Trust but Verify: Auditing Secure Internet of Things Devices

Keith Winstein

Assistant Professor of Computer Science
Assistant Professor of Law (by courtesy)

Joint work with Judson Wilson, Riad S. Wahby, Henry Corrigan-Gibbs, Dan Boneh, Philip Levis.

Stanford University

Most communications applications are built on **one venerable abstraction**:

Venerable abstraction

An **end-to-end inviolable** channel **between two endpoints**

Venerable abstraction

An **end-to-end inviolable** channel **between two endpoints**

- Bluetooth API provides it (app to device)

Venerable abstraction

An **end-to-end inviolable** channel **between two endpoints**

- Bluetooth API provides it (app to device)
- TCP provides it (app to app)

Venerable abstraction

An **end-to-end inviolable** channel **between two endpoints**

- Bluetooth API provides it (app to device)
- TCP provides it (app to app)
- TLS enforces it (no more Web caches)

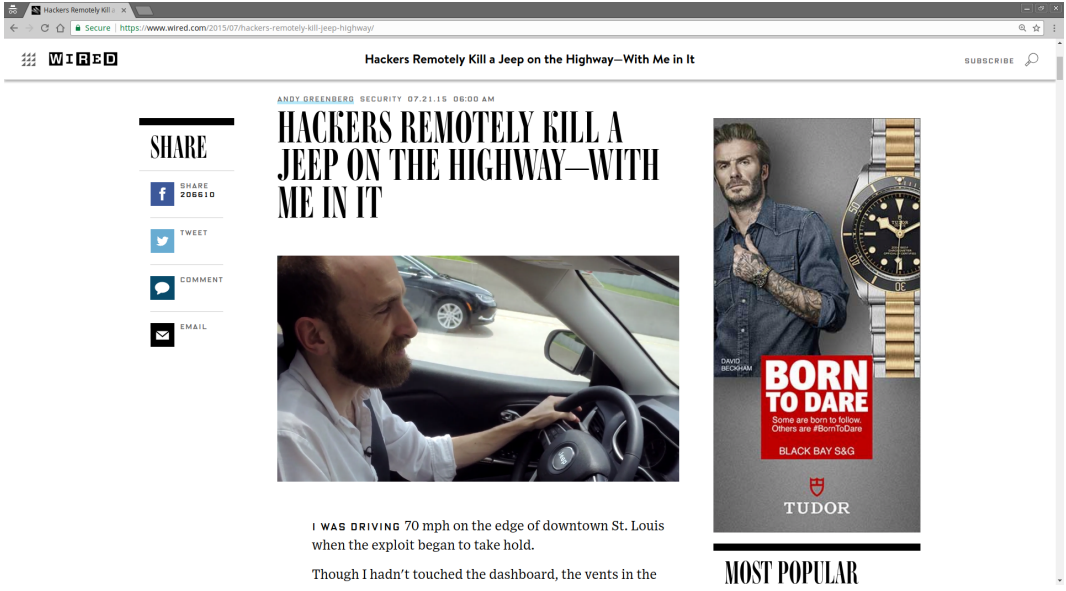
Venerable abstraction

An **end-to-end inviolable** channel **between two endpoints**

- Bluetooth API provides it (app to device)
- TCP provides it (app to app)
- TLS enforces it (no more Web caches)
- QUIC and Mosh enforce it even for control information (no more accelerators)

