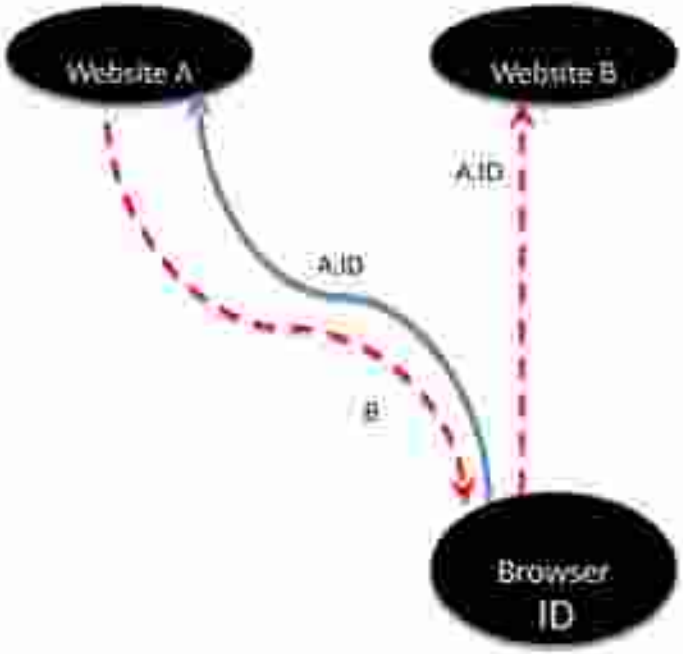
Tracking via embedded content



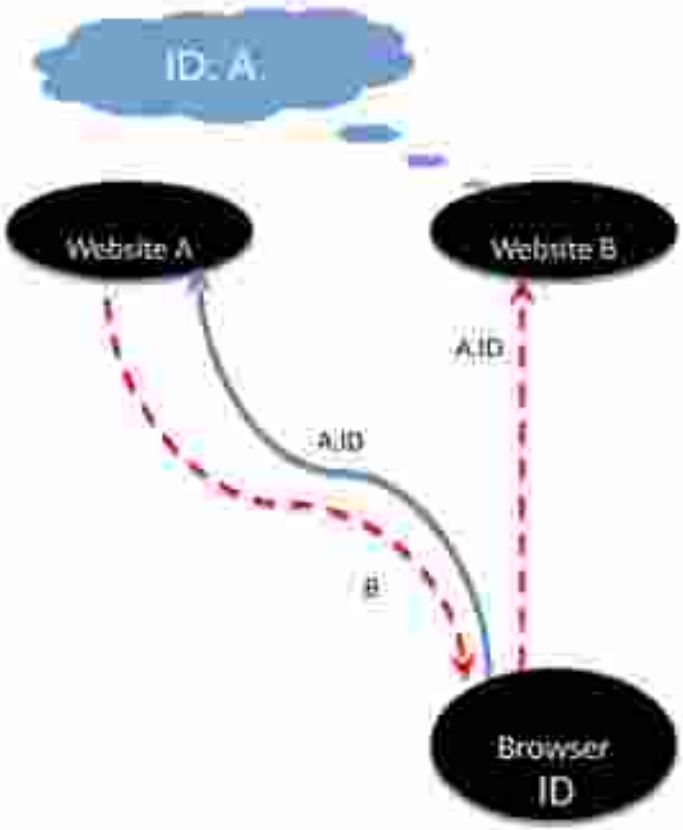
Tracking via embedded content



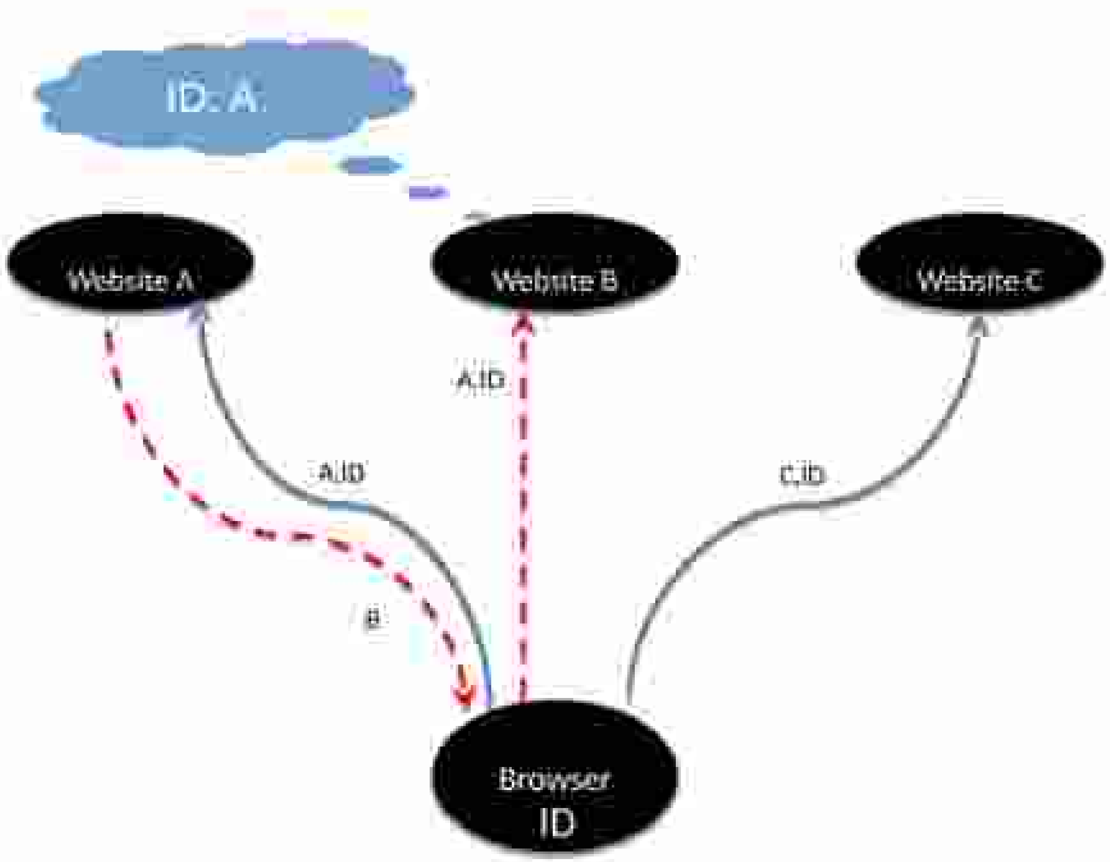
Tracking via embedded content



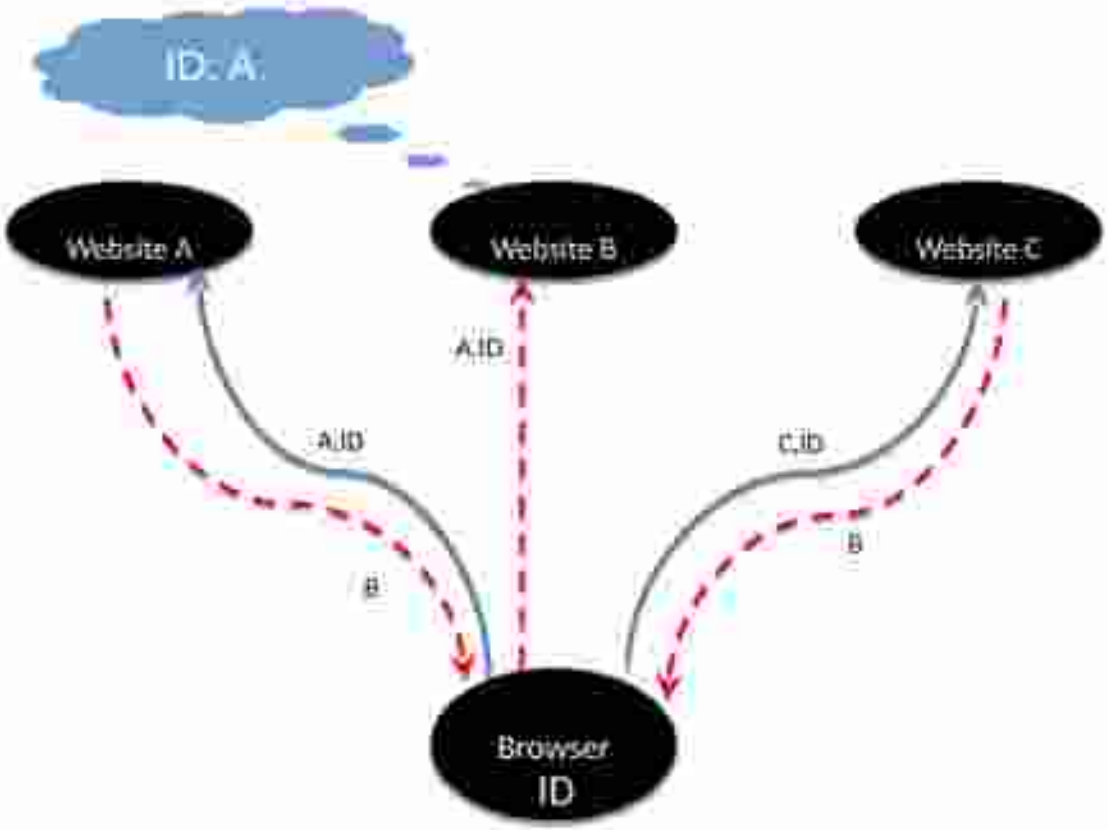
Tracking via embedded content



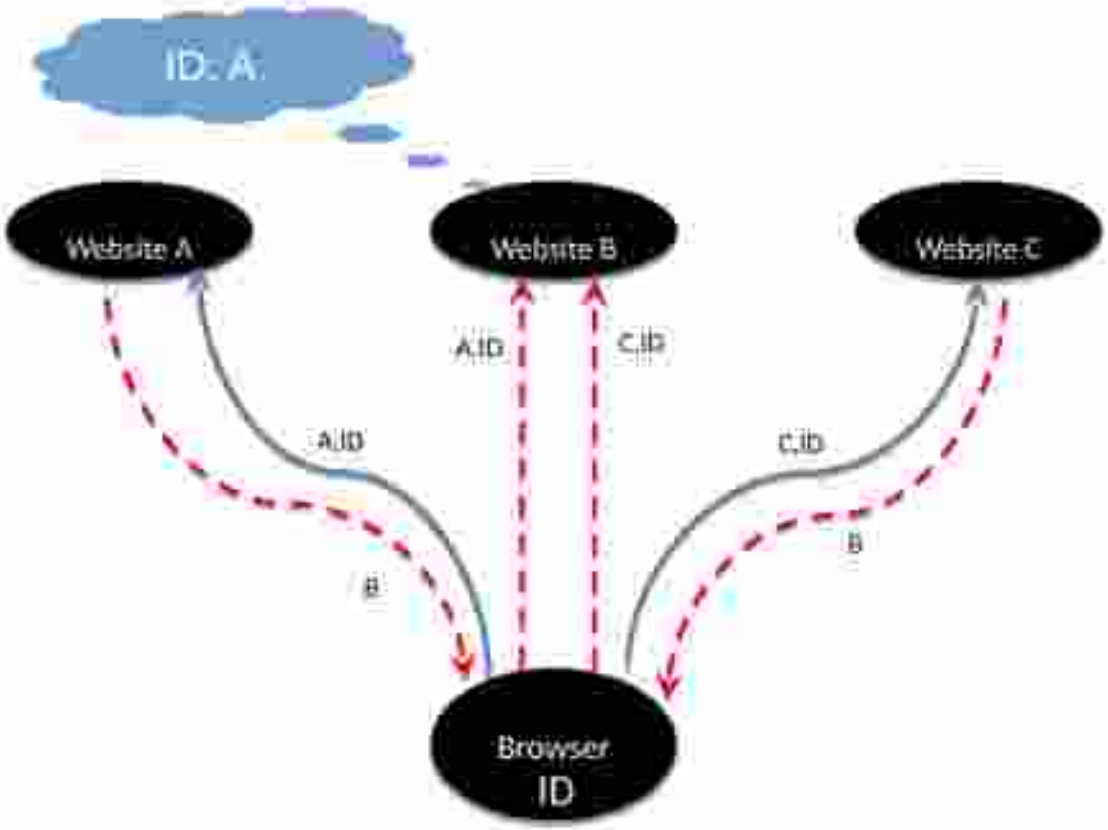
Tracking via embedded content



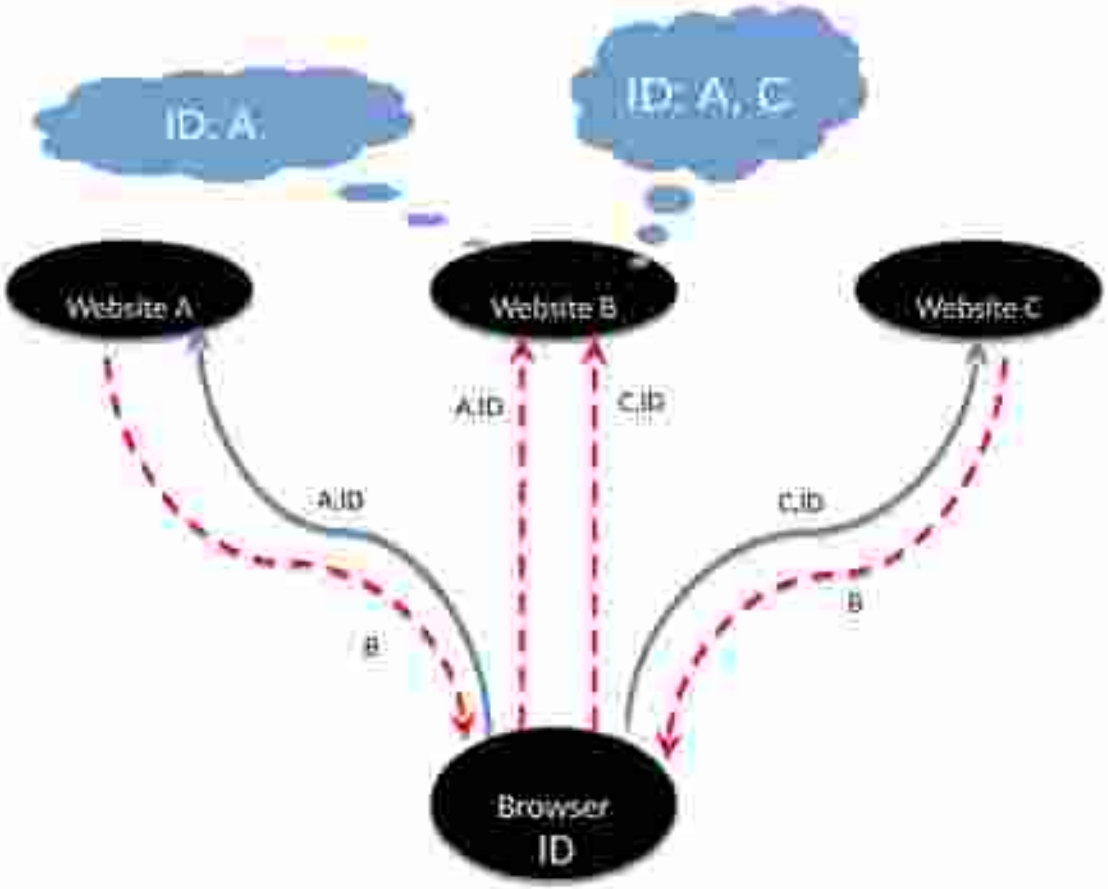
Tracking via embedded content



Tracking via embedded content



Tracking via embedded content



Tracking: fingerprint or cookies?

