CSE 484 / CSE M 584: Computer Security and Privacy

Loose Ends: Side Channels, Government Surveillance & Targeted Attacks

Spring 2015

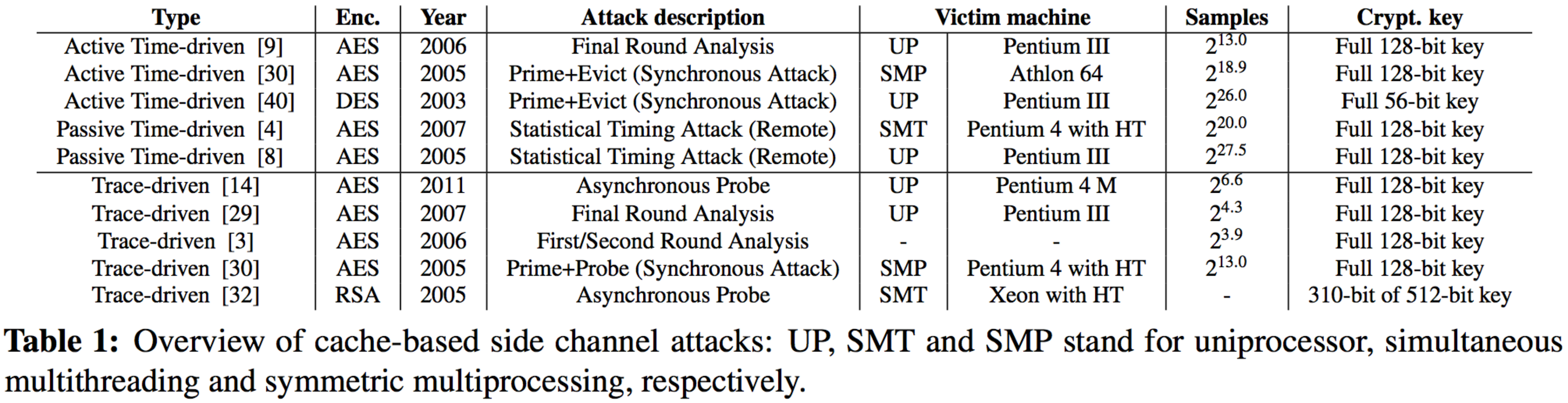
Franziska (Franzi) Roesner
franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Side Channel Attacks

- Attacks based on information that can be gleaned from the physical implementation of a system, rather than breaking its theoretical properties
  - Most commonly/devastatingly used against cryptosystems
  - But also prevalent in other contexts, e.g., due to widespread smartphone sensors

Cache-Based Side Channels



Type	Enc.	Year	Attack description	Victim machine		Samples	Crypt. key
Active Time-driven [9]	AES	2006	Final Round Analysis	UP	Pentium III	$2^{13.0}$	Full 128-bit key
Active Time-driven [30]	AES	2005	Prime+Evict (Synchronous Attack)	SMP	Athlon 64	$2^{18.9}$	Full 128-bit key
Active Time-driven [40]	DES	2003	Prime+Evict (Synchronous Attack)	UP	Pentium III	$2^{26.0}$	Full 56-bit key
Passive Time-driven [4]	AES	2007	Statistical Timing Attack (Remote)	SMT	Pentium 4 with HT	$2^{20.0}$	Full 128-bit key
Passive Time-driven [8]	AES	2005	Statistical Timing Attack (Remote)	UP	Pentium III	$2^{27.5}$	Full 128-bit key
Trace-driven [14]	AES	2011	Asynchronous Probe	UP	Pentium 4 M	$2^{6.6}$	Full 128-bit key
Trace-driven [29]	AES	2007	Final Round Analysis	UP	Pentium III	$2^{4.3}$	Full 128-bit key
Trace-driven [3]	AES	2006	First/Second Round Analysis	-	-	$2^{3.9}$	Full 128-bit key
Trace-driven [30]	AES	2005	Prime+Probe (Synchronous Attack)	SMP	Pentium 4 with HT	$2^{13.0}$	Full 128-bit key
Trace-driven [32]	RSA	2005	Asynchronous Probe	SMT	Xeon with HT	-	310-bit of 512-bit key

Table 1: Overview of cache-based side channel attacks: UP, SMT and SMP stand for uniprocessor, simultaneous multithreading and symmetric multiprocessing, respectively.

"By exploiting side channels that arise from shared CPU caches, researchers have demonstrated attacks extracting encryption keys of popular cryptographic algorithms such as AES, DES, and RSA."

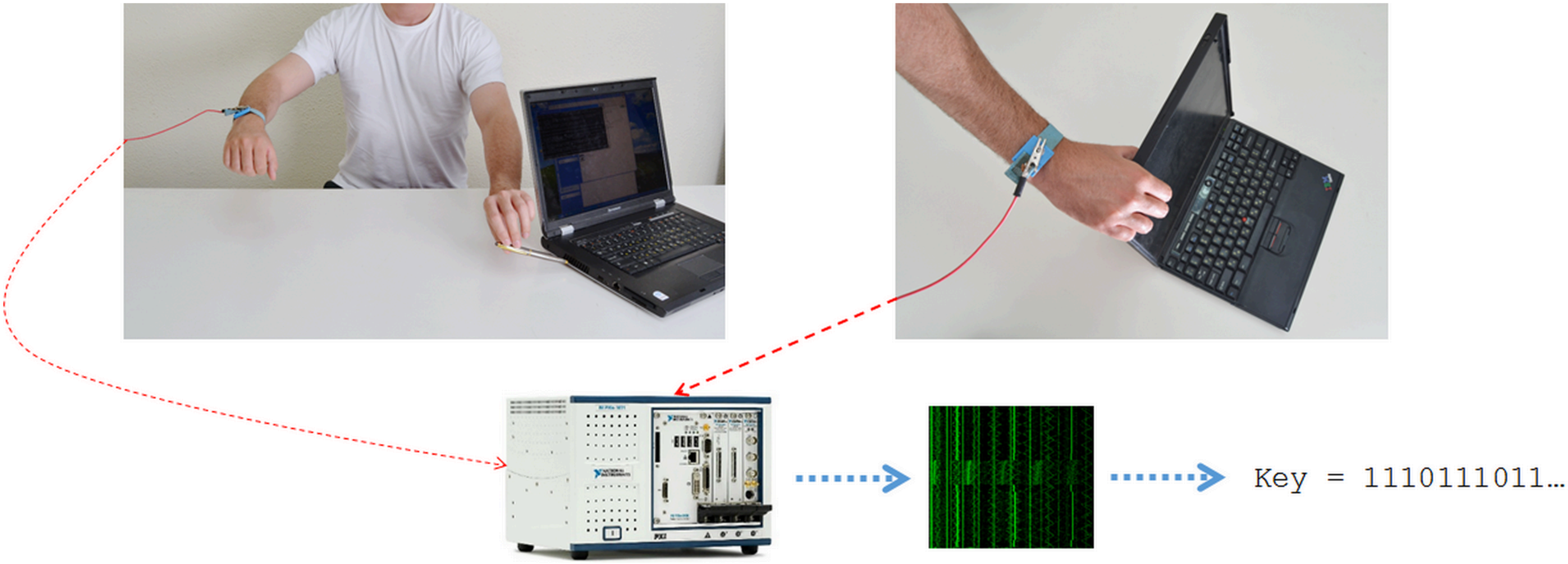
Kim et al. "STEALTHMEM: System-Level Protection Against Cache-Based Side Channel Attacks in the Cloud" USENIX Security 2012

Others (on Cryptosystems)

- Timing attacks
- Power analysis
- Etc.