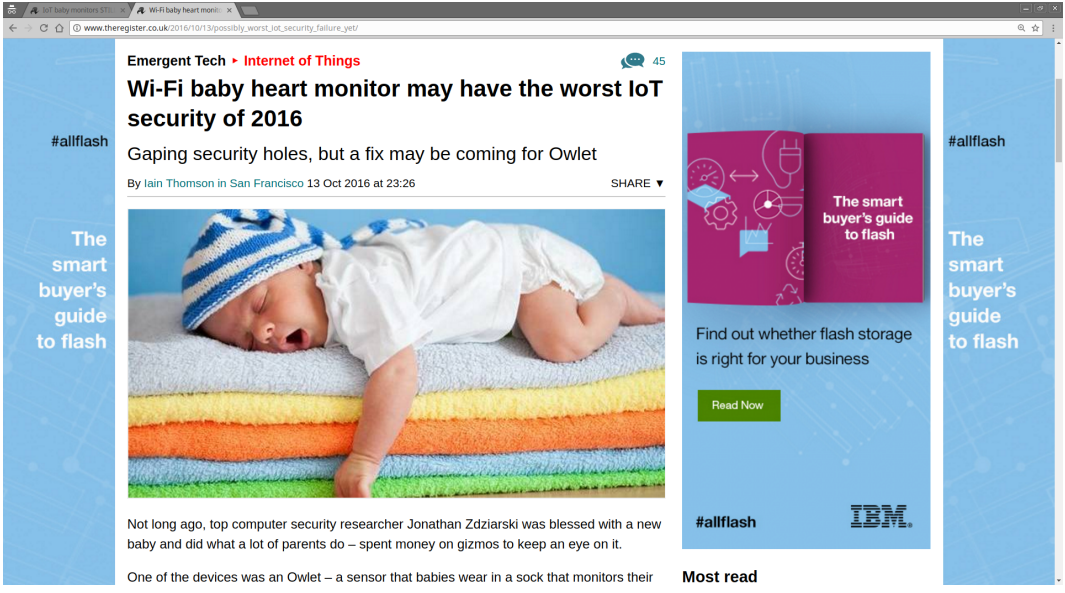
- The Internet owes much of its success to the view that the network should avoid meddling in endpoints' affairs.
- Traditional view: "The endpoints are the principals."
- But...

Connectivity creates new risks (car)



Connectivity creates new risks (baby monitor I)

Connectivity creates new risks (baby monitor II)



Connectivity creates new risks (camera)

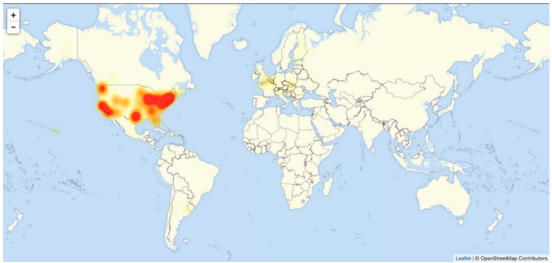
Secure | https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?mcubz=0

TECHNOLOGY | Hackers Used New Weapons to Disrupt Major Websites Across U.S.

Subscribe

Hackers Used New Weapons to Disrupt Major Websites Across U.S.

By NICOLE PERLROTH OCT. 21, 2016



A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com.

SAN FRANCISCO — Major websites were inaccessible to people across wide swaths of the United States on Friday after a company that manages crucial parts of the internet's infrastructure said it was under attack.

Connectivity creates new risks (camera)

SECTIONS HOME SEARCH The New York Times keithw

POLITICS

A New Era of Internet Attacks Powered by Everyday Devices

By DAVID E. SANGER and NICOLE PERLROTH OCT. 22, 2016

WASHINGTON — When surveillance cameras began popping up in the 1970s and '80s, they were welcomed as a crime-fighting tool, then as a way to monitor traffic congestion, factory floors and even baby cribs. Later, they were adopted for darker purposes, as authoritarian governments like China's used them to prevent challenges to power by keeping tabs on protesters and dissidents.

But now those cameras — and many other devices that today are connected to the internet — have been commandeered for an entirely different purpose: as a weapon of mass disruption. The internet slowdown that swept the East Coast on Friday, when many Americans were already jittery about the possibility that hackers could interfere with election systems, offered a glimpse of a new era of vulnerabilities confronting a highly connected society.

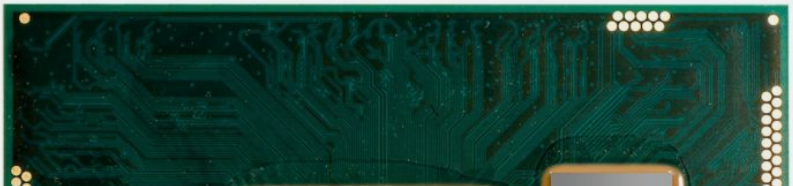
Connectivity creates new risks (computer)

RISK ASSESSMENT —

Intel patches remote hijacking vulnerability that lurked in chips for 7 years

Flaw in remote management feature gives attackers a way to breach networks.