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

Tracking: fingerprint or cookies?

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

- Effective?
  - [PETS10]: 90% desktop browsers is unique.
- Actually in use?
  - [S&P13, CCS13]: some, but not much... yet.

Tracking: fingerprint or cookies?

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

- Effective?
  - [PETS10]: 90% desktop browsers is unique.
- Actually in use?
  - [S&P13, CCS13]: some, but not much... yet.
  - **Firefox 42 Beta will lead to increase.**

Fighting fingerprinting

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

- FireGloves [NordSec11]? [CCS13]: **X**
- Tor Browser? [CCS13]: **X**

Any countermeasure can be broken if specifically targetted.

Fighting fingerprinting

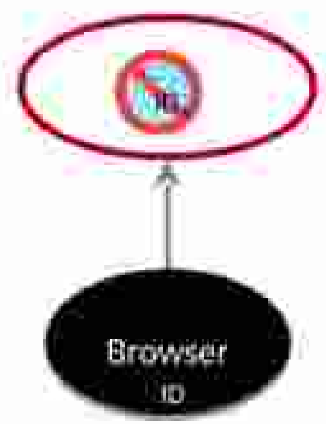
- Do Not Track header? [NSDI12]: **X**
- Blacklisting fingerprinters? [W2SP11]: **X**

- FireGloves [NordSec11]? [CCS13]: **X**
- Tor Browser? [CCS13]: **X**

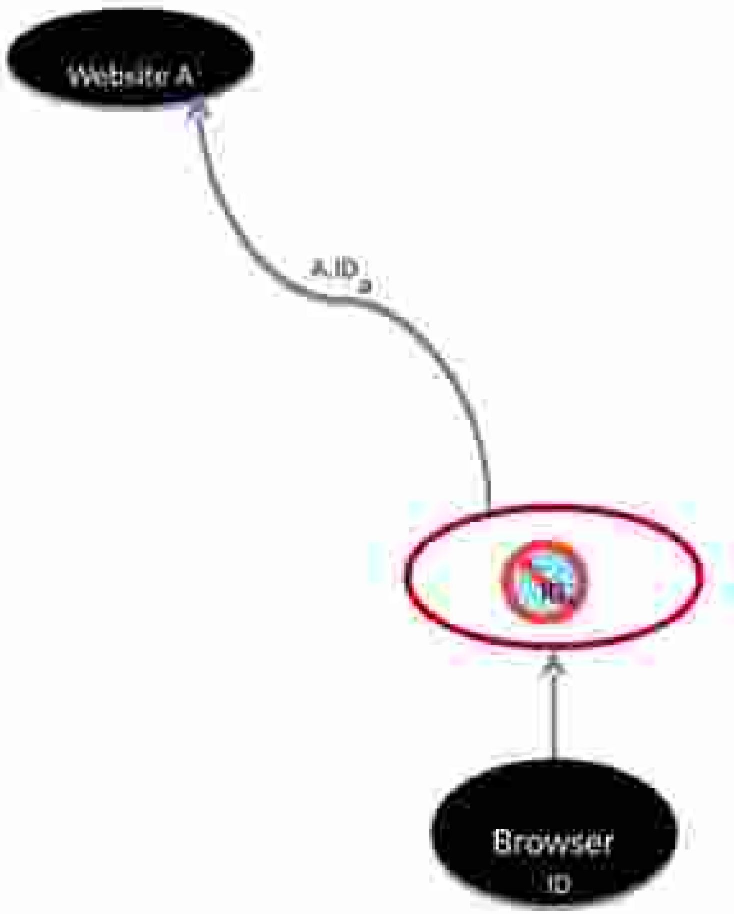
Any countermeasure can be broken if specifically targetted.