If you do something different for secret key bits 1 vs. 0, attacker can learn something…

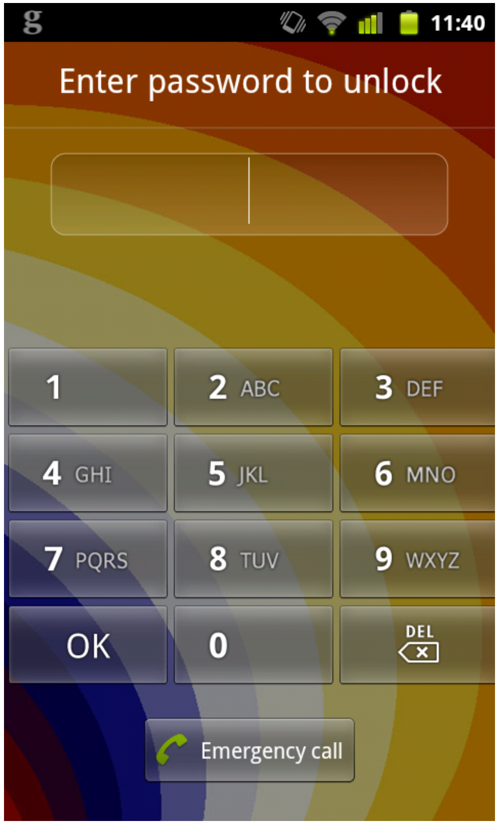
Key Extraction via Electric Potential



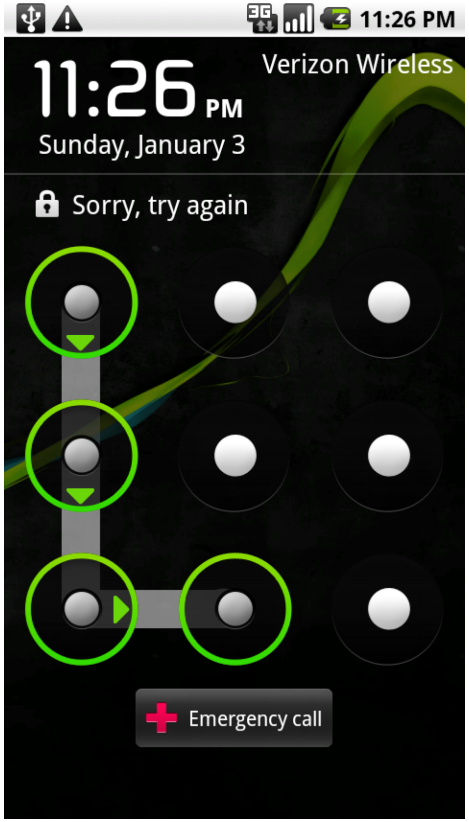
Key = 1110111011…

Genkin et al. “Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks On PCs” CHES 2014

Accelerometer Eavesdropping



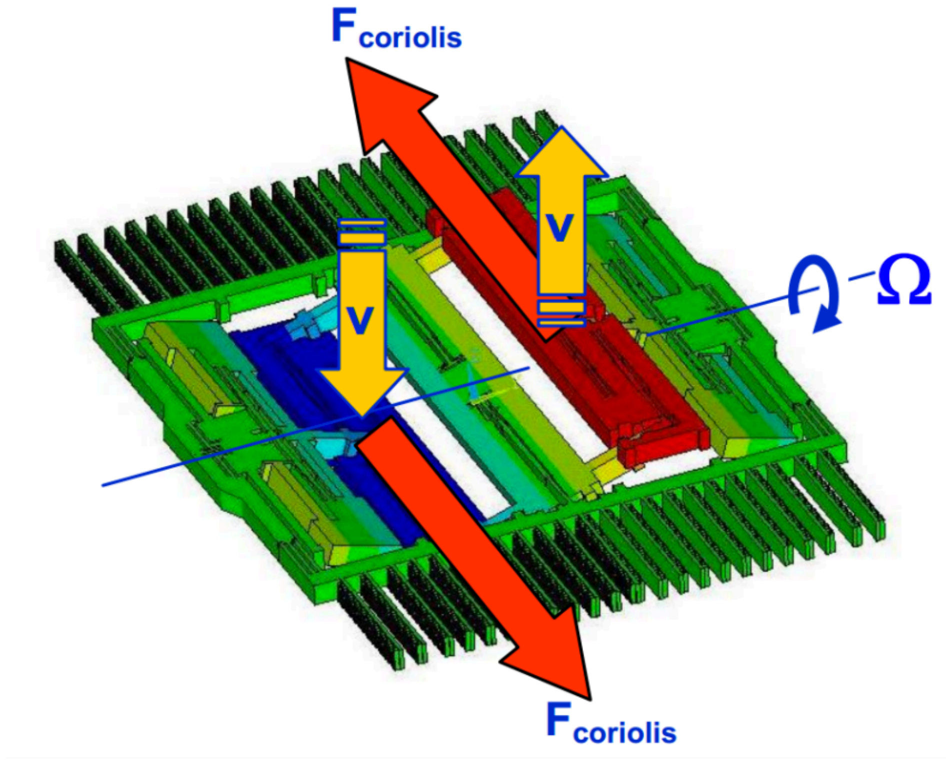
Enter password to unlock



Sorry, try again

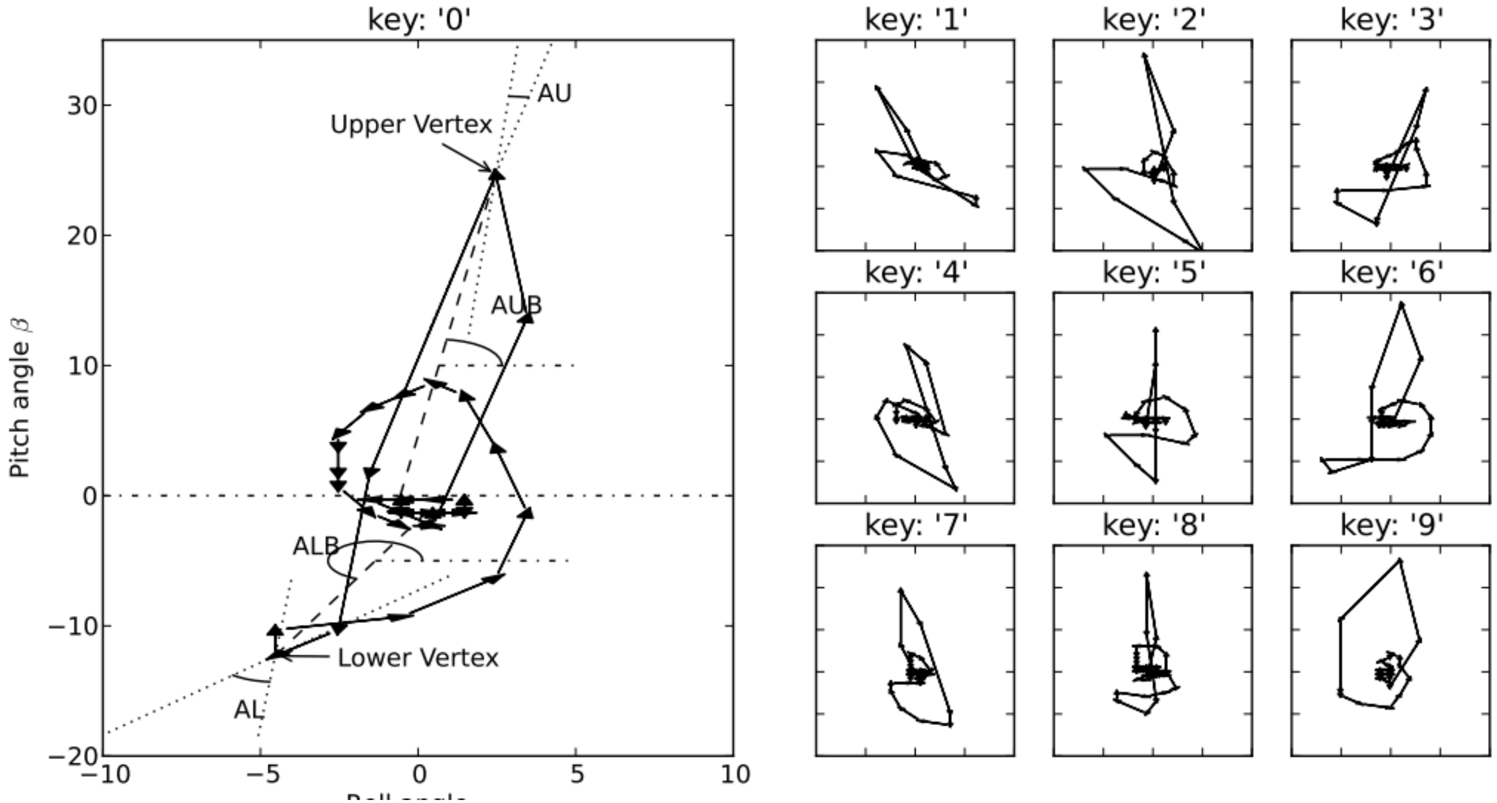
Aviv et al. “Practicality of Accelerometer Side Channels on Smartphones” ACSAC 2012