DAN GOODIN - 5/1/2017, 4:55 PM



Connectivity creates new risks (videogame machine)

Forbes

MAY 23, 2011 @ 10:36 AM 6,698

Sony Pegs PSN Attack Costs at $170 Million, $3.1B Total Loss for 2011

Paul Tassi, CONTRIBUTOR

News and opinion about video games, technology and the internet

FULL BIO

Opinions expressed by Forbes Contributors are their own.

Just how much does it cost a company which has had its security hacked and the personal info of every one of its customers leaked? Well now we have some idea, as Sony has somehow or another come up with an official figure of just how much the PSN attacks have cost them.

The grand total? $170M. At least that's what they said in an official earnings forecast statement today:

Connectivity creates new risks (doll)

Germany Issues Kill Or...

Secure | https://www.wsj.com/articles/germany-issues-kill-order-for-a-domestic-spycayla-the-toy-doll-1492098755

A-HED

Germany Issues Kill Order for a Domestic Spy—Cayla the Toy Doll

On a campaign to promote digital privacy, authorities warn that "My Friend Cayla" makes children vulnerable to malicious surveillance—parents who fail to destroy the doll face a €25,000 fine; 'destroy it with a hammer'

By *Andrea Thomas*

April 13, 2017 11:52 a.m. ET

44 COMMENTS

BERLIN—Earlier this year, Lisa Harmann received a warning from the German government: A spy might be lurking in her child's bedroom. She should find it and destroy it.

With their 10-year-old daughter sound asleep, Ms. Harmann and her husband sneaked into the room armed with a flashlight and soon found the culprit sitting inside the cupboard, sporting a frozen smile and billowing pink skirt.

Despite her innocent looks, "My Friend Cayla" isn't a doll—at least not in the eyes of German authorities—but an illegal eavesdropping device. On Feb. 17, after a lengthy investigation, the Federal Network Agency, Germany's top telecommunications watchdog, issued an order to parents to find Cayla and destroy her. It also banned its sale, purchase and ownership.

"It's about the protection of the weakest in our society," said Jochen Homann, president of the body known as Bundesnetzagentur.

Privacy may be eroding around the world, but not in Germany, where encroachment is met with the kind of treatment reserved

Connectivity creates new risks (television)

TV Maker Vizio to Pay

gizmodo.com/tv-maker-vizio-to-pay-out-millions-after-secretly-colle-1792056140

Want Gizmodo's email newsletter?

Add your email address

Subscribe

You may also like

The Garage

Here's What Happened When I Drove 500 Miles To Pick Up A Free Car

Yesterday 5:20pm

TV Maker Vizio to Pay Out Millions After Secretly Collecting Customer Data

Libby Watson

2/06/17 6:09pm · Filed to: PRIVACY

64.1K 179 9

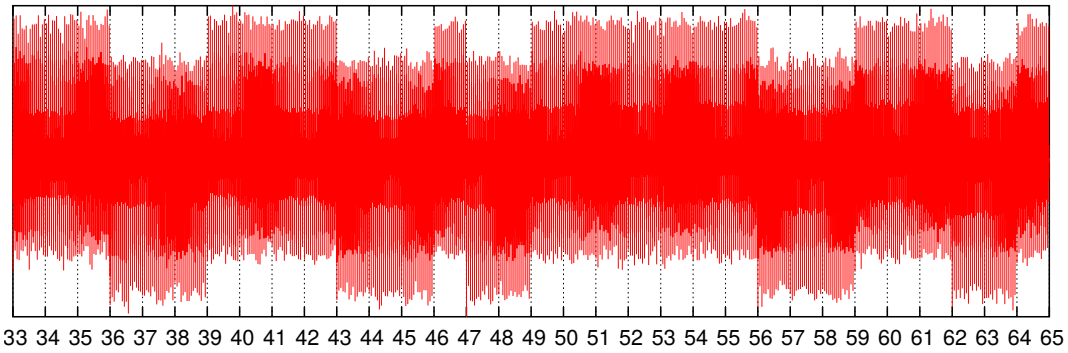
The Federal Trade Commission announced today that it has reached a settlement with Vizio, which it alleged misled customers about what data its smart TVs were collecting. Vizio agreed to pay $2.2 million in penalties, including $1.5 million to the FTC and $1 million to the New Jersey Division of Consumer Affairs, with $300,000 suspended.

