Fingerprinting Techniques for Target-oriented Investigations in Network Forensics

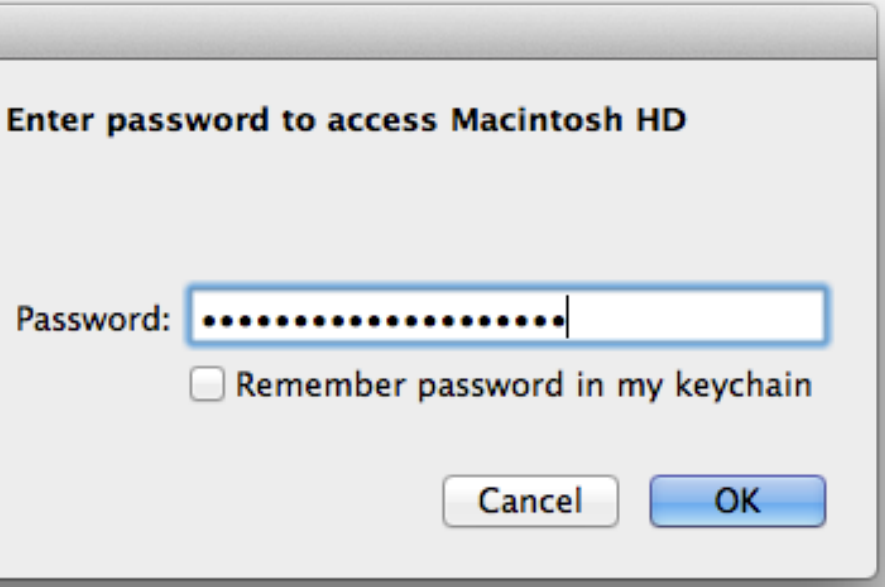
Dominik Herrmann
Karl-Peter Fuchs
Hannes Federrath

Folien: http://dhgo.to/fpforensics

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Verschlüsselungstechniken erschweren forensische Ermittlungen

- Bestandsdatenauskunft (§ 113 TKG)
- Telekommunikationsüberwachung (§§ 100a, 100b StPO)
- Sicherstellung/Durchsicht von Festplatten (§§ 97, 110 StPO)



> With current resources, law enforcement's hands are tied when it comes to FDE when used by anyone who is diligent with the passphrase.

Casey et al: The growing impact of full disk encryption on digital forensics

Forderung nach unverhältnismäßigen Ermittlungsmethoden

http://gutjahr.biz/2013/12/vorratsdaten

The Australian Security Intelligence Organization (ASIO) is pushing for laws that would make telecommunications companies **retain their customers' web-browsing data, as well as forcing web users to decrypt encrypted messages.**

http://rt.com/news/australia-nsa-snowden-surveillance-510
http://arstechnica.com/tech-policy/2014/03/after-snowden-australias-cops-worry-about-people-using-crypto

Einsatz von unverhältnismäßigen Ermittlungsmethoden

Jürgen Schmidt

Trojaner im Staatsauftrag

Online-Überwachung durch Bundes- und Landespolizei

Mit großem Trara veröffentlichte der CCC seine Analyse eines Staatstrojaners. In der folgenden hitzigen Diskussion um Computerwanzen zwischen Terrorgefahr und Privatsphäre kamen die Fakten oft zu kurz.

c't 2011, Heft 23, S. 28

```
Dummheit ist ein grausamer, globaler Got
_0zapftis_aes_secretkey db 49h, 3, 93h,

db 0A8h, 0F5h, 0Ah, 0B9h, 94h, 2,
db 0F3h, 0ADh, 93h, 0F5h, 32h, 93h
db    0
db    0
db    0
db    0
```

Anatomie eines digitalen Ungeziefers

Wie der Staatstrojaner zerlegt wurde: Die Hacker vom Chaos Computer Club haben die Überwachungssoftware gefunden, analysiert – und gehackt. Das Ergebnis ist erschreckend. Der Trojaner kann unsere Gedanken lesen und unsere Computer fernsteuern

Von Frank Rieger

les Stirnrunzeln hervorrief: Es ist der Abschnitt zur sogenannten „Quellen-Telekommunikationsüberwachung". Die Regierung und Vertreter der Ermittlungsbehörden hatten in der Karlsruher Verhandlung vehement argumentiert, dass sie eine Möglichkeit brauchten, etwaige verschlüsselte Kommunikation schon auf dem Computer des Verdächtigen abzufangen, bevor sie verschlüsselt wird. Das Gericht mochte sich diesem Begehren nicht ganz verschließen und ließ eine sogenannte „Quellen-Telekommunikationsüberwachung" zu – allerdings nur, „wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein."