Gyroscope Eavesdropping



Michalevsky et al. "Gyrophone: Recognizing Speech from Gyroscope Signals" USENIX Security 2014

More Gyroscope



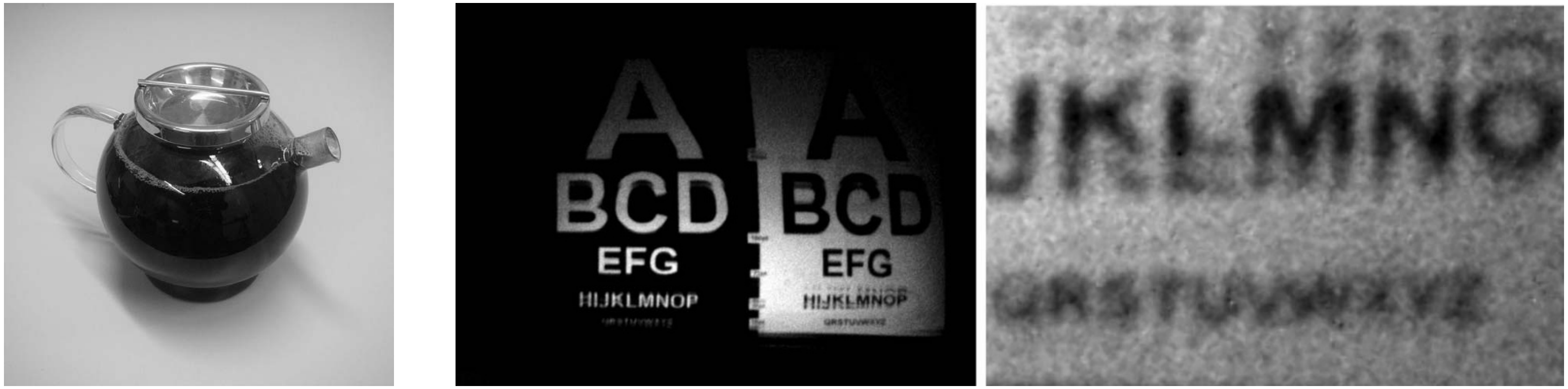
Chen et al. "TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion" HotSec 2011

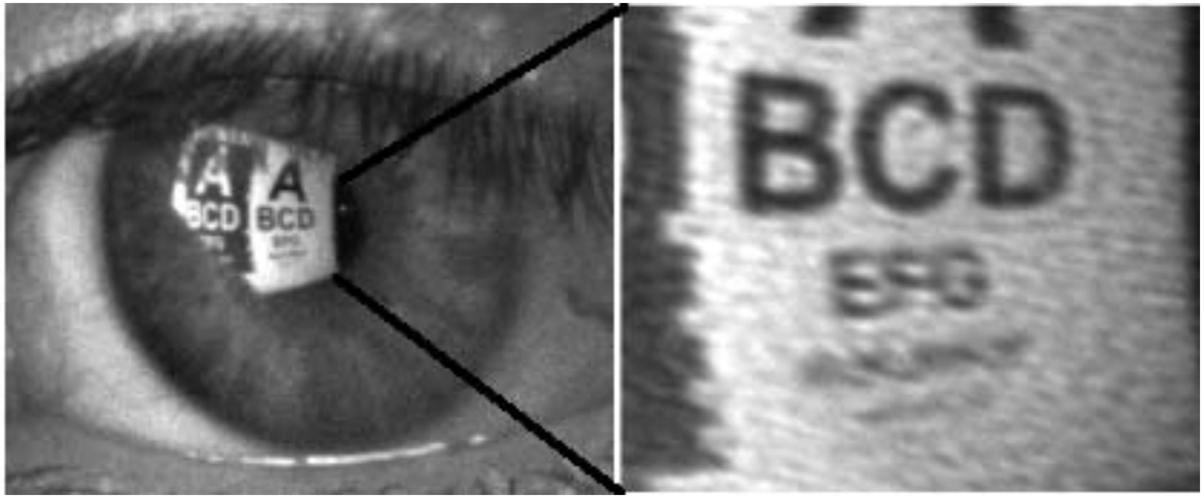
Keyboard Eavesdropping

Zhuang et al. “Keyboard Acoustic Emanations Revisited” CCS 2005
Vuagnoux et al. “Compromising Electromagnetic Emanations of Wired and Wireless Keyboards” USENIX Security 2009

[Backes et al.]

Compromising Reflections





Audio from Video

Davis et al. "The Visual Microphone: Passive Recovery of Sound from Video" SIGGRAPH 2014