Share Tweet

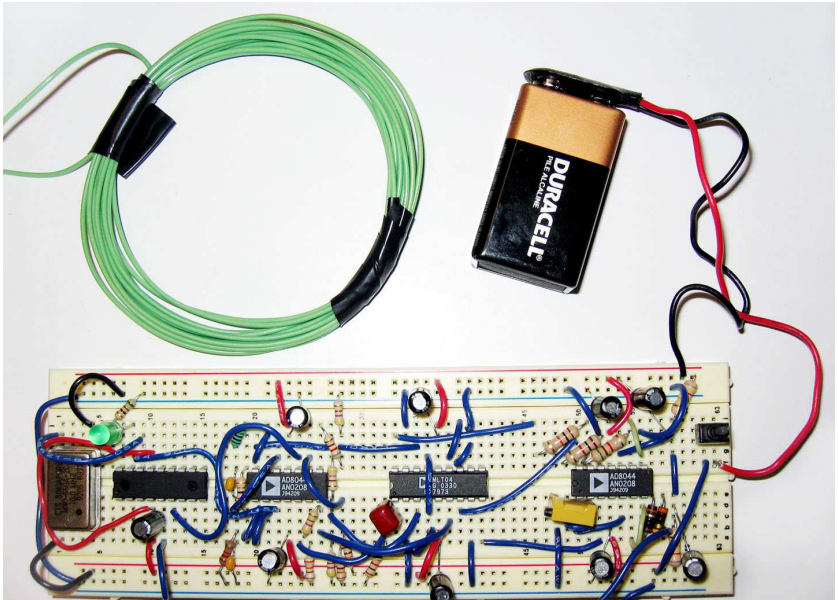
RFID system (2003)

- 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 wit

androidandme.com/2011/05/news/google-partners-with-n

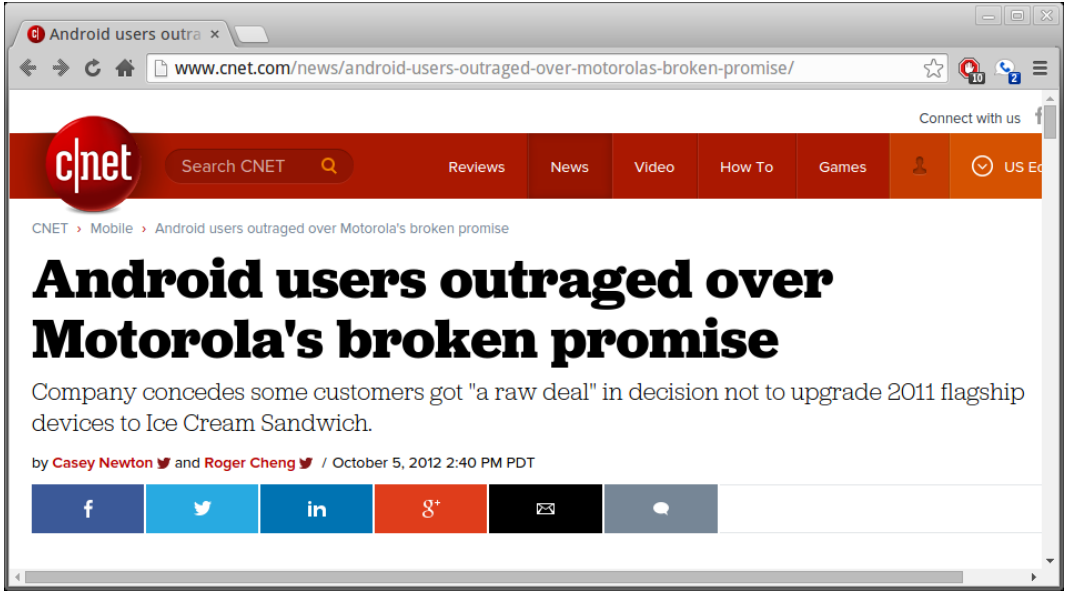
Google partners with manufacturers and carriers to speed up Android updates