Wie denn eine derartige Sicherstellung in der Praxis technisch funktionieren sollte, war schon während der mündlichen Anhörung zum Bundestrojaner in Karlsruhe ein höchst umstrittener Punkt. Das Gericht hatte die Gefahren jedenfalls erkannt und schrieb: „Wird ein komplexes informa-

Chat-Gespräche dokumentiert. Beantragt und richterlich genehmigt wird die sogenannte „Quellen-Telekommunikationsüberwachung" wie eine normale Telefonüberwachung.

Wehren sich Beschuldigte gegen die-

Festplatten tatsächlich jeweils eine behördliche Computerwanzensoftware. Die Trojaner-Varianten sind einander ausgesprochen ähnlich und weisen nur geringfügige Unterschiede auf. Die Dateien, die einst die Betroffenen ausspioniert

Das Betriebssystem eines Computers stellt ganz grundlegende Funktionen bereit, die jedes Programm benötigt, um auf dem Computer zu laufen. Dazu gehören zum Beispiel das Lesen und Schreiben von Dateien. Senden und Empfan-

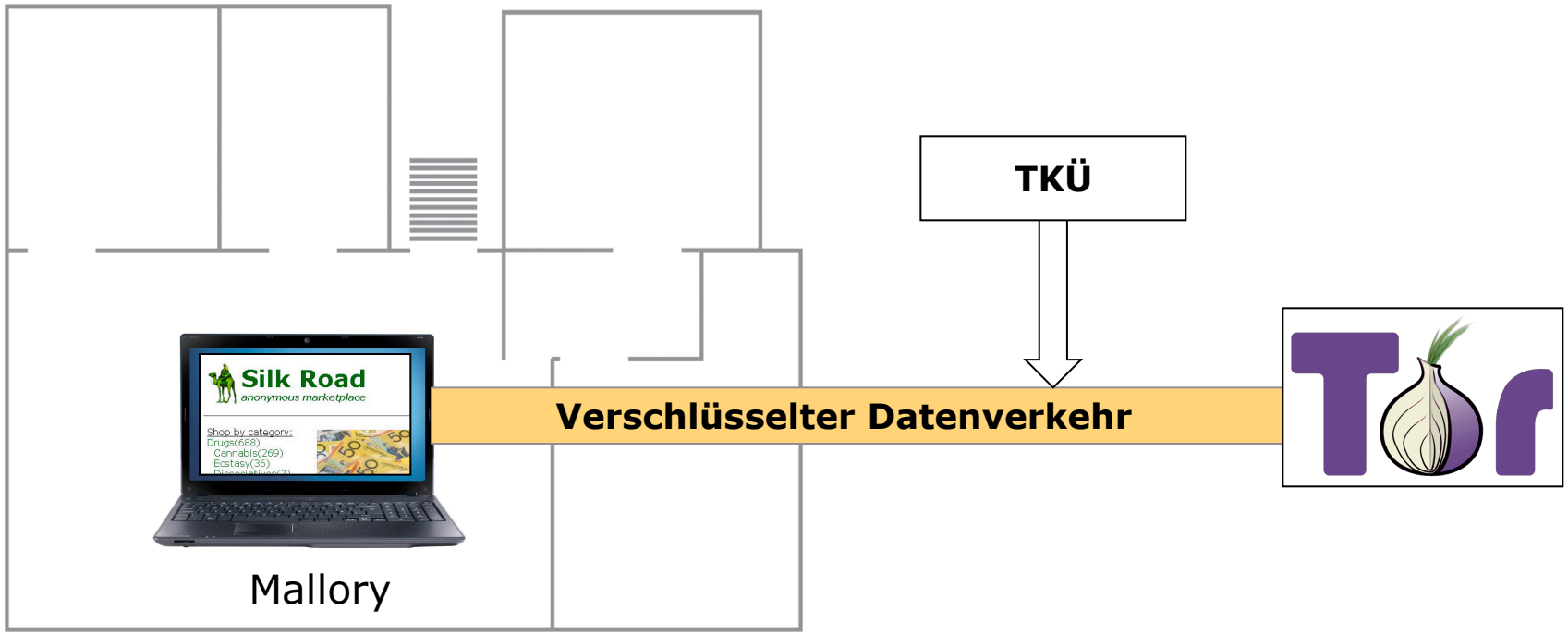
mussten die Hacker nur den Schlüssel aus einem der Trojaner extrahieren und den Trojaner in einem von der Außenwelt isolierten Netz in Betrieb nehmen. Dabei mussten sie allerdings feststellen, dass die Verschlüsselung fachlich falsch

