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

<table>
<thead>
<tr>
<th>Type</th>
<th>Enc.</th>
<th>Year</th>
<th>Attack description</th>
<th>Victim machine</th>
<th>Samples</th>
<th>Crypt. key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Time-driven [9]</td>
<td>AES</td>
<td>2006</td>
<td>Final Round Analysis</td>
<td>UP</td>
<td>213.0</td>
<td>Full 128-bit key</td>
</tr>
<tr>
<td>Active Time-driven [30]</td>
<td>AES</td>
<td>2005</td>
<td>Prime+Elicit (Synchronous Attack)</td>
<td>SMP</td>
<td>218.9</td>
<td>Full 128-bit key</td>
</tr>
<tr>
<td>Active Time-driven [40]</td>
<td>DES</td>
<td>2003</td>
<td>Prime+Elicit (Synchronous Attack)</td>
<td>UP</td>
<td>226.0</td>
<td>Full 56-bit key</td>
</tr>
<tr>
<td>Trace-driven [14]</td>
<td>AES</td>
<td>2011</td>
<td>Asynchronous Probe</td>
<td>UP</td>
<td>26.6</td>
<td>Full 128-bit key</td>
</tr>
<tr>
<td>Trace-driven [29]</td>
<td>AES</td>
<td>2007</td>
<td>Final Round Analysis</td>
<td>UP</td>
<td>24.5</td>
<td>Full 128-bit key</td>
</tr>
<tr>
<td>Trace-driven [30]</td>
<td>AES</td>
<td>2005</td>
<td>Prime+Probe (Synchronous Attack)</td>
<td>SMP</td>
<td>213.0</td>
<td>Full 128-bit key</td>
</tr>
<tr>
<td>Trace-driven [32]</td>
<td>RSA</td>
<td>2005</td>
<td>Asynchronous Probe</td>
<td>SMT</td>
<td>-</td>
<td>310-bit of 512-bit key</td>
</tr>
</tbody>
</table>

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

Accelerometer Eavesdropping

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

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
Compromising Reflections
Audio from Video

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

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
THE GREAT SIM HEIST
HOW SPIES STOLE THE KEYS TO THE ENCRYPTION CASTLE

BY JEREMY SCAHILL AND JOSH BEGLEY  

A
MERICAN 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
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…
“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]
“When Governments Hack Opponents”
“When Governments Hack Opponents”
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, ...)
• ...

6/5/15
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