Google's Android Update Alliance Is Already Dead

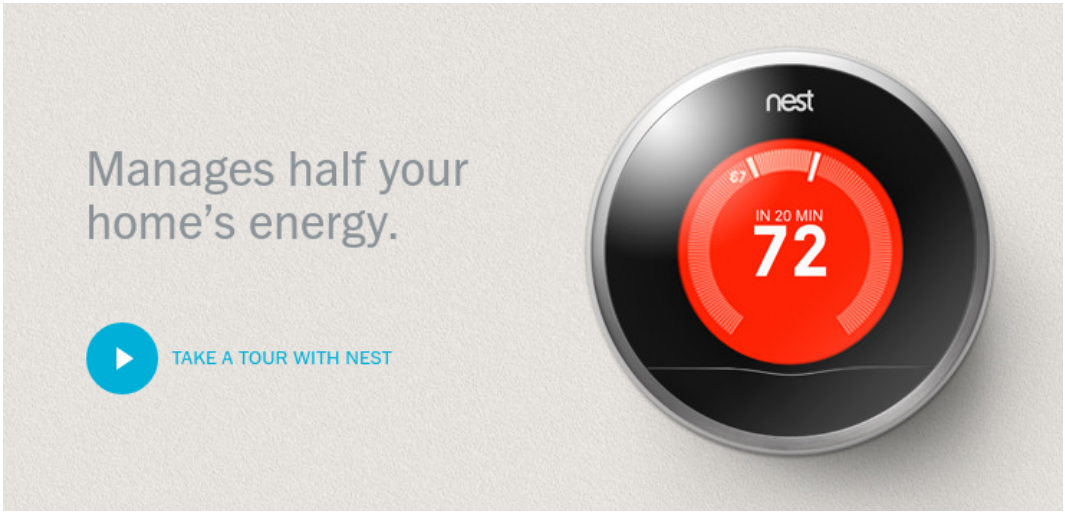
BY JAMIE LENDINO DECEMBER 16, 2011 156 COMMENTS

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 outra
www.cnet.com/news/android-users-outraged-over-motorolas-broken-promise/
Connect with us
c|net
Search CNET
Reviews
News
Video
How To
Games
US Ed
CNET › Mobile › Android users outraged over Motorola's broken promise
Android users outraged over Motorola's broken promise
Company concedes 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

Internet of Things, version 3 (201x–)



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?

Robustness in the Large

"Biodiversity" is valuable to prevent the systemic exposure from any monoculture of devices—or software components—growing too widespread.