Identifying Web Pages: Traffic Analysis

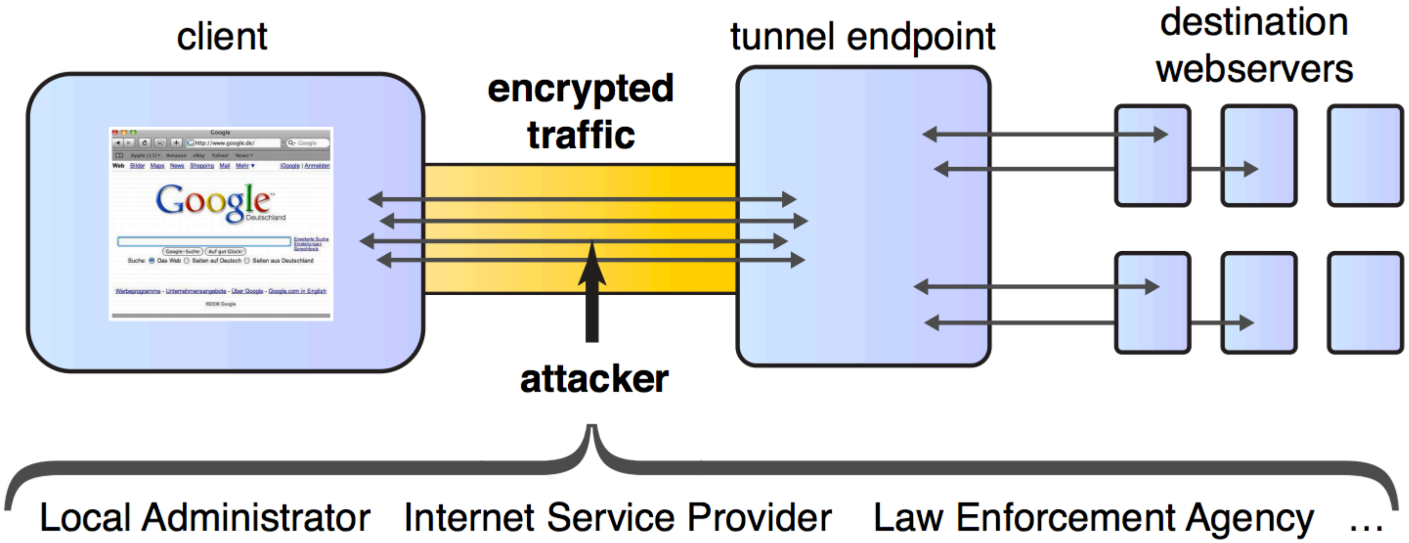
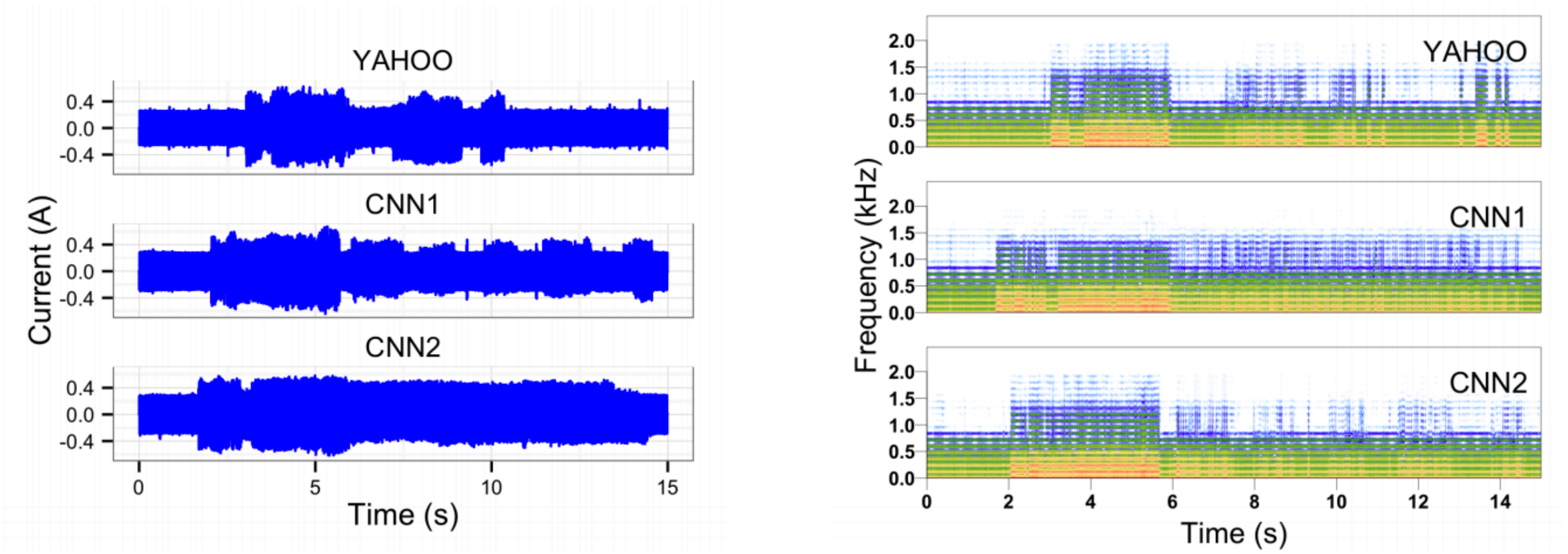


Figure 1: Website fingerprinting scenario and conceivable attackers

Herrmann et al. "Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naïve-Bayes Classifier" CCSW 2009

Identifying Web Pages: Electrical Outlets



(a) Time-domain plots

(b) Spectrogram plots

Fig. 1: Time- and frequency-domain plots of several power traces as a MacBook loads two different pages. In the frequency domain, brighter colors represent more energy at a given frequency. Despite the lack of obviously characteristic information in the time domain, the classifier correctly identifies all of the above traces.

Clark et al. “Current Events: Identifying Webpages by Tapping the Electrical Outlet” ESORICS 2013

Powerline Eavesdropping

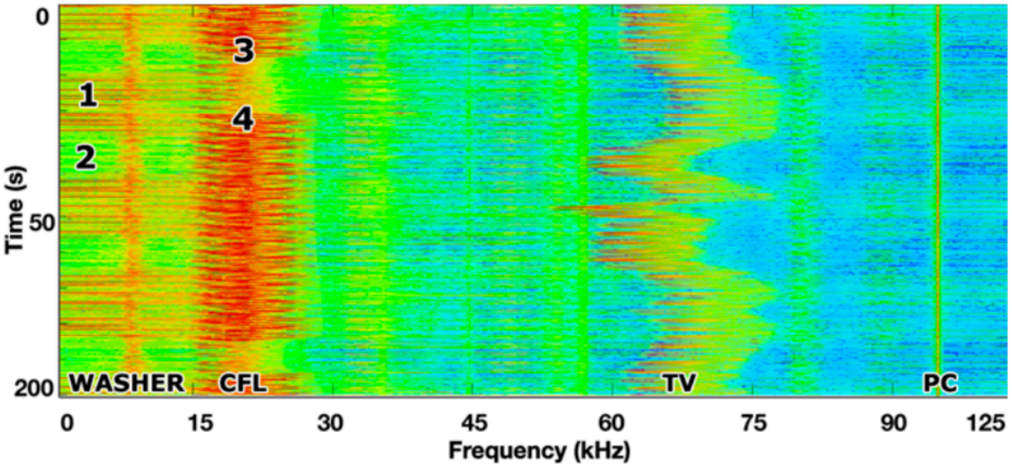
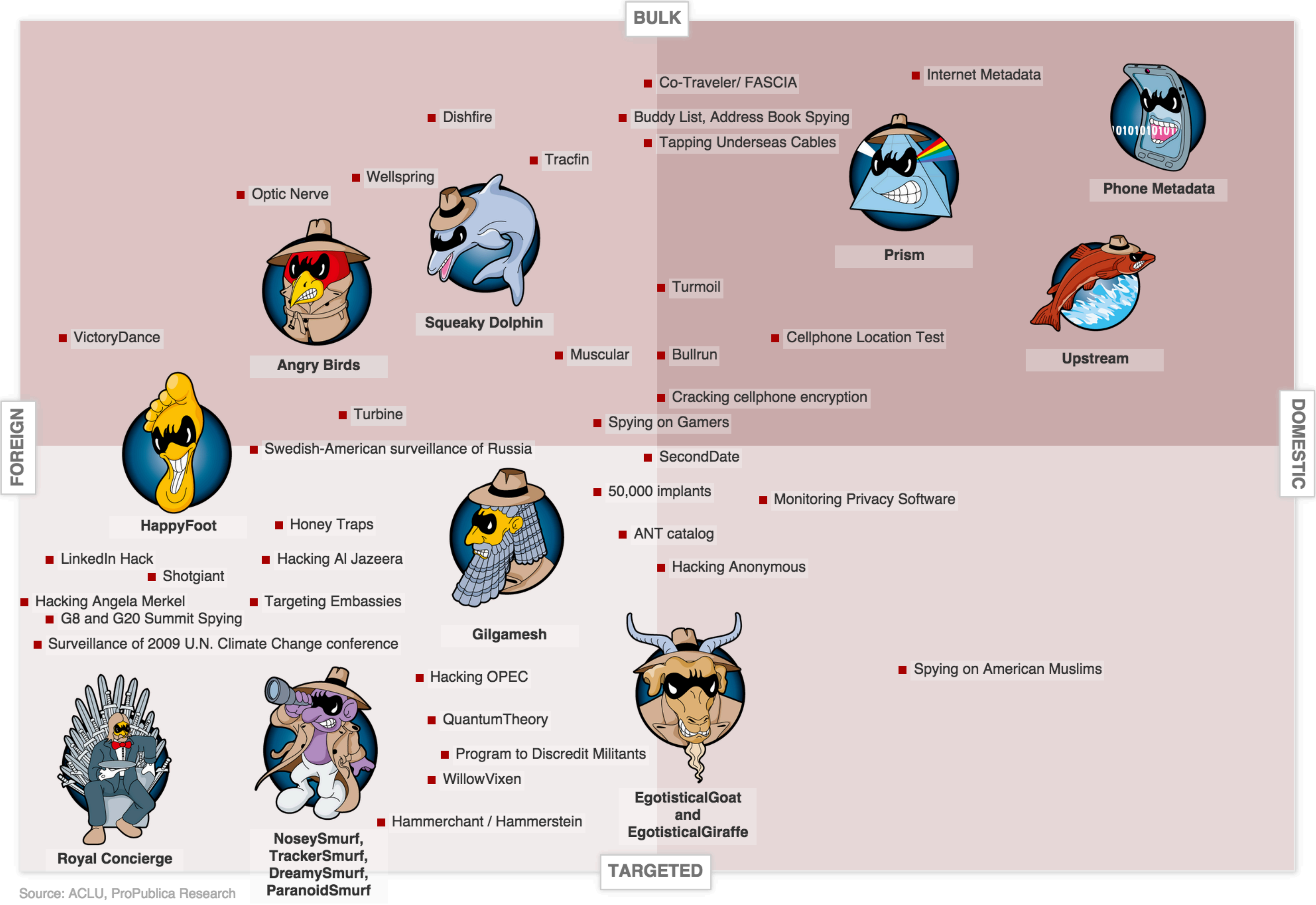


