SECURITY DILEMMAS IN PUBLISHING LEAKS

Sander Venema
The Logan Symposium
London, 6 December 2014
@VenemaSander, sander@sandervenema.ch

OUTLINE:

Dilemma: Publicity vs security

Domain jurisdiction problems

Tracking & Profiling

Basic web security & operator OPSEC

Tor hidden services

Q&A

THE PROBLEM OF DOMAIN JURISDICTION


TRACKING
& PROFILING

facebook


Jan 4
Dec 28
Search Engines
1,385.00 (59.65%)
Referring Sites
771.00 (33.20%)
Direct Traffic

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	8.13	280.77	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
HTTP_ACCEPT Headers	3.8	13.91	text/html, */* gzip, deflate en-us
Browser Plugin Details	21.76+	3559260	QuickTime 7.7.2.0; Shockwave 11.6.5.635; Flash 11.3.300.257; WindowsMediaplayer 12.0.7601.17514; Silverlight 5.1.20913.0; Adobe Acrobat version 7.?
Time Zone	3.66	12.66	300
Screen Size and Color Depth	4.47	22.22	1280x1024x24
System Fonts	11.82	3613.46	Marlett, Arial, Arabic Transparent, Arial Baltic, Arial CE, Arial CYR, Arial Greek, Arial TUR, Batang, BatangChe, Gungsuh, GungsuhChe, Courier New, Courier New Baltic, Courier New CE, Courier New CYR, Courier New Greek, Courier New TUR, DaunPenh, DokChampa, Estrangelo Edessa, Euphemia, Gautami, Vani, Gulim, GulimChe, Dotum, DotumChe, Impact, Iskoola Pota, Kalinga, Kartika, Khmer UI, Lao UI, Latha, Lucida Console, Malgun Gothic, Mangal, Meiryo, Meiryo UI, Microsoft Himalaya, Microsoft JhengHei, Microsoft YaHei, MingLiU, PMingLiU, MingLiU_HKSCS, MingLiU-ExtB, PMingLiU-ExtB, MingLiU_HKSCS-ExtB, Mongolian Baiti, MS Gothic, MS PGothic, MS UI Gothic, MS Mincho, MS PMincho, MV Boli, Microsoft New Tai Lue, Nyala, Microsoft PhagsPa, Plantagenet Cherokee, Raavi, Segoe Script, Segoe UI, Segoe UI Semibold, Segoe UI Light, Segoe UI Symbol, Shruti, SimSun, NSimSun, SimSun-ExtB, Sylfaen, Microsoft Tai Le, Times New Roman, Times New Roman Baltic, Times New Roman CE, Times New Roman CYR, Times New Roman Greek, Times New Roman TUR, Tunga, Vrinda, Shonar Bangla, Microsoft Yi Baiti, Tahoma, Microsoft Sans Serif, Angsana New, Aparajita, Cordia New, Ebrima, Gisha, Kokila, Leelawadee, Microsoft Uighur, MoolBoran, Symbol, Utsaah, Vijaya, Wingdings, Andalus, Arabic Typesetting, Simplified Arabic, Simplified Arabic Fixed, Sakkal Majalla, Traditional Arabic, Aharoni, David, FrankRuehl, Levenim MT, Miriam, Miriam Fixed, Narkisim, Rod, FangSong, SimHei, KaiTi, AngsanaUPC, BrowalliaNew, BrowalliaUPC, CordiaUPC, DilleniaUPC, EucrosiaUPC, FreesiaUPC, IrisUPC, JasmineUPC, KodchiangUPC, LilyUPC, DFKai-SB, Lucida