The IoT, as it is played

Alphabet

Alphabet

The IoT, as it is played

Apple

Apple

The IoT, as it is played

The IoT, as it is played

Some Random Manufacturer

Some Random Manufacturer

The IoT, as it is played

Voting Machine

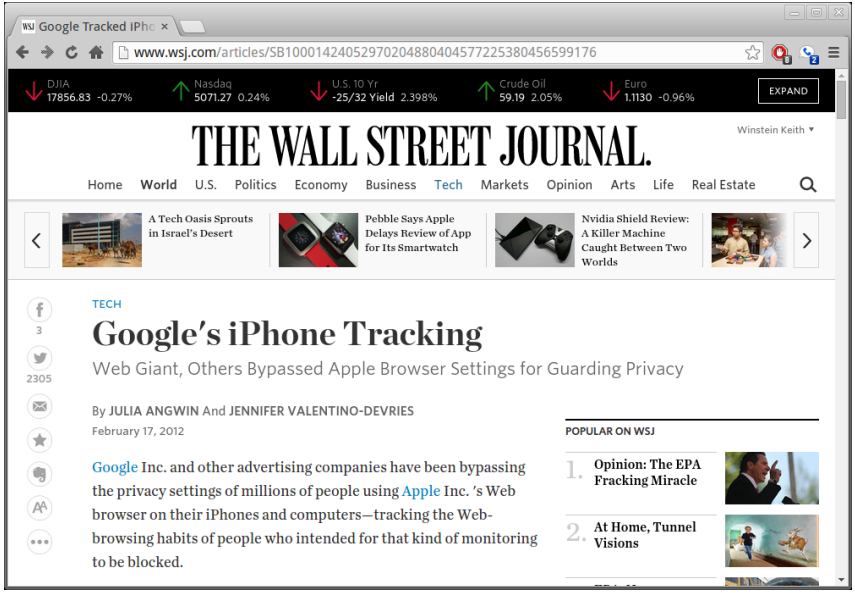
Vladimir Putin

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 way for owner to eavesdrop.
Communications are end-to-end signed/encrypted.
Also true of Android $\geq$ 7.0 (2016)!

The hierarchy of security bugs

- Bugs that exist
- Bugs that somebody has discovered
- Bugs that somebody has told the manufacturer about
- Bugs the manufacturer has fixed correctly
- Bugs where a fix is available for my device
- Bugs where the fix has been installed on my device

The risks of end-to-end secure communications

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.

Nightmare scenarios

- Light bulb botnet [← this one came true]
- Smart fridge barcode scanner
- Alexa—how do we know that the light correctly indicates recording?

Robustness in the Small

Independent "layers of security"—watchers watching watchers within the home—can prevent any single device from being the bulwark of its own security.

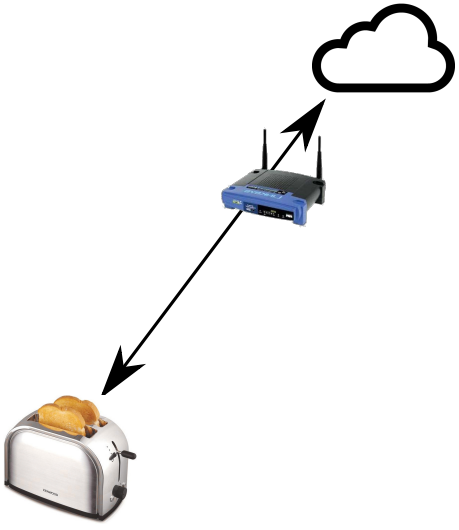
Proposed architecture

Allow market for **intrusion-detection systems** that can:

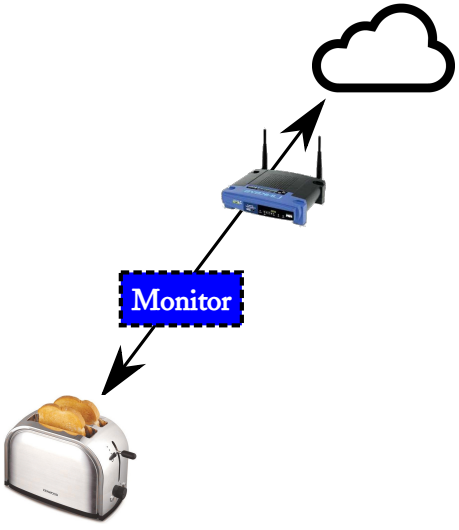
- inspect
- audit
- interdict
- ~~modify~~

. . . communications to/from their devices.

