Resolved: Owners should be able to eavesdrop on what their devices are saying about them.

Keith Winstein

Stanford Computer Science Department
https://cs.stanford.edu/~keithw
Assistant Professor, Stanford
- Computer Science
- Law (by courtesy)
- Robert N. Noyce Family Faculty Scholar

Research interests:
- Internet video
- congestion control
- network economics
- anonymous aggregation
  - Mosh (mobile shell)
Internet of Things, version 1 (1975)

+ currency, Chinese food, elevators, hot tubs, ...
Since December 15, 1999 (start of current logs):

There have been 4291 cans purchased.

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Drink</th>
<th>Purchasers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1355</td>
<td>dietcoke</td>
<td>davidmit: 571, manual: 312, tk: 207, bob: 164</td>
</tr>
<tr>
<td>661</td>
<td>coke</td>
<td>davidmit: 138, bianca: 114, cph: 58, thomer: 45</td>
</tr>
<tr>
<td>493</td>
<td>mtdew</td>
<td>manual: 344, keithw: 103, matthewf: 10, jered: 8</td>
</tr>
<tr>
<td>293</td>
<td>nestea</td>
<td>manual: 200, coho: 21, keithw: 19, rfrankel: 8</td>
</tr>
<tr>
<td>254</td>
<td>punch</td>
<td>manual: 119, keithw: 72, rweiss: 34, davidmit: 8</td>
</tr>
<tr>
<td>125</td>
<td>mystery</td>
<td>manual: 96, davidmit: 8, jered: 5, jakebeal: 5</td>
</tr>
<tr>
<td>70</td>
<td>sprite</td>
<td>keithw: 28, manual: 12, jakebeal: 10, rweiss: 6</td>
</tr>
<tr>
<td>23</td>
<td>cherrycoke</td>
<td>manual: 18, keithw: 3, jakebeal: 1, davidmit: 1</td>
</tr>
<tr>
<td>21</td>
<td>dietpepsi</td>
<td>davidmit: 14, bob: 3, manual: 3, philg: 1</td>
</tr>
</tbody>
</table>

Your privacy-unconcerned Coke Czars,
Keith & Dave
Auto-ID Labs

The Leading Academic Research Network on the Internet of Things
RFID system (2003)

- Motorola FlexSecur
- “end-to-end encryption”
- “challenge-response”
Anklebiters with an oscilloscope
Clone four cards
Meanwhile, consumer software meets the Internet...

- Explosion of the Internet
- “Patch Tuesday” (2003)

**Truism**

 Anything connected to the Internet needs to be patched regularly to fix bugs, or it becomes vulnerable to vandals who will break in and commandeer it to their own ends.
Google partners with manufacturers and carriers to speed up Android updates

Are you sick and tired of waiting for your carrier or phone manufacturer to roll out the latest updates?
Google's Android Update Alliance Is Already Dead

BY JAMIE LENDINO  DECEMBER 16, 2011  156 COMMENTS

Numerous phone vendors and U.S. carriers pledged that Android 4.0 (Ice Cream Sandwich) upgrades would be available for all new devices for at least 18 months, but they're already going back on their word.

At the Google I/O conference in May, many Android phone vendors and U.S. wireless carriers made a long-awaited promise: From then on, any new Android phone would receive timely OS
Android users outraged over Motorola's broken promise

Company conceives some customers got "a raw deal" in decision not to upgrade 2011 flagship devices to Ice Cream Sandwich.

by Casey Newton and Roger Cheng / October 5, 2012 2:40 PM PDT
Manages half your home’s energy.

TAKA A TOUR WITH NEST
Manufacturer economics

- Makers of $500 smartphones lose interest after 6 months
- What about a $50 or $5 device?
- ... that stays in your house for 7 years?
Lambs to the slaughter

- Smart fridge barcode scanner
- Hertz camera
- Toaster
- Light bulb botnet
Independent checks serve an important role

Google (2012)

“Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the opt-out cookie.”
Stanford student (J. Mayer) eavesdrops on his PC...
This is a big deal

- Federal penalty (2012): $22.5 million
- State penalty (2013): $17 million
- Class-action consumer lawsuit: ???
- Europe: ???
The big difference today

Anklebiters

No UI to eavesdrop.
Communications are end-to-end signed/encrypted.
Checks and balances

Expecting any one component to be the bulwark of its own security, by itself, dependent on a manufacturer’s aftermarket benevolence and interest, is a recipe for regret.
Defense in depth
Defense in depth
Layers of security
Proposed architecture

Allow market for intrusion-prevention systems that can:

▷ inspect
▷ audit
▷ interdict
▷ modify

...communications to/from their devices.
Read-only monitor
Read-only monitor
We need new crypto construction
Final thoughts

Academy’s role

Let’s give the industry the tools to enable independent checks and anklebiters in the IoT.

Resolved

Owners should be able to eavesdrop on what their devices are saying about them.