Sans Unicode, Arial Black, Calibri, Cambria, Cambria Math, Candara, Comic Sans MS, Consolas, Constantia, Corbel, Franklin Gothic Medium, Gabriola, Georgia, Palatino Linotype, Segoe Print, Trebuchet MS, Verdana, Webdings, MT Extra, Arial Unicode MS, Century, Wingdings 2, Wingdings 3, Book Antiqua, Century Gothic, Haettenschweiler, MS Outlook, Tempus Sans ITC, Pristina, Papyrus, Mistral, Lucida Handwriting, Kristen ITC, Juice ITC, French Script MT, Freestyle Script, Bradley Hand ITC, Arial Narrow, Garamond, Monotype Corsiva, Algerian, Baskerville Old Face, Bauhaus 93, Bell MT, Berlin Sans FB, Bernard MT Condensed, Bodoni MT Poster Compressed, Britannic Bold, Broadway, Brush Script MT, Californian FB, Centaur, Chiller, Colonna MT, Cooper Black, Footlight MT Light, Harlow Solid Italic, Harrington, High Tower Text, Jokerman, Kunstler Script, Lucida Bright, Lucida Calligraphy, Lucida Fax, Magneto, Matura MT Script Capitals, Modern No. 20, Niagara Engraved, Niagara Solid, Old English Text MT, Onyx, Parchment, Playbill, Poor Richard, Ravie, Informal Roman, Showcard Gothic, Snap ITC, Stencil, Viner Hand ITC, Vivaldi, Vladimir Script, Wide Latin, Tw Cen MT, Tw Cen MT Condensed, Script MT Bold, Rockwell Extra Bold, Rockwell Condensed, Rockwell, Rage Italic, Perpetua Titling MT, Perpetua, Palace Script MT, OCR A Extended, Malandra GD, Lucida Sans Typewriter, Lucida Sans, Imprint MT Shadow, Goudy Stout, Goudy Old Style, Gloucester MT Extra Condensed, Gill Sans Ultra Bold Condensed, Gill Sans Ultra Bold, Gill Sans MT Condensed, Gill Sans MT, Gill Sans MT Ext Condensed Bold, Gigi, Franklin Gothic Medium Cond, Franklin Gothic Heavy, Franklin Gothic Demi Cond, Franklin Gothic Demi, Franklin Gothic Book, Forte, Felix Titling, Eras Medium ITC, Eras Light ITC, Eras Demi ITC, Eras Bold ITC, Engravers MT, Elephant, Edwardian Script ITC, Curlz MT, Copperplate Gothic Light, Copperplate Gothic Bold, Century Schoolbook, Castellar, Calisto MT, Bookman Old Style, Bodoni MT Condensed, Bodoni MT Black, Bodoni MT, Blackadder ITC, Arial Rounded MT Bold, Agency FB, Bookshelf Symbol 7, MS Reference Sans Serif, MS Reference Specialty, Berlin Sans FB Demi, Tw Cen MT Condensed Extra Bold, Calibri Light (via Flash)
Are Cookies Enabled?	0.43	1.35	Yes
Limited supercookie test	0.95	1.94	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No