Idea:
- local tracking okay,
- 3rd party tracking not

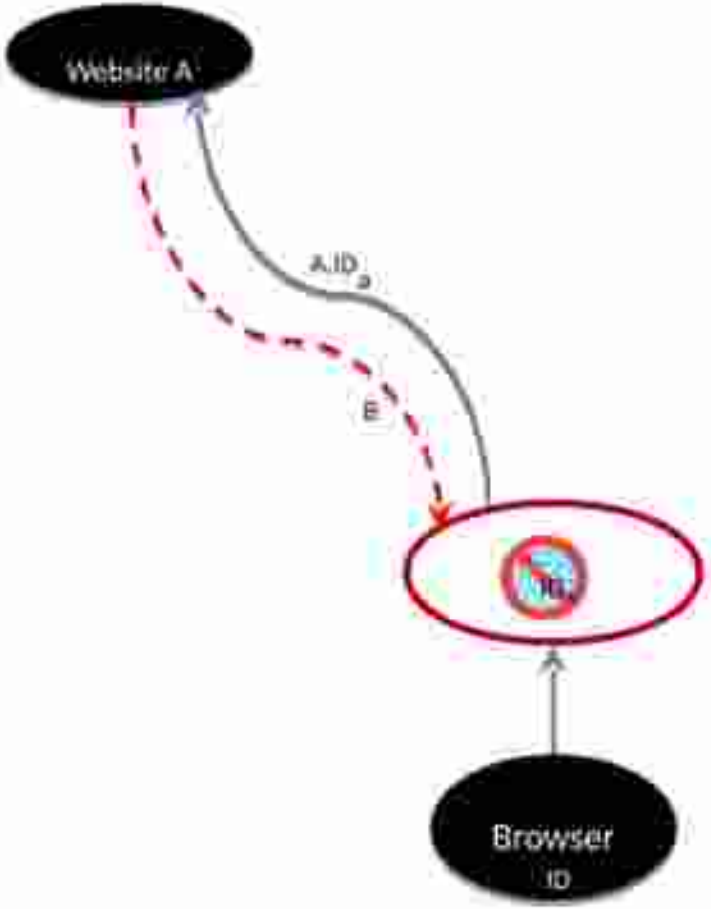
Separate web identities



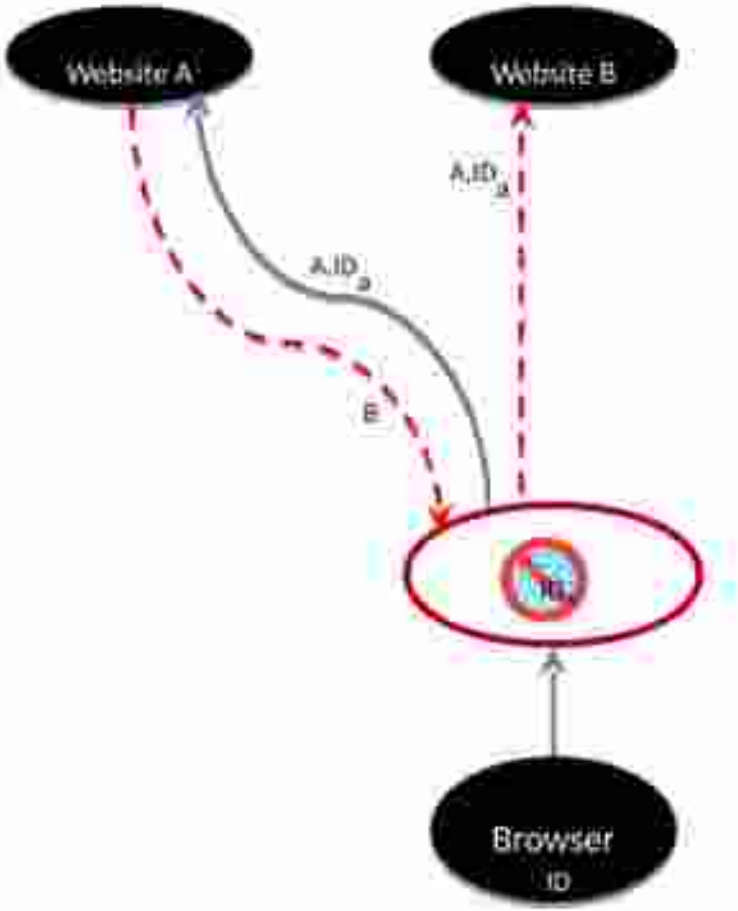
Separate web identities



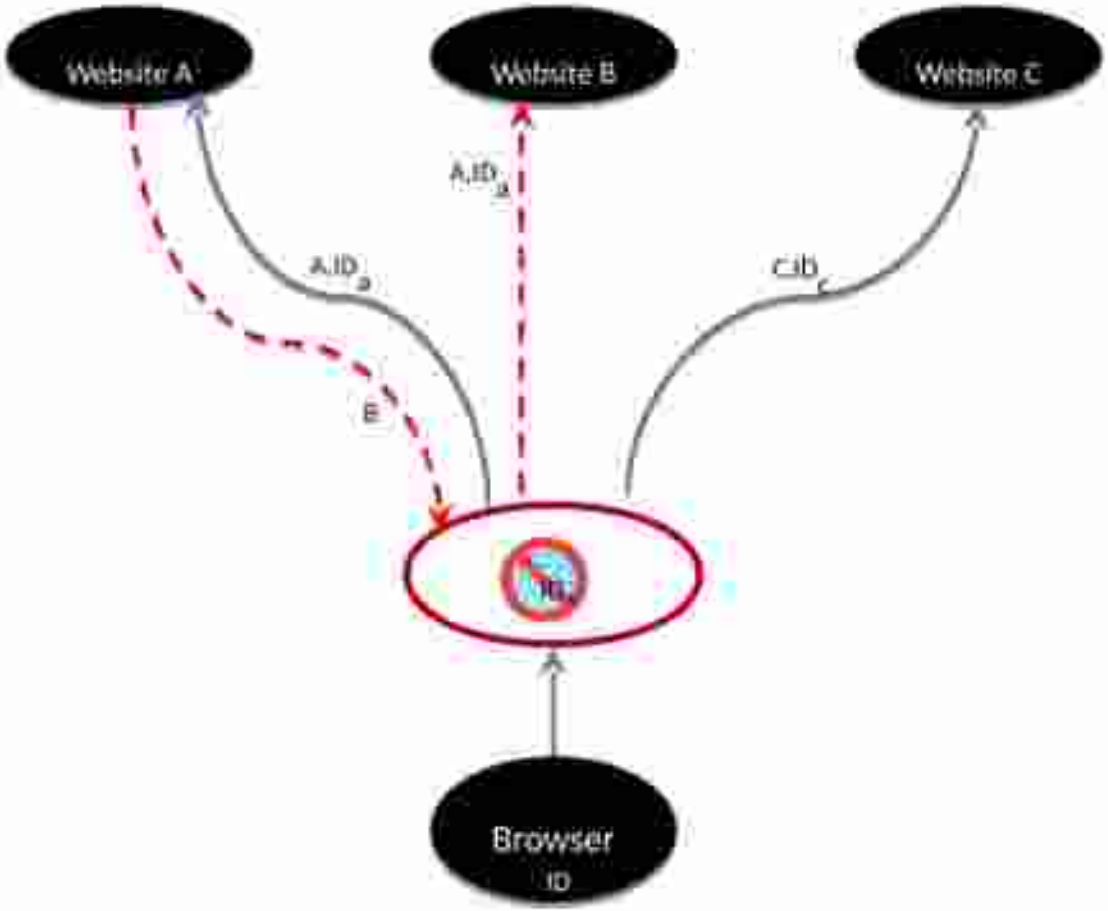
Separate web identities