Überall sonst im N
line-Banking oder s
sind das längst ü
mechanismen. Die
für die Akzeptanz d
liche Spionagesoftw
sie so aussehen, als
Adresse des Weite
men. Das Vorspiege
senderadresse ist je
Leichtes. Dadurch
Computerwanze ei
Sicherheitsloch aufg
fach ausgenutzt wer
Die Funktionen,
steuerungsschnittste
können, sind aufschl
menstellung und Ar
sen keinen Zweifel
ein von Ermittlung
tes Schnüffelprogra
ternettelefonate mit
und Bildschirmfotos
befindlichen Webbr
chen sind genau die
den Ermittlungsbeh
lautstark gefordert w
schung zu umgehen
Abhören unmöglich
le" Trojaner, wie sie
fen von Online-Ba
det werden, hätten
gantere Mechanism
gängigen Antivirus
Trojaner völlig unbe
Die weitaus scho
bei der die beteiligt
ren Augen nicht tra
dem Kommando r
kann der Inhaber de
walt ein beliebiges
Netz auf den infizie
und ausführen lasse
troffene Nutzer
bekommt. Genau
lich höchst problem
der die Ermittlungs

FAS, 9.10.2011, S. 41

„Quellen-TKÜ"

Website-Fingerprinting zur Ermittlung abgerufener Webseiten

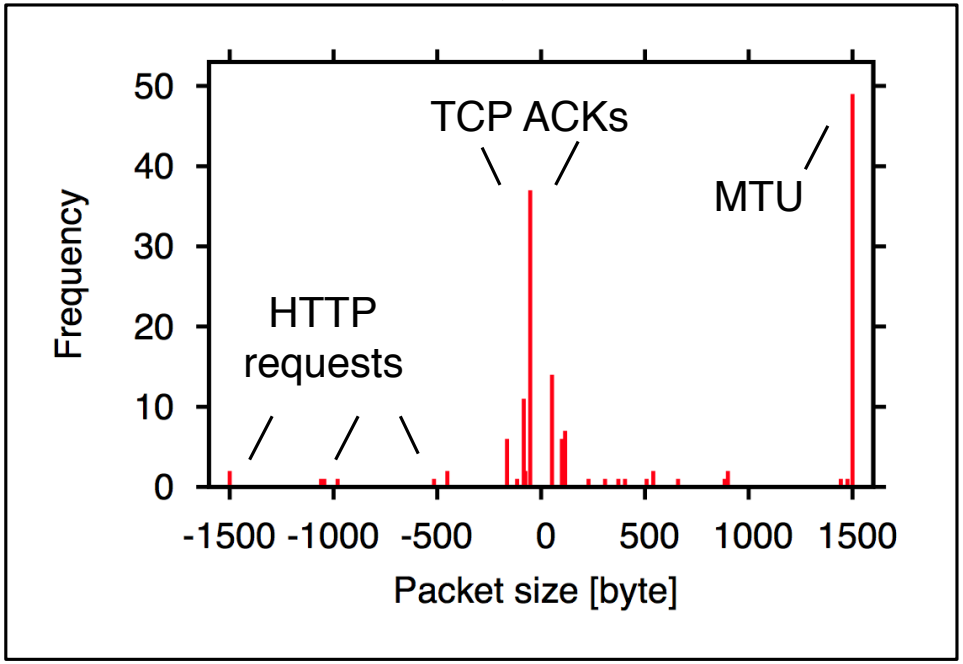


Beobachtbare verschlüsselte IP-Pakete:

Zeit

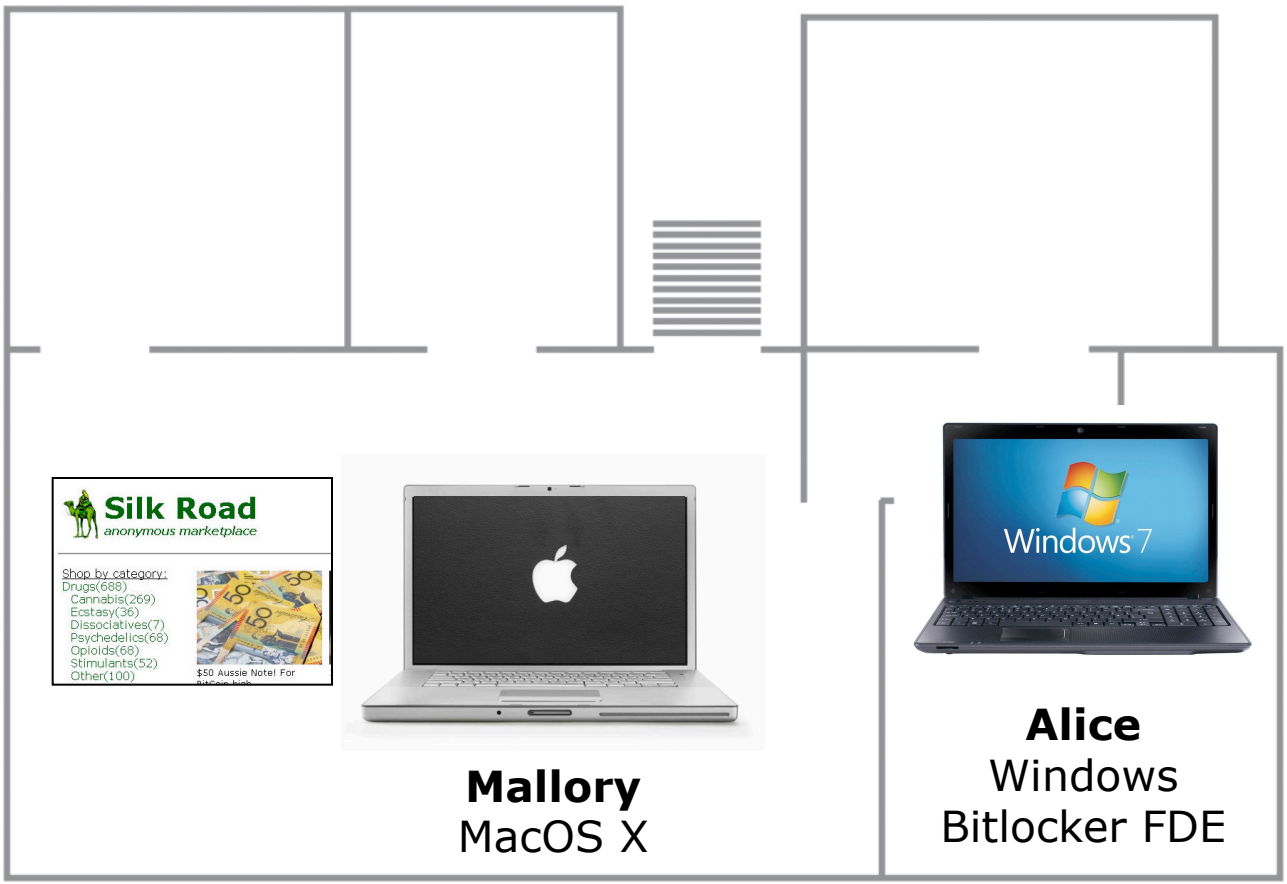
Trotz Verschlüsselung charakteristische Verteilung der Paketgrößen

IP Packet Fragmentation



[Hin02, BLJL05, LL06, HWF09, PNZE11, …]