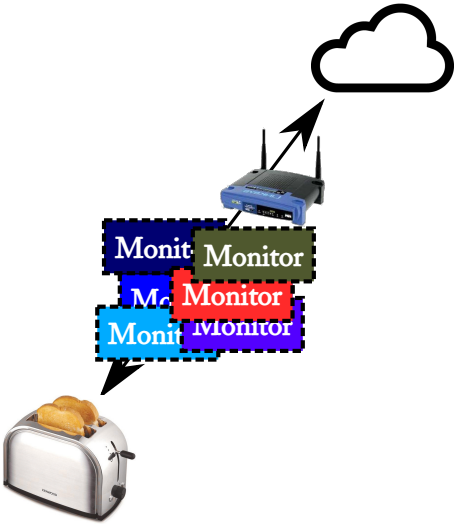
Read-only monitor**s** watching each other



Read-only monitor**s** watching each other



Read-only monitors watching each other



One way to do it

1. User tells Google, "My auditor wants to inspect the last minute of traffic."
2. Google rotates the key on the thermostat-Google connection.
3. **After rotation is complete**, thermostat shares old (superseded) key with auditor.
4. Auditor uses key to decrypt old ciphertext.

"Perfect" Forward Secrecy

Level 1:

A: "Please delete the keys."

Level 2:

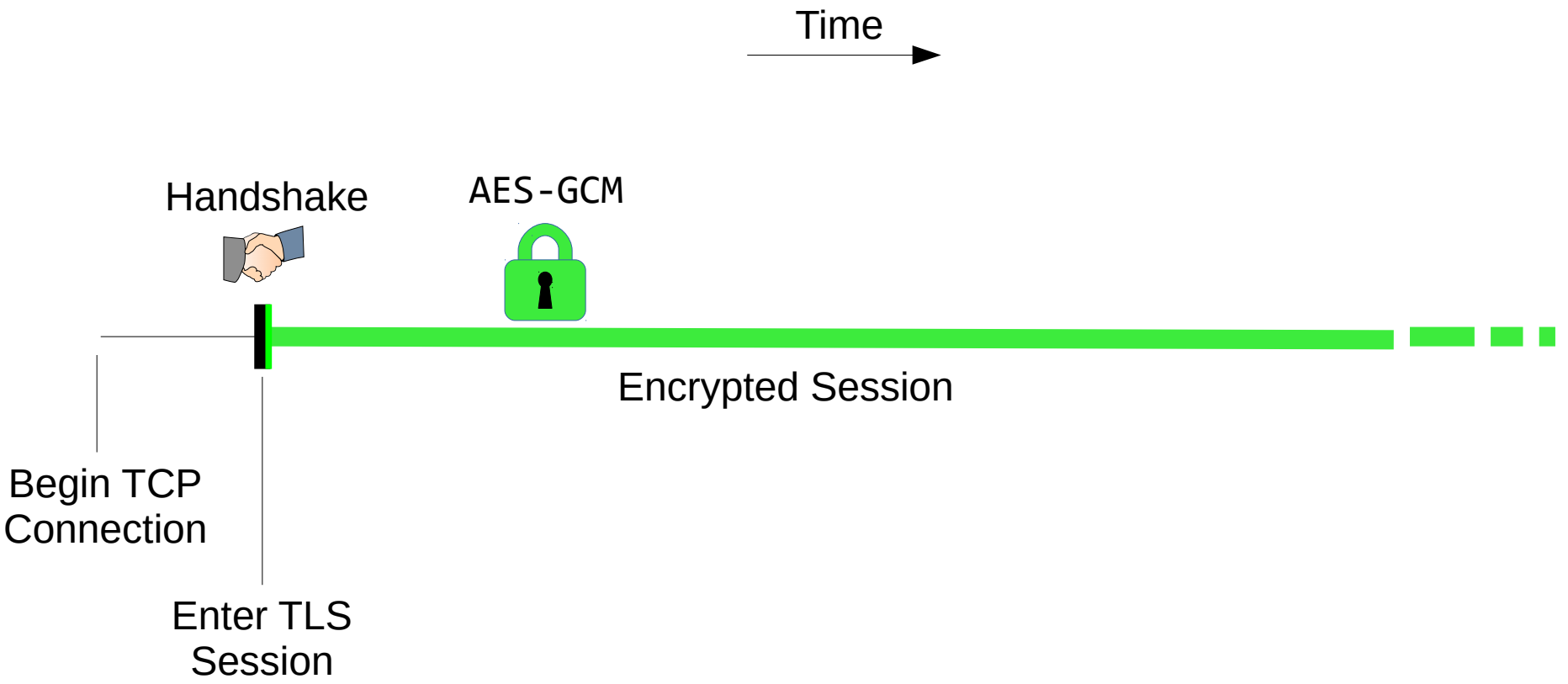
A: "Please delete the keys."
B: "Okay, I deleted the keys."