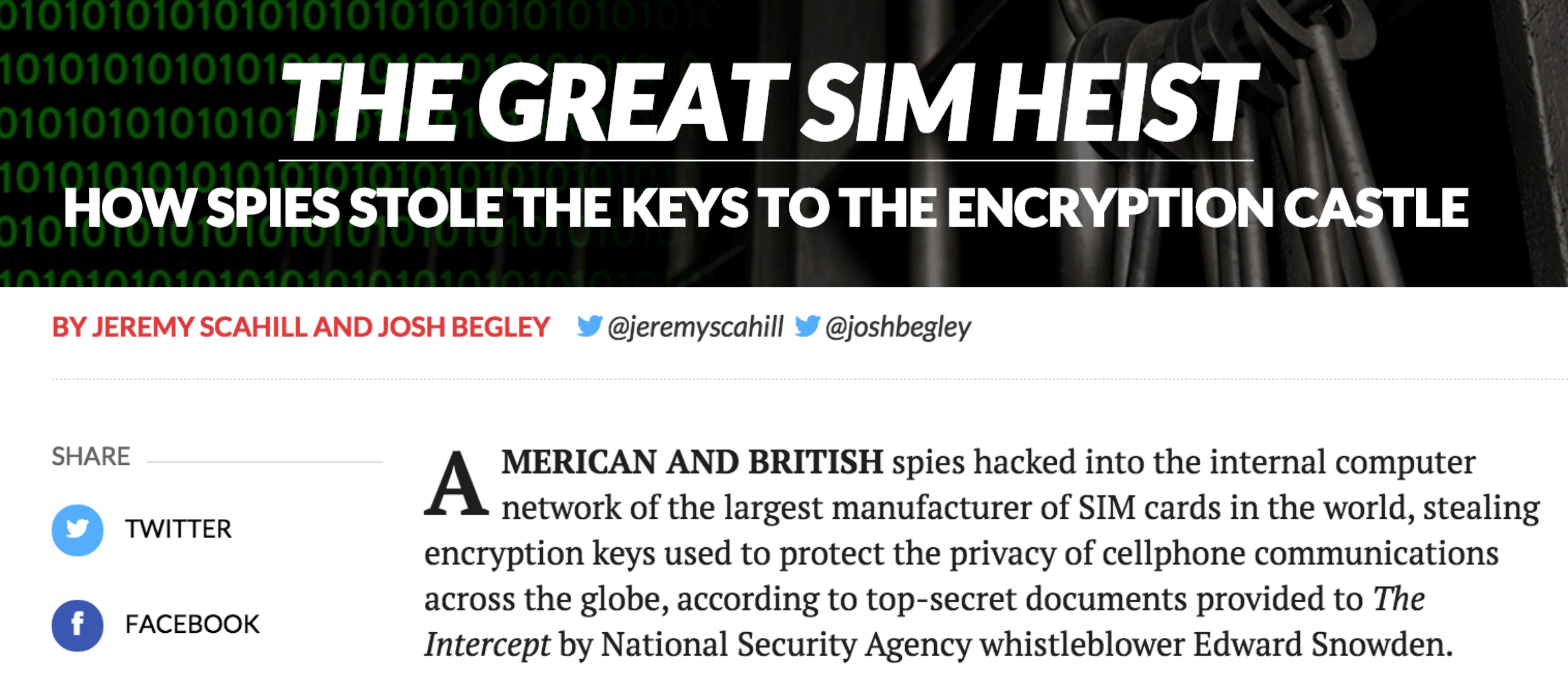
Figure 1: Frequency spectrogram showing various electrical appliances in the home. Washer cycle on (1) and off (2). CFL lamp turning off briefly (3) and then on (4). Note that the TV's (Sharp 42" LCD) EMI shifts in frequency, which happens as screen content changes.

Enev et al.: Televisions, Video Privacy, and Powerline Electromagnetic Interference, CCS 2011

Government Surveillance and Targeted Attacks



Source: ACLU, ProPublica Research



THE GREAT SIM HEIST

HOW SPIES STOLE THE KEYS TO THE ENCRYPTION CASTLE

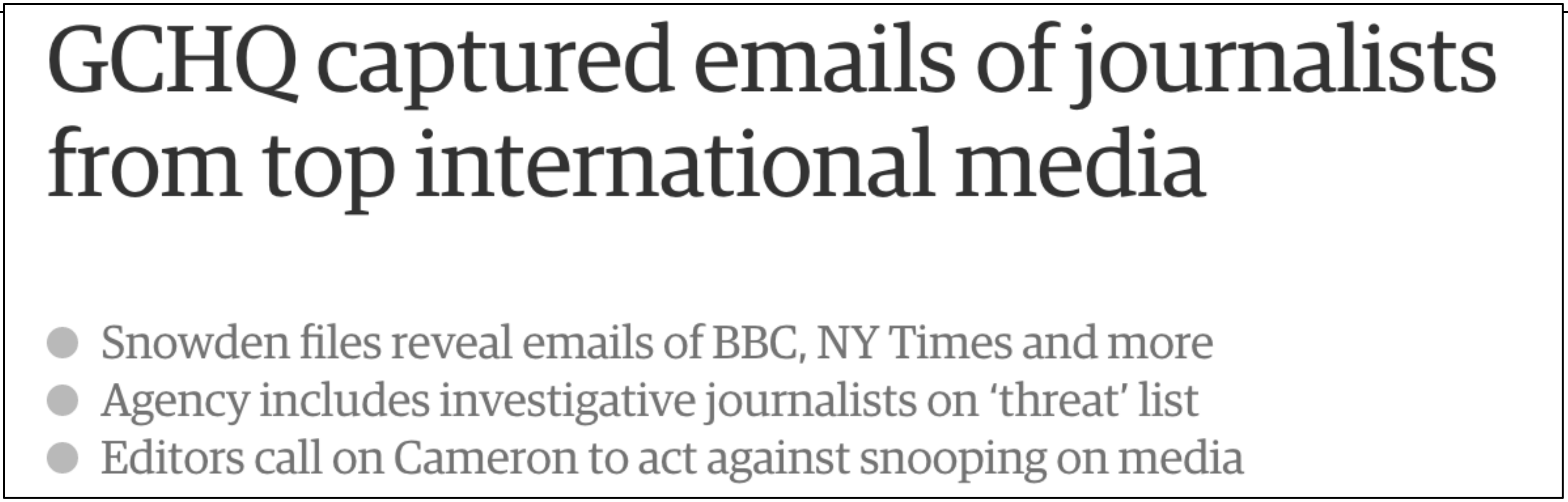
BY JEREMY SCAHILL AND JOSH BEGLEY @jeremyscahill @joshbegley