Device-Fingerprinting zur Eingrenzung

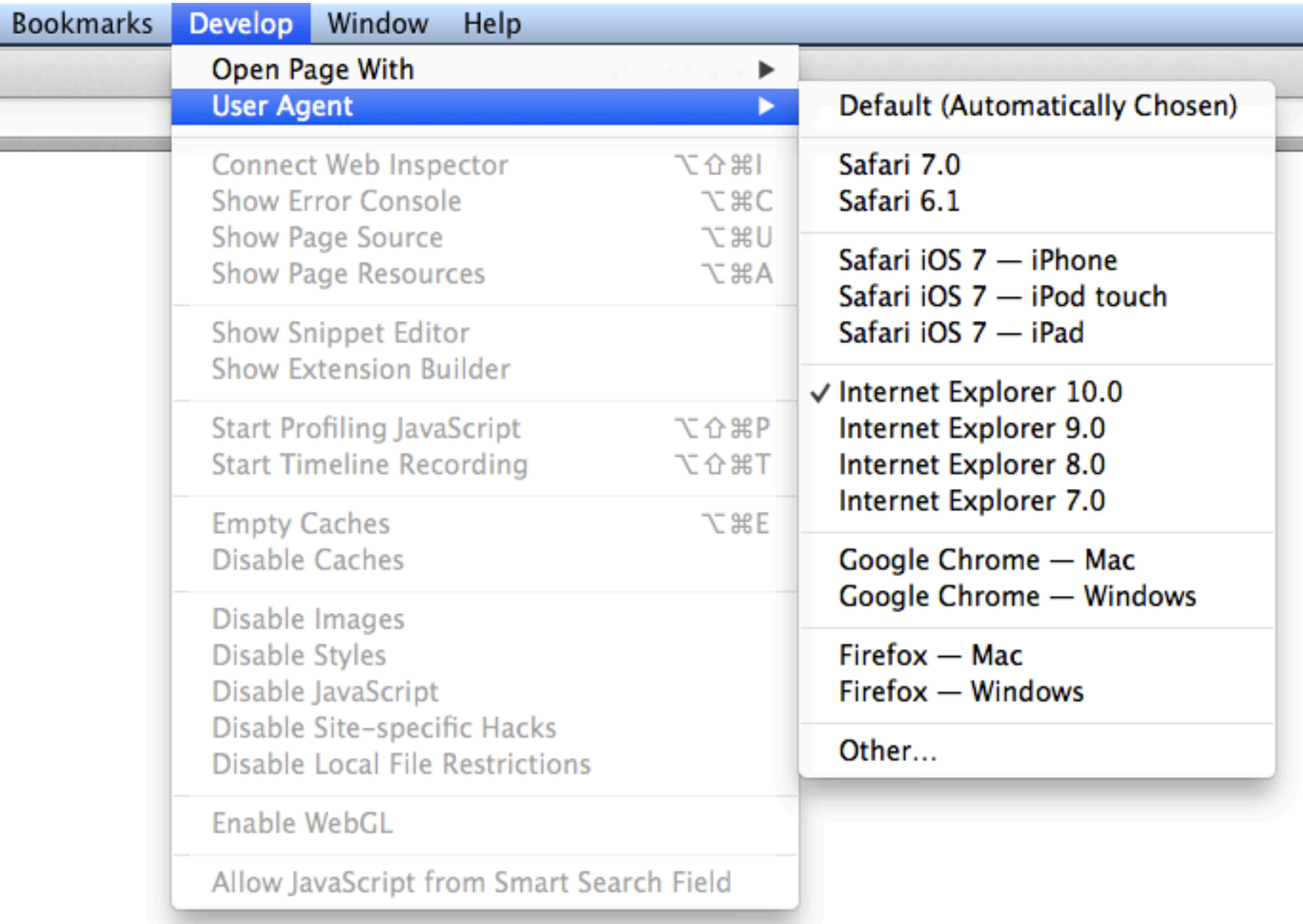


Device-Fingerprinting zur Eingrenzung

GET / HTTP/1.1
Host: silkroad6ownowfk.onion
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Win64; x64)
Accept-Encoding: gzip

Mallory
MacOS X

Alice
Windows
Bitlocker FDE


Bookmarks
Develop
Window
Help
Open Page With
User Agent
Connect Web Inspector ⌥⇧⌘I
Show Error Console ⌥⌘C
Show Page Source ⌥⌘U
Show Page Resources ⌥⌘A
Show Snippet Editor
Show Extension Builder
Start Profiling JavaScript ⌥⇧⌘P
Start Timeline Recording ⌥⇧⌘T
Empty Caches ⌥⌘E
Disable Caches
Disable Images
Disable Styles
Disable JavaScript
Disable Site-specific Hacks
Disable Local File Restrictions
Enable WebGL
Allow JavaScript from Smart Search Field
Default (Automatically Chosen)
Safari 7.0
Safari 6.1
Safari iOS 7 — iPhone
Safari iOS 7 — iPod touch
Safari iOS 7 — iPad
✓ Internet Explorer 10.0
Internet Explorer 9.0
Internet Explorer 8.0
Internet Explorer 7.0
Google Chrome — Mac
Google Chrome — Windows
Firefox — Mac
Firefox — Windows
Other…