Level 3:

A: "Please delete the keys."
B: "Here is a proof that I deleted the keys."

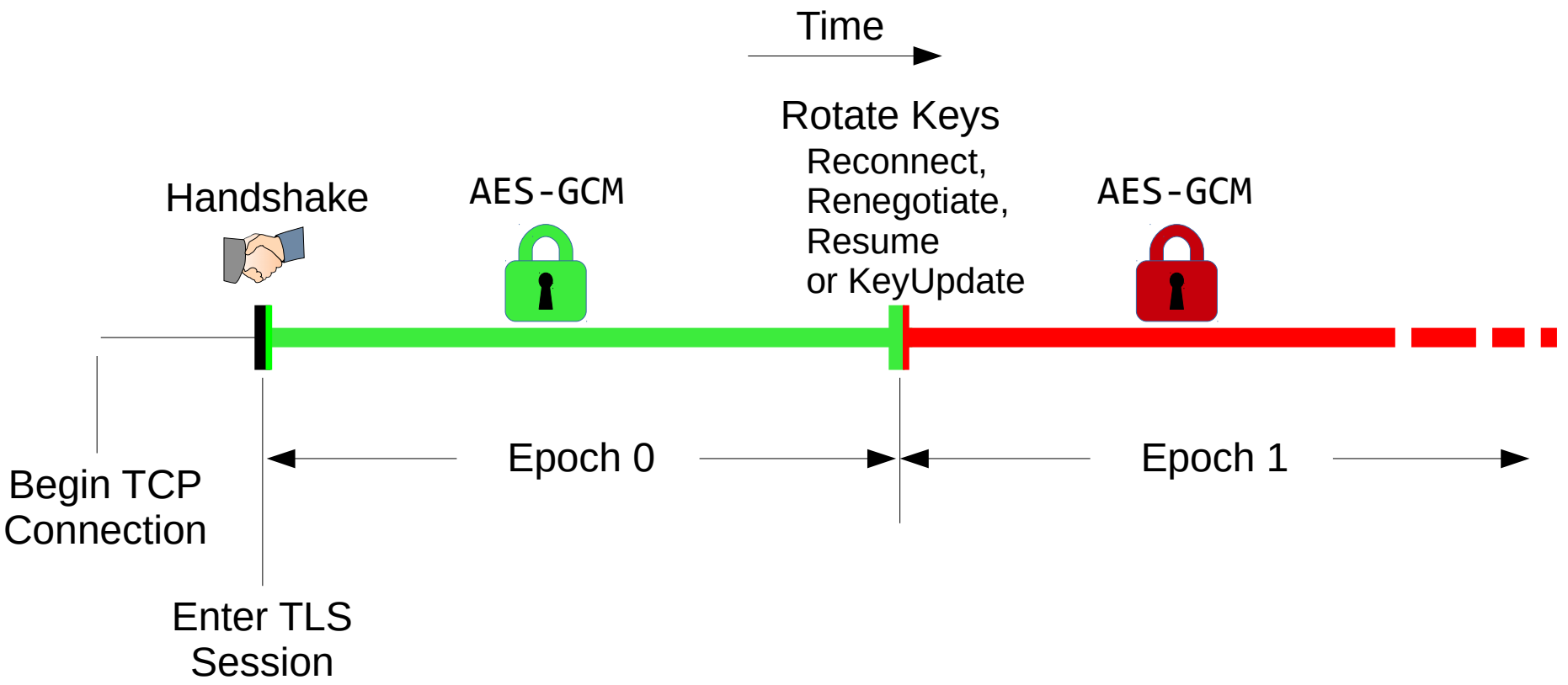
Solution: TLS-RaR

A standard TLS connection...