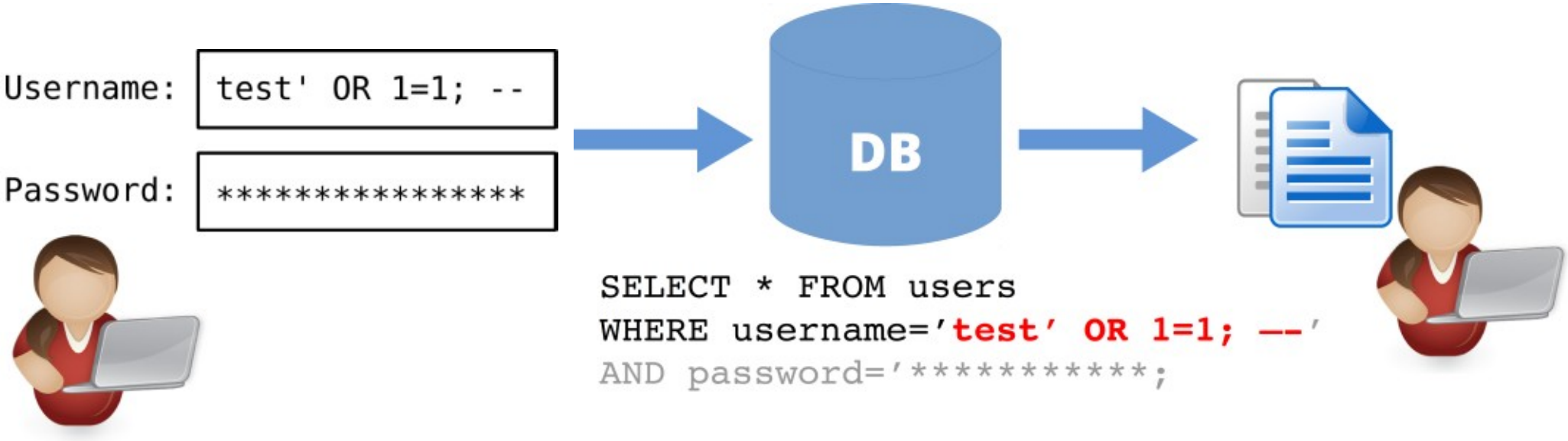
Panopticlick

How Unique — and Trackable — Is Your Browser?

EFF Releases Research on Web Tracking

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	8.47	354.09	Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0
HTTP_ACCEPT Headers	5	32.03	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 gzip, deflate en-us,en;q=0.5
Browser Plugin Details	1.76	3.39	no javascript
Time Zone	1.76	3.38	no javascript
Screen Size and Color Depth	1.76	3.38	no javascript
System Fonts	1.76	3.38	no javascript
Are Cookies Enabled?	0.43	1.34	Yes
Limited supercookie test	1.76	3.38	no javascript

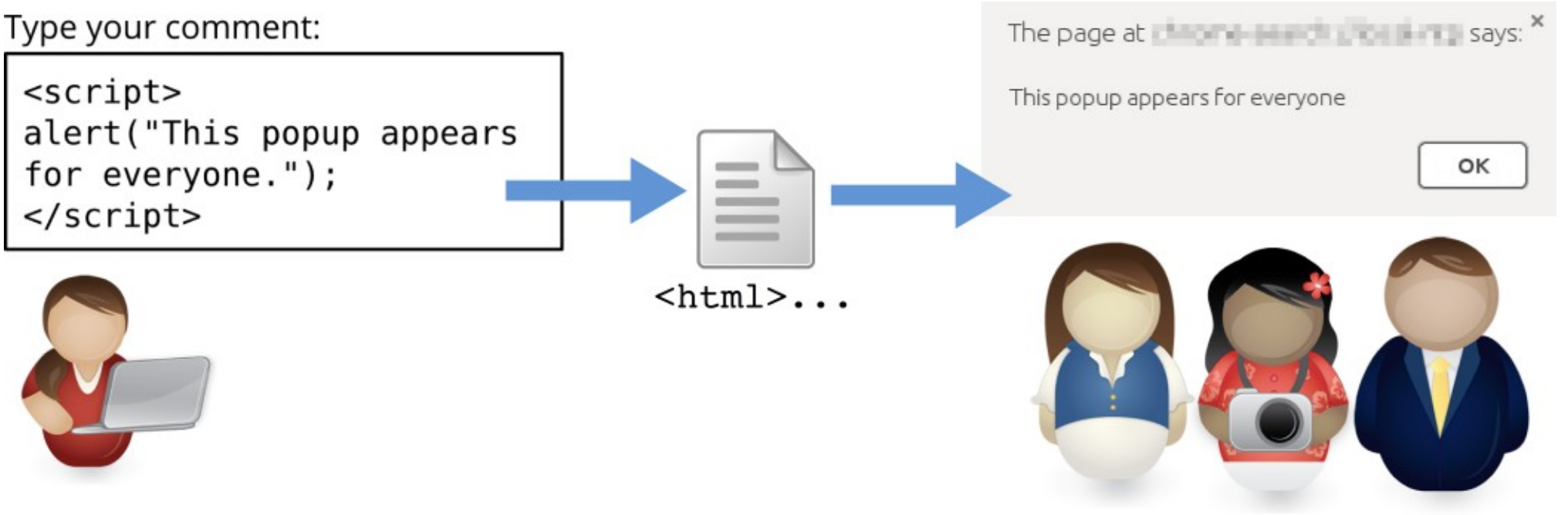

Basic Security
Against Common
Web-based Attacks



SQL Injection:

Attack against a database,

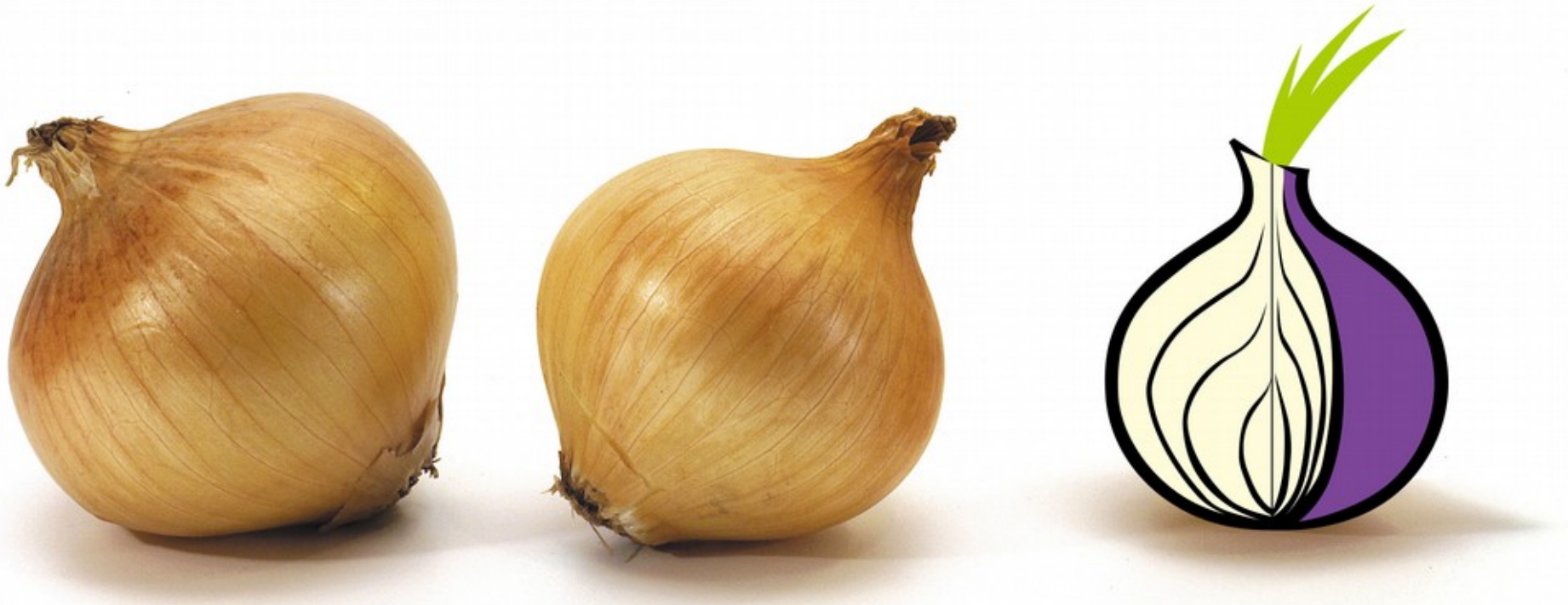
in order to gain access to, change or delete data.



XSS (Cross-Site Scripting) Attack:

Attack against website visitors, by injecting code into web pages viewed by other visitors.

Don’t trust user input!



TOR HIDDEN SERVICES

Sander Venema
Blog: https://sandervenema.ch Twitter: @VenemaSander

E-mail: sander@sandervenema.ch, GPG-key ID: 0x7FB3C51263C3DDAF
Fingerprint: 37FA 9E76 FD24 498E D283 E9A6 7FB3 C512 63C3 DDAF
This presentation: https://sandervenema.ch/slides/logan1214.pdf