Betriebssystem-Fingerprinting anhand impliziter Merkmale

Operating System (OS)	IP Initial TTL	TCP window size
Linux (kernel 2.4 and 2.6)	64	5840
Google's customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows 7, Vista and Server 2008	128	8192
Cisco Router (IOS 12.4)	255	4128

Tools: p0f, ettercap

http://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting

Betriebssystem-Fingerprinting mittels DNS-Anfragen

Windows 7

swdist.apple.com su.itunes.apple.com
time.euro.apple.com internalcheck.apple.com
identity.apple.com configuration.apple.com
keyvalueservice.icloud.com

au.v4.download.windowsupdate.com
definitionupdates.microsoft.com
spynet2.microsoft.com
watson.telemetry.microsoft.com
clientconfig.passport.net …

MacOS X 10.8.5

mirrorlist.centos.org
[x].centos.pool.ntp.org

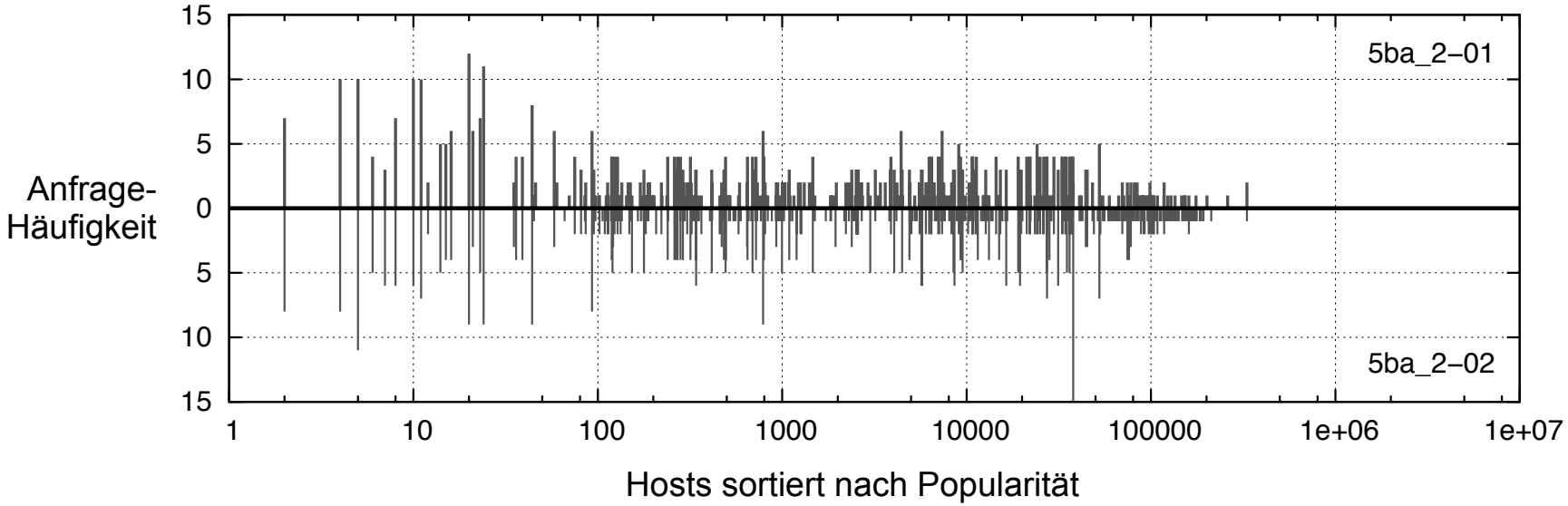
CentOS 6

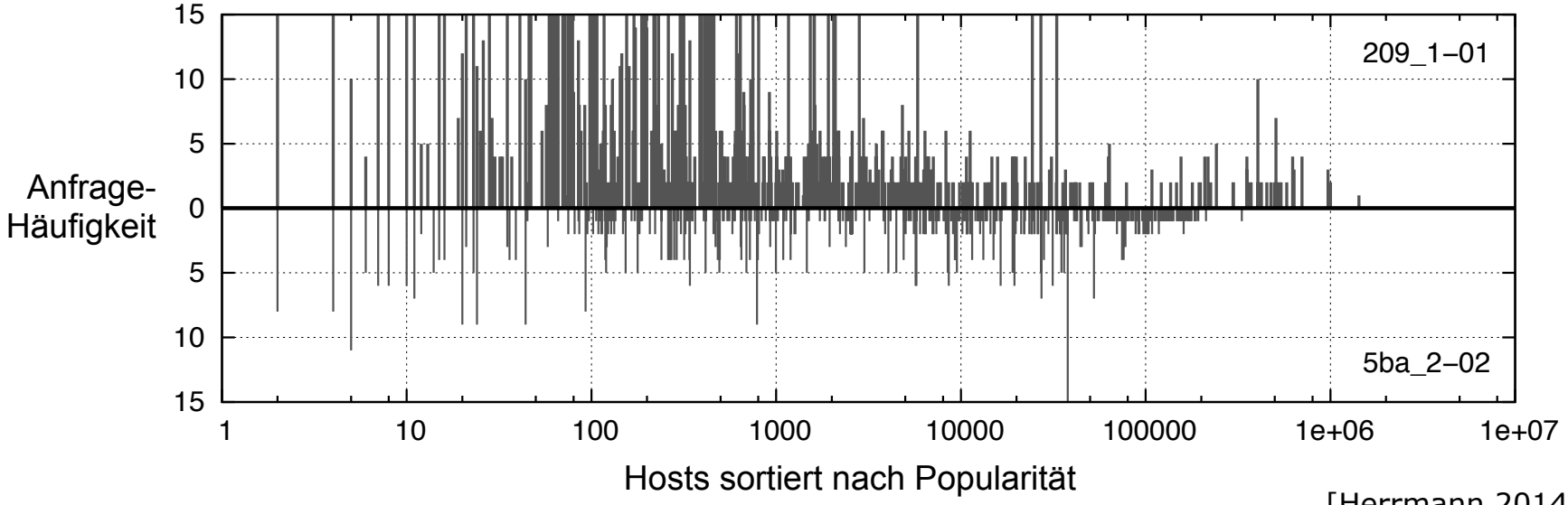
changelogs.ubuntu.com ntp.ubuntu.com geoip.ubuntu.com daisy.ubuntu.com _https._tcp.fs.one.ubuntu.com fs-[x].one.ubuntu.com

Ubuntu 12.04

Nutzerverhalten-Fingerprinting: Verkettung von Sitzungen

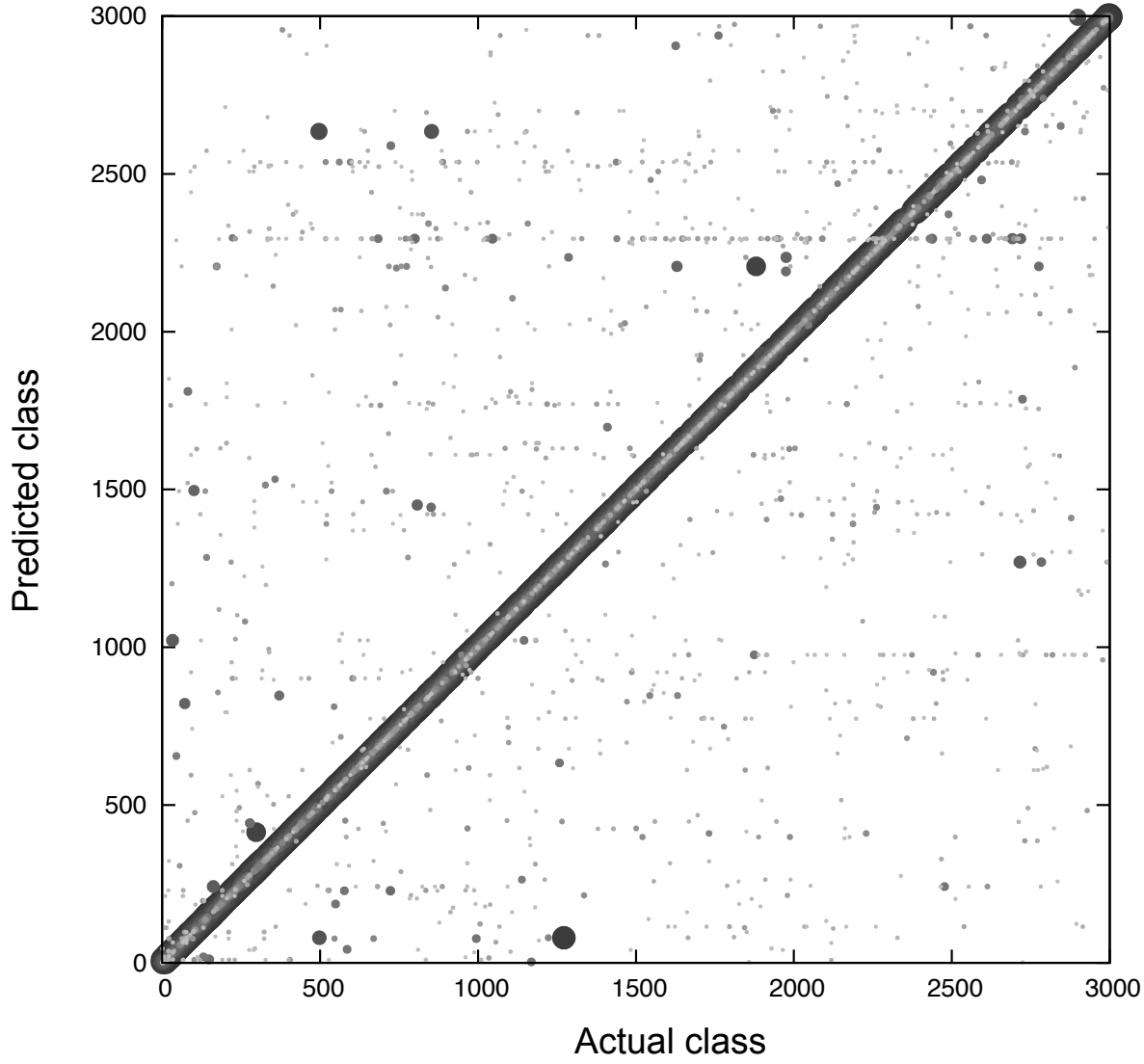
Nutzer haben charakteristische Verhaltensmuster