SHARE

TWITTER

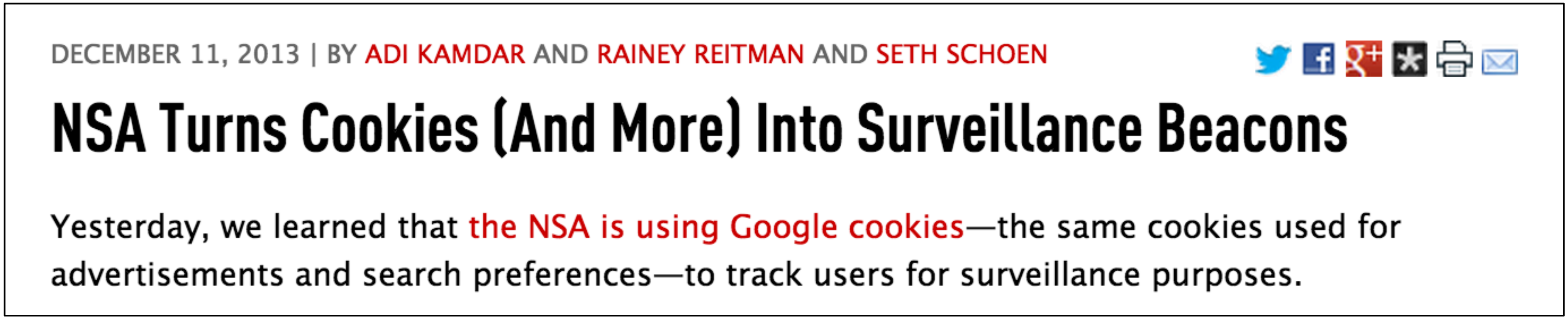
FACEBOOK

AMERICAN AND BRITISH spies hacked into the internal computer network of the largest manufacturer of SIM cards in the world, stealing encryption keys used to protect the privacy of cellphone communications across the globe, according to top-secret documents provided to *The Intercept* by National Security Agency whistleblower Edward Snowden.



GCHQ captured emails of journalists from top international media

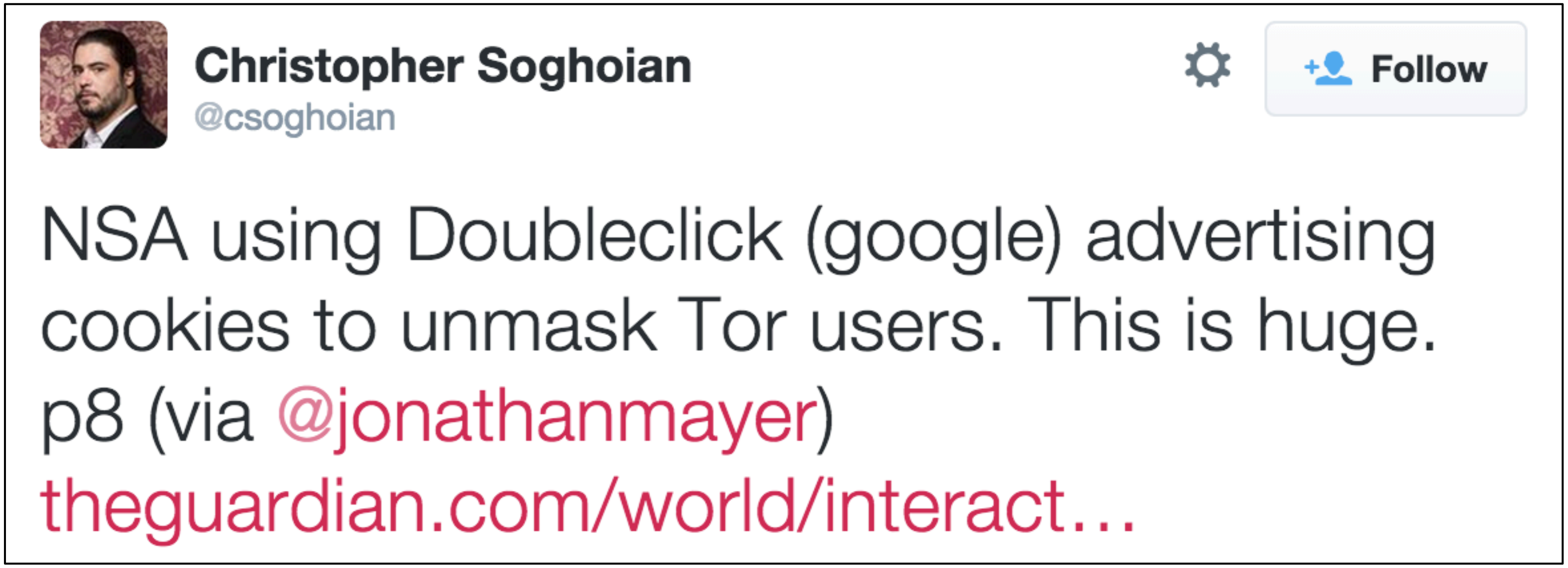
- Snowden files reveal emails of BBC, NY Times and more
- Agency includes investigative journalists on 'threat' list
- Editors call on Cameron to act against snooping on media



DECEMBER 11, 2013 | BY ADI KAMDAR AND RAINEY REITMAN AND SETH SCHOEN

NSA Turns Cookies (And More) Into Surveillance Beacons

Yesterday, we learned that the NSA is using Google cookies—the same cookies used for advertisements and search preferences—to track users for surveillance purposes.