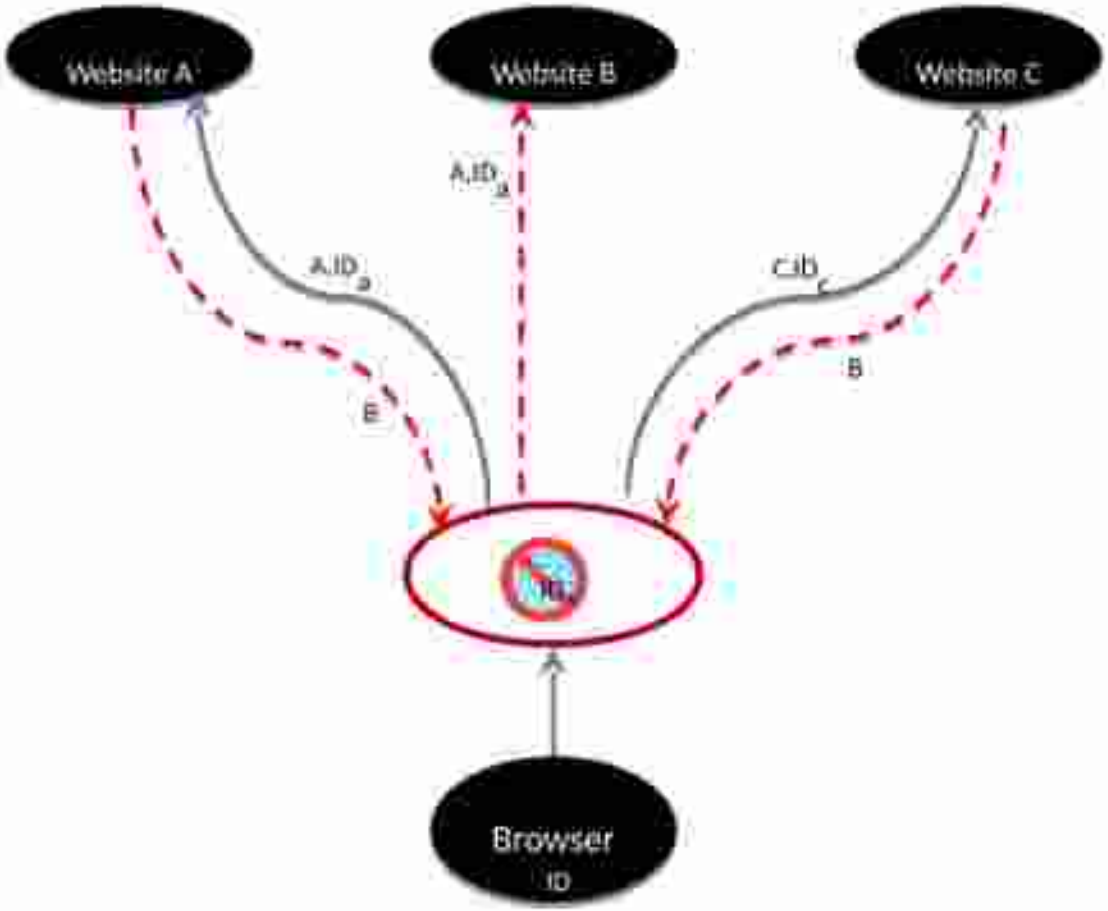
Separate web identities



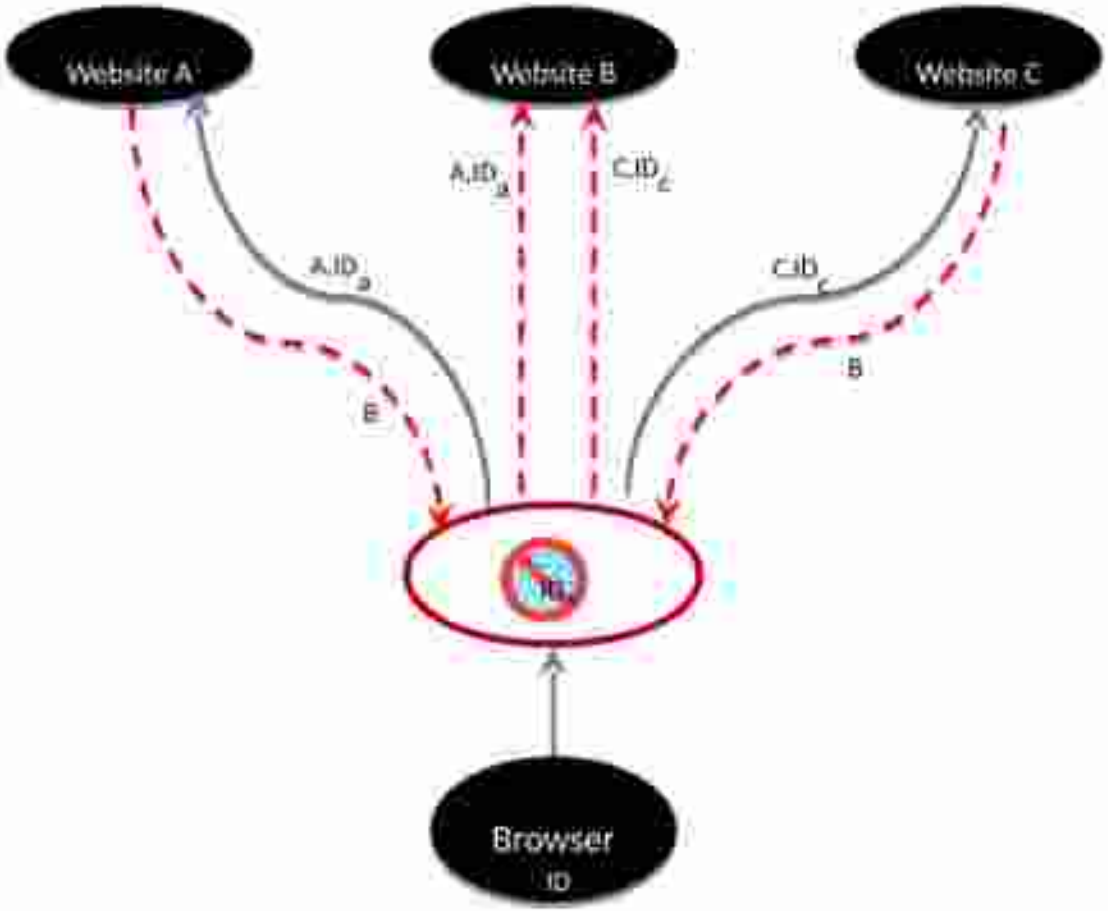
Separate web identities



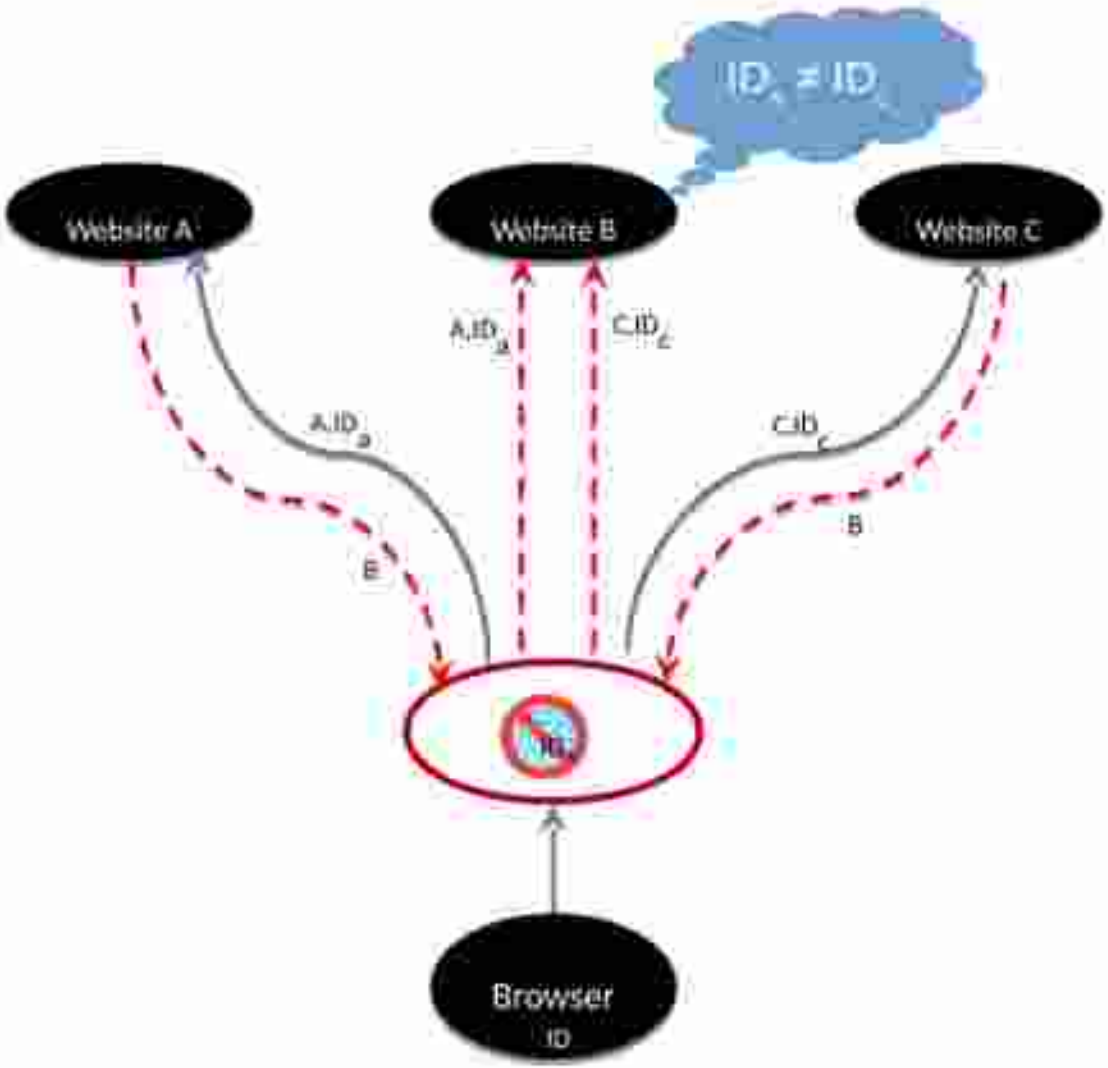
Separate web identities



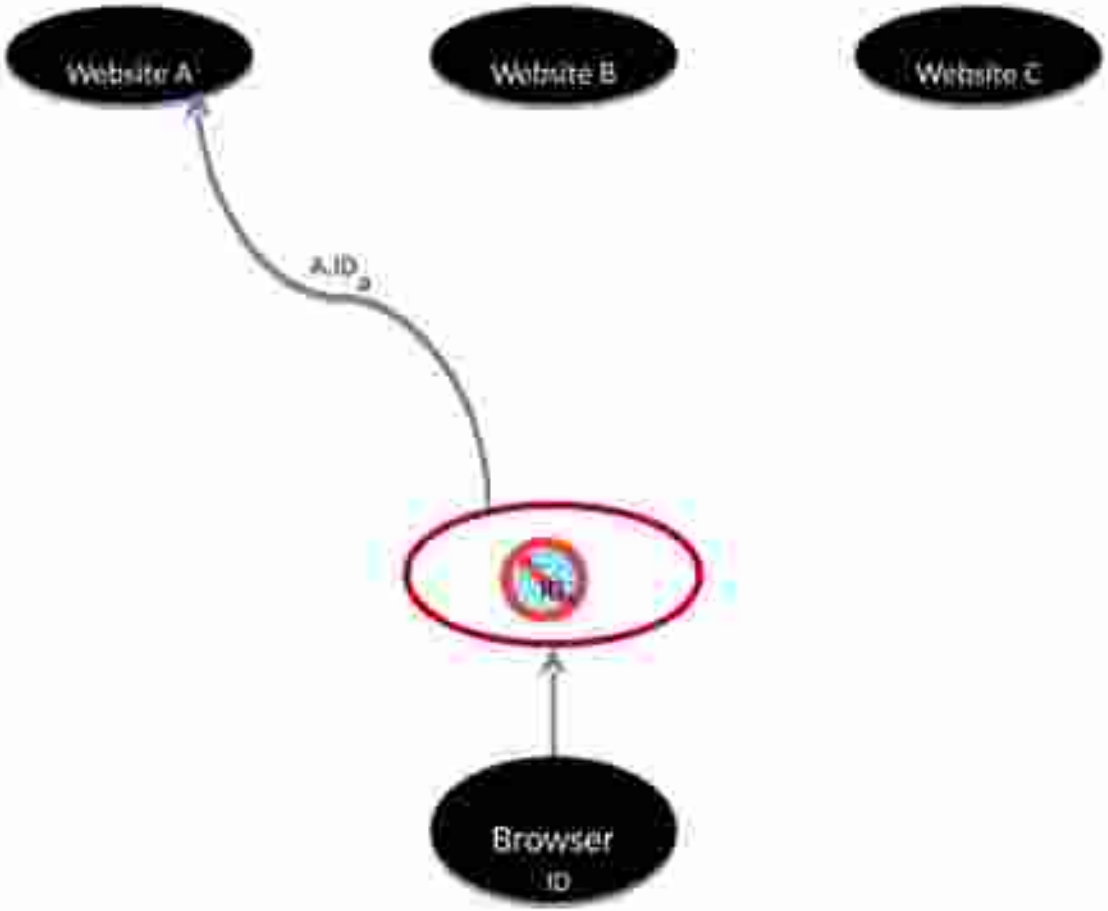