[Herrmann 2014]

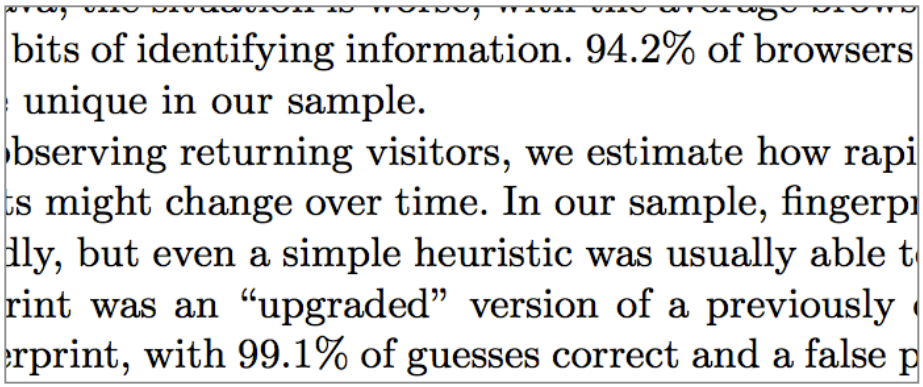
Bei 3000 Nutzern im Mittel 86 % der Sitzungen verkettbar



[Herrmann 2014]

Soll Fingerprinting zur Strafverfolgung eingesetzt werden?

- Unklare Beweiskraft
  - Mangelhafte Erklärbarkeit von Entscheidungen
  - Trügerische Genauigkeitswerte in Veröffentlichungen



bits of identifying information. 94.2% of browsers
unique in our sample.
bserving returning visitors, we estimate how rapi
s might change over time. In our sample, fingerpr
dly, but even a simple heuristic was usually able t
rint was an "upgraded" version of a previously
rprint, with 99.1% of guesses correct and a false p

- Neue Begehrlichkeit: Eignung zur Massenüberwachung

  „besonders datenschutzfreundlich"

Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)

BY MATT BLAZE 06.19.13 9:30 AM

Eckersley: How Unique Is Your Web Browser? (2010)
http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again/ (2013)

Zusammenfassung

- Forensische Ermittlung durch Verschlüsselung erschwert
- Potenziell anwendbare Fingerprinting-Techniken
  - Erkennung verschlüsselt übertragener Webseiten
  - Implizite Merkmale von Betriebssystemen und Web-Browsern
  - Charakteristisches Nutzerverhalten zur Sitzungsverkettung
- Einsatz bei forensischen Untersuchungen zu diskutieren
  - Unklare Aussagekraft
  - Missbrauchspotenzial

Dominik Herrmann (Universität Hamburg)
herrmann@informatik.uni-hamburg.de
Folien: http://dhgo.to/fpforensics