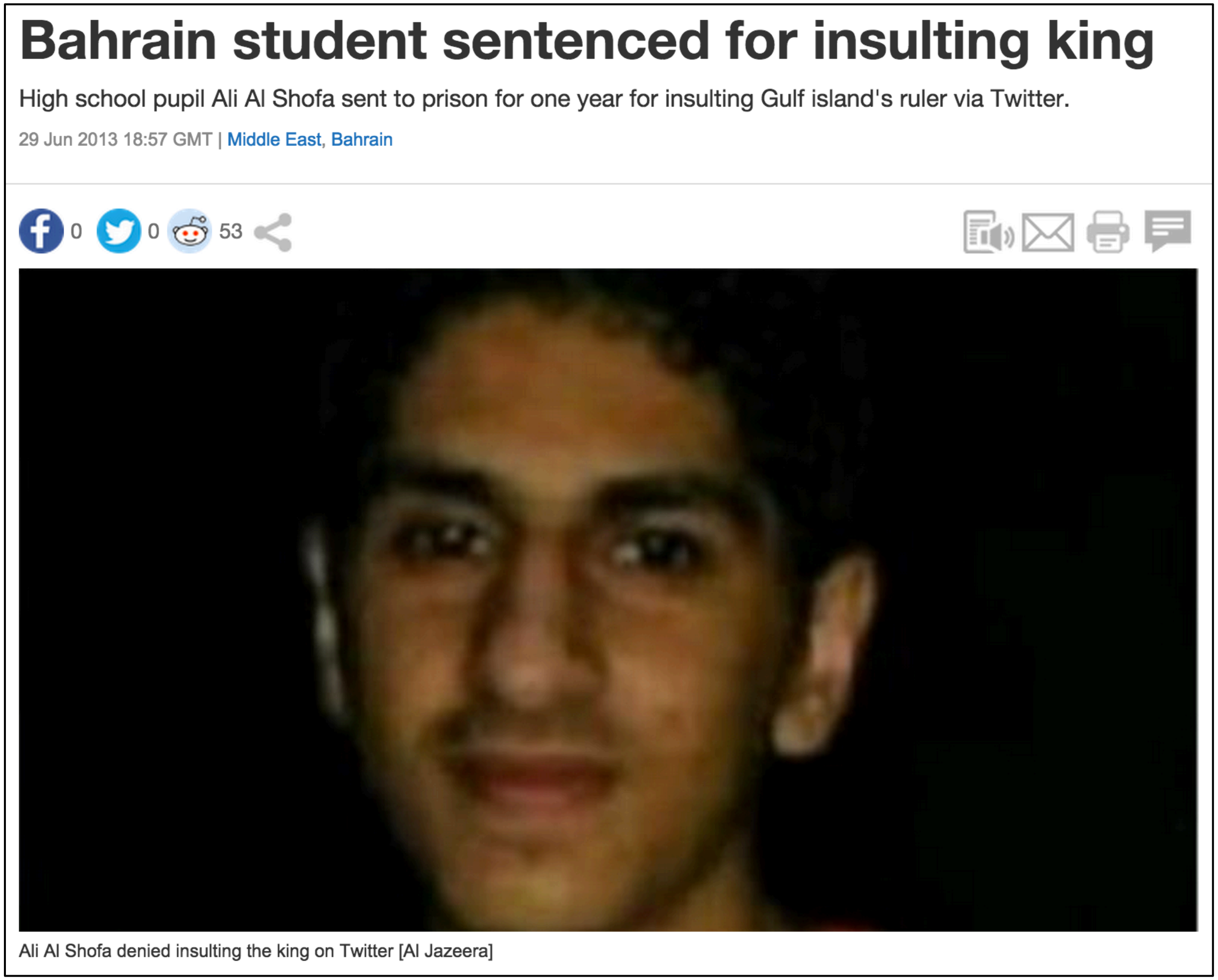


Christopher Soghoian
@csoghoian

NSA using Doubleclick (google) advertising cookies to unmask Tor users. This is huge. p8 (via @jonathanmayer) theguardian.com/world/interact…

[Marczak et al.]

"When Governments Hack Opponents"



Bahrain student sentenced for insulting king

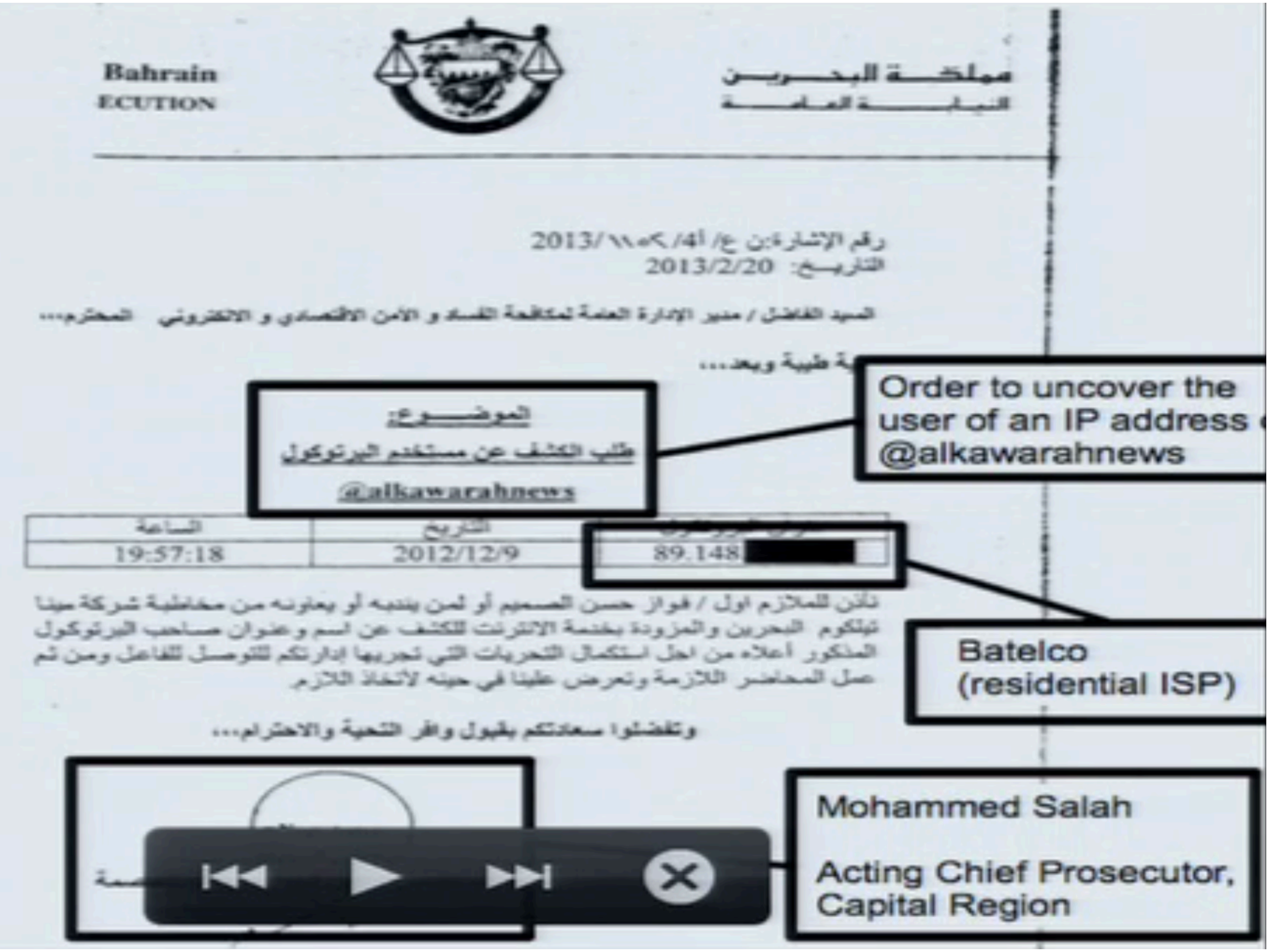
High school pupil Ali Al Shofa sent to prison for one year for insulting Gulf island's ruler via Twitter.

29 Jun 2013 18:57 GMT | Middle East, Bahrain

Ali Al Shofa denied insulting the king on Twitter [Al Jazeera]

[Marczak et al.]

“When Governments Hack Opponents”



Bahrain
ECUTION

مملكة البحرين
النيابة العامة

رقم الإشارة: ن ع/ أ4/ ١١٠٥٧/ 2013
التاريخ: 2013/2/20

السيد الفاضل / مدير الإدارة العامة لمكافحة الفساد و الأمن الاقتصادي و الالكتروني المحترم...