Separate web identities



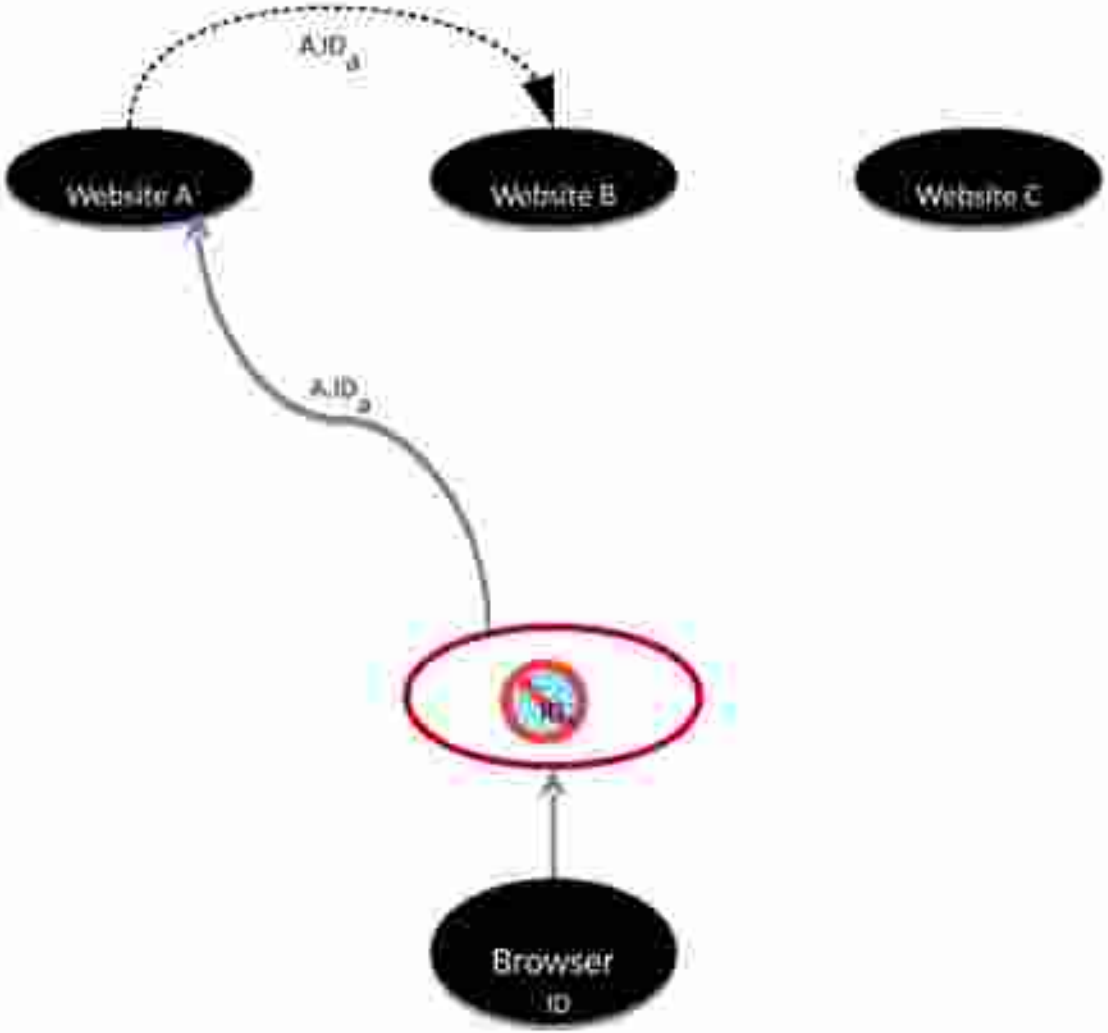
Separate web identities



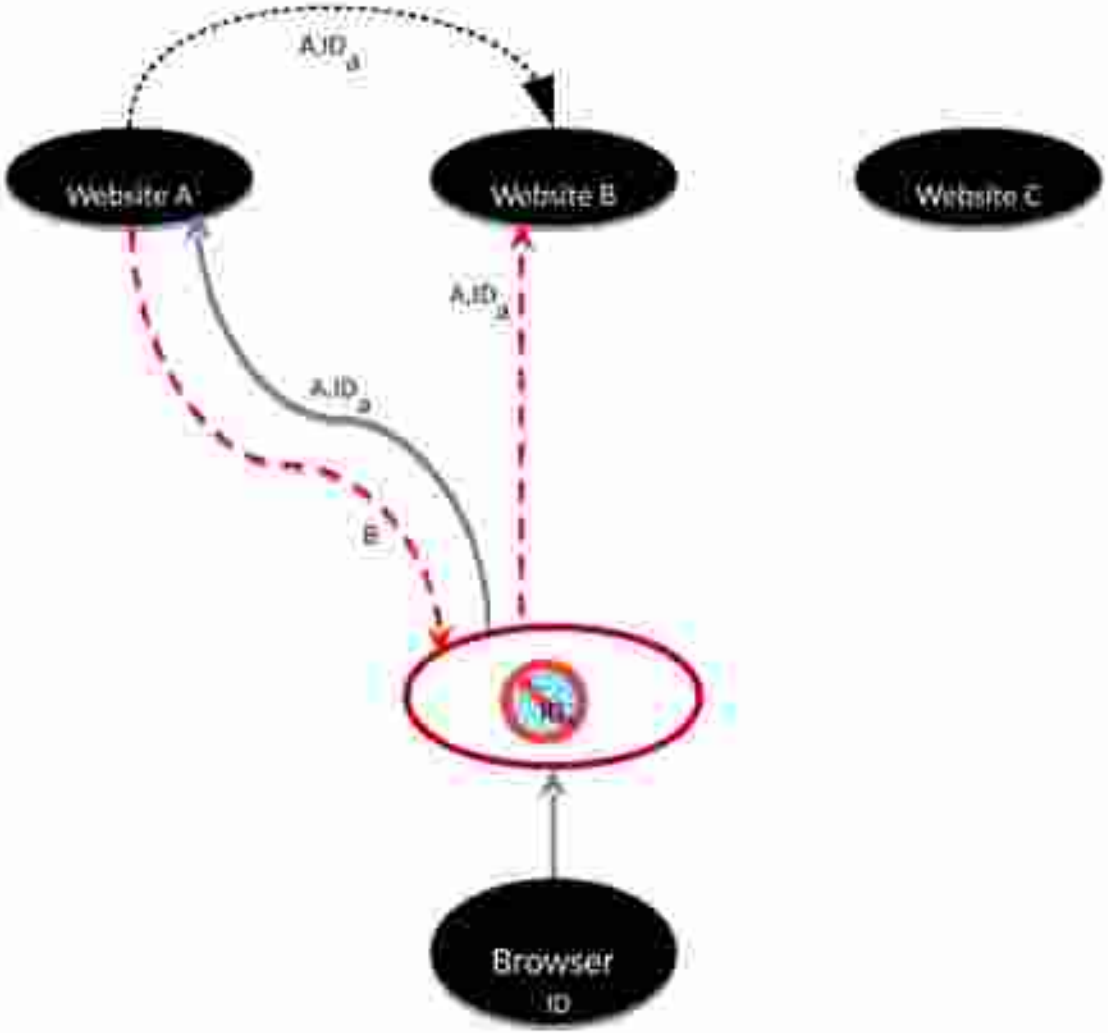
Separate web identities



Separate web identities



Separate web identities



Fingerprinters

Non-profit:

- Panopticlick - academic study
- FingerPrintJS - open source

Commercial:

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

Fingerprinters

Non-profit:

- Panopticlick - academic study
- FingerPrintJS - open source

Commercial:

- AddThis - social media buttons
- BlueCava - advertisements [S&P13]
- Iovation - fraud prevention [S&P13]
- ThreatMetrix - fraud prevention [S&P13]

Fingerprint vectors

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

Attribute	Pan	BC	IO	TM	AM	FPFx
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 per primary domain
- 23 attributes (Tor: 14, FireGloves: 8)
- Covers
  - HTTP (passive fingerprinting)
  - JavaScript (active fingerprinting)
- Additional coverage to ensure functionality
- Canvas fingerprint
  - detection [CCS14]
  - prevention (new)

FP-Block's fingerprint surface

Attribute	FG	FP	PV	KAS	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					✔
DST Daylight Saving				✔	✔
Cookies Enabled					✔
JS doNotTrack Flash Enabled					✔
ActiveX + CLSIDs					
Date & Time					
PHP				✔	✔
System/User Language					✔
OpenDatabase					✔
Canvas Fingerprinting		✔		✔	✔
Mime-type Enumeration	✔	✔	✔		✔
HTTP Pipelining					
IndexedDB					✔
Math Constants					
Windows Registry					
TCP/IP Parameters		✔			
Google Gears Detection					
Flash Manufacturer					
IBM Security Policy					
AJAX Implementation					
MSIE Product Key					
Device Enumeration					
Device Identifiers					
IP address		✔			
HTML Body Behavior					
Battery		✔			✔
WebGLRenderingContext		✔		✔	✔

FP-Block's fingerprint surface

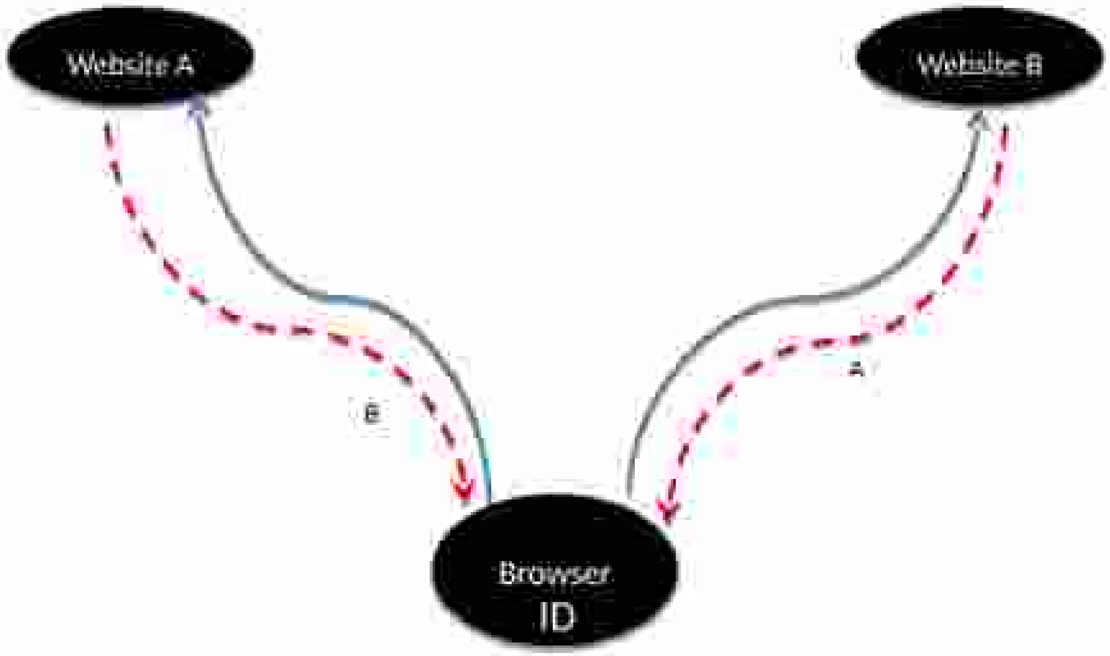
Attribute	FG	FP	PV	KAS	FPB
Plugin Enumeration	✔	✔	✔		✔
Font Detection	✔	✔	✔	✔	✔
User-Agent	✔	✔		✔	✔
HTTP Header Accept					
HTTP Header Accept-Charset		✔			
HTTP Header Accept-Encoding				✔	✔
HTTP Header Accept-Language		✔		✔	✔
Screen Resolution	✔	✔		✔	✔
Timezone	✔	✔		✔	✔
Browser Language	✔				✔
OS & Kernel Version	✔	✔		✔	✔
DOM Storage				✔	✔
IE userData					
Java Enabled					✔
DST Daylight Saving Time				✔	✔
Cookies Enabled					✔
JS do not Flash Enabled					✔
ActiveX + CLSIDs					
Date & Time					
PHP				✔	✔
System/User Language					✔
Open Ports					✔
Canvas Fingerprinting		✔		✔	✔
Supported Video Formats	✔	✔	✔		✔
HTTP Request Header Order					
IndexedDB					✔
Math Constants					
Windows Registry					
TCP/IP Parameters		✔			
Google Gears Detection					
Flash Manufacturer					
IBB Security Policy					
AJAX Implementation					
MSIE Product Key					
Device Enumeration					
Device Identifiers					
IP address		✔			
HTML Body Behavior					
Battery		✔			✔
WebGLRenderingContext		✔		✔	✔

FP-Block's fingerprint surface

Original canvas

Attribute	FG	FP	PM	KAS	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					✔
DST Date Check				✔	✔
Cookies Enabled					✔
JS detect: Flash Enabled					✔
ActiveX + CLSIDs					
Date & Time					
PHP				✔	✔
System/User Language					✔
Open Proxy					✔
Canvas Fingerprinting		✔		✔	✔
Supercookie Detection	✔	✔	✔		✔
HTTP Proxy Detection					
IndexedDB					✔
Math Constants					
Windows Registry					
TCP/IP Parameters		✔			
Google Gears Detection					
Flash Manufacturer					
IBIR Security Policy					
AJAX IntraNetIdentification					
MSIE Product key					
Device Enumeration					
Device Identifiers					
IP address		✔			
HTML Body Behavior					
Battery		✔			✔
WebGLRenderingContext		✔		✔	✔

Validation setup



Validation

- Verify setup
  - Generate fingerprint with fingerprintJS
  - Test without and with FP-Block

- Run validation
  - BC, IO, TM, fingerprintJS, Panopticlick, AddThis

- Additional test: BlueCava ID request

Monitoring evolution of fingerprinters

Updates since September 2014:

• Panopticlick	–
• **BlueCava**	*** (2 updates)**
• **AddThis**	*** (many updates)**
• **Iovation**	**35.7kb, 36.8kb, 35.7kb, 36.8kb, 36.7kb, 37.1kb**
• FingerPrintJS	added screen orientation, *****
• **ThreatMetrix**	**major changes since 27 oct '14**

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!

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)

[Roos12] Arnold Roosendaal. We are all connected to facebook ... by facebook! In European Data Protection: In Good Health, pages 3–19. Springer, 2012.

[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.