ية طيبة وبعد...

الموضوع:
طلب الكشف عن مستخدم البروتوكول
@alkawarahnews

الساعة	التاريخ	عنوان البروتوكول
19:57:18	2012/12/9	89.148[redacted]

تأذن للملازم اول / فواز حسن الصميم أو لمن ينديه أو يعاونه من مخاطبة شركة مينا
تيلكوم البحرين والمزودة بخدمة الانترنت للكشف عن اسم وعنوان صاحب البروتوكول
المذكور أعلاه من اجل استكمال التحريات التي تجريها إدارتكم للتوصل للفاعل ومن ثم
عمل المحاضر اللازمة وتعرض علينا في حينه لاتخاذ اللازم.

وتفضلوا سعادتكم بقبول وافر التحية والاحترام...

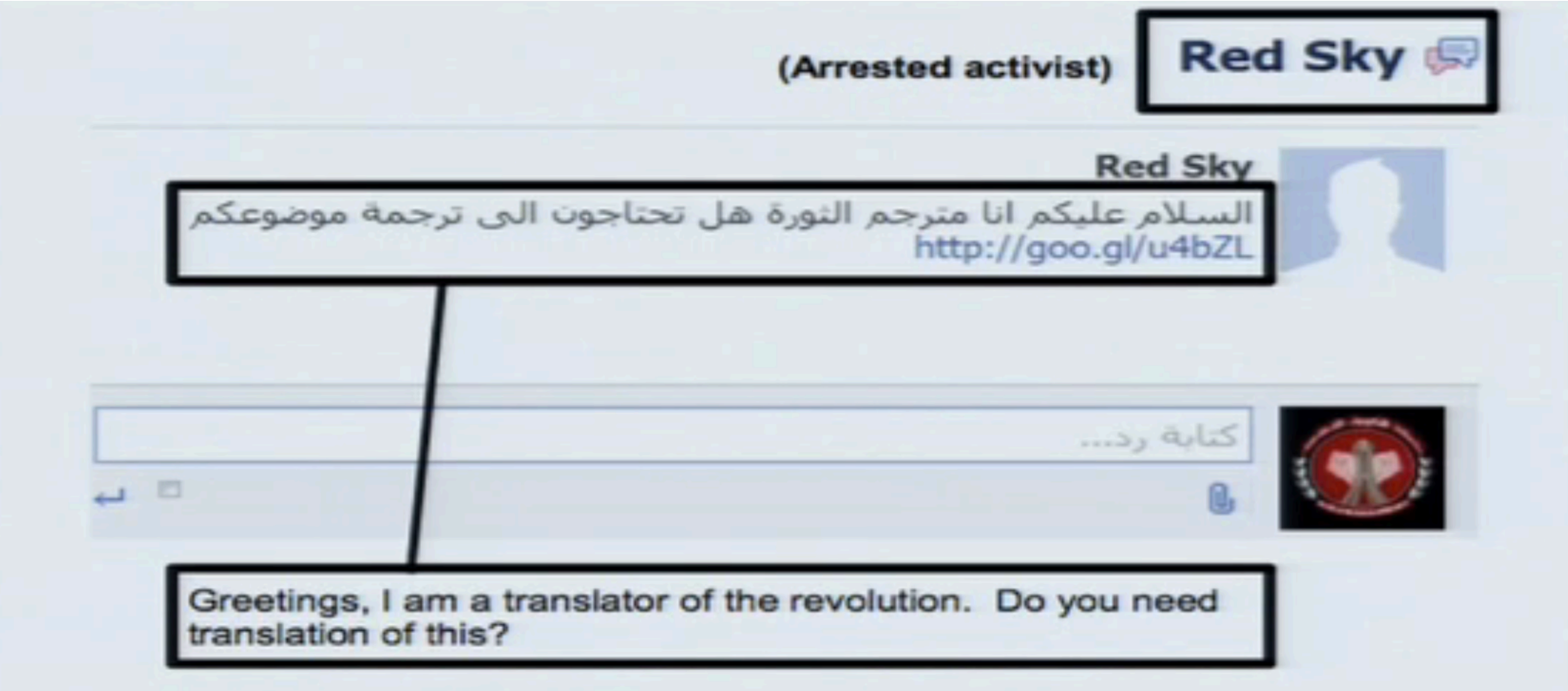
Order to uncover the user of an IP address @alkawarahnews

Batelco (residential ISP)

Mohammed Salah

Acting Chief Prosecutor, Capital Region

"When Governments Hack Opponents"



(Arrested activist)

Red Sky

Red Sky

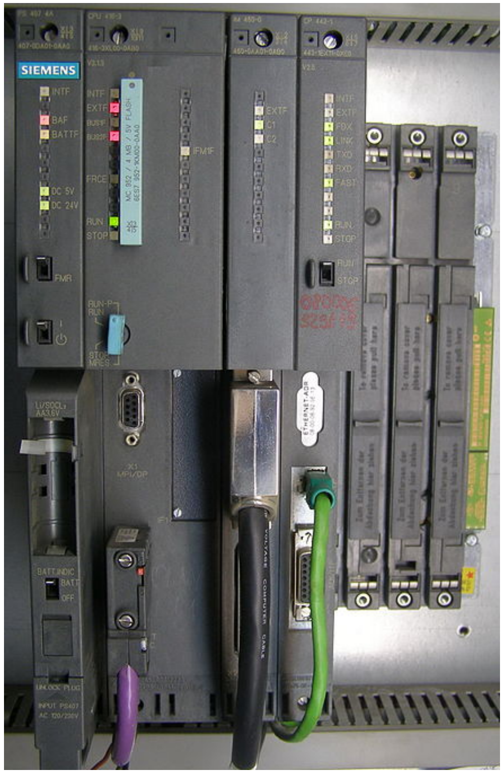
السلام عليكم انا مترجم الثورة هل تحتاجون الى ترجمة موضوعكم
http://goo.gl/u4bZL

كتابة رد...

Greetings, I am a translator of the revolution. Do you need translation of this?

Targeted Attack: Stuxnet (2010)

- Designed to attack industrial systems
- Targeted Windows, exploited **four** zero-days vulnerabilities
- Targeted Iranian nuclear centrifuges
- Introduced to target environment via infected USB stick; spreads but remains inert except in presence of target systems (Siemens S7 PLCs)



Wrap-Up

This Quarter

- Overview of:
  - Security mindset
  - Software security
  - Cryptography
  - Web security
  - Web privacy
  - Malware
  - Mobile platform security
  - Underground ecosystem studies
  - Usable security
  - Anonymity
  - Social engineering
  - Physical security
  - Side channels

Lots We Didn't Cover…

- Deep dive into any of the above topics
- (Most) network security
- (Most) recent attacks/vulnerabilities
- (Most) specific protocols (e.g., Kerberos)
- Spam
- Bitcoin
- Emerging technologies (e.g., AR, wearables, brain-computer interfaces, synthetic biology, …)
- …

Still Interested?

- Yoshi Kohno will be teaching undergraduate cryptography in Winter 2016

- CSE 590Y: graduate research seminar

- Apply to do research in our lab: http://goo.gl/forms/sD40kxIXM6

Thanks for a great quarter!

- Reminders:
  - **Lab 3** due at 5pm today
  - **Extra credit readings** due at 5pm today
  - Stop by my office if you'd like your worksheets back to study for the exam
  - **Office hours:** 1-2pm on Monday, June 8
  - **Final exam:** 8:30-10:20am on Tuesday, June 9
    - 2 sided sheet of notes allowed
  - **Course eval:** https://uw.iasystem.org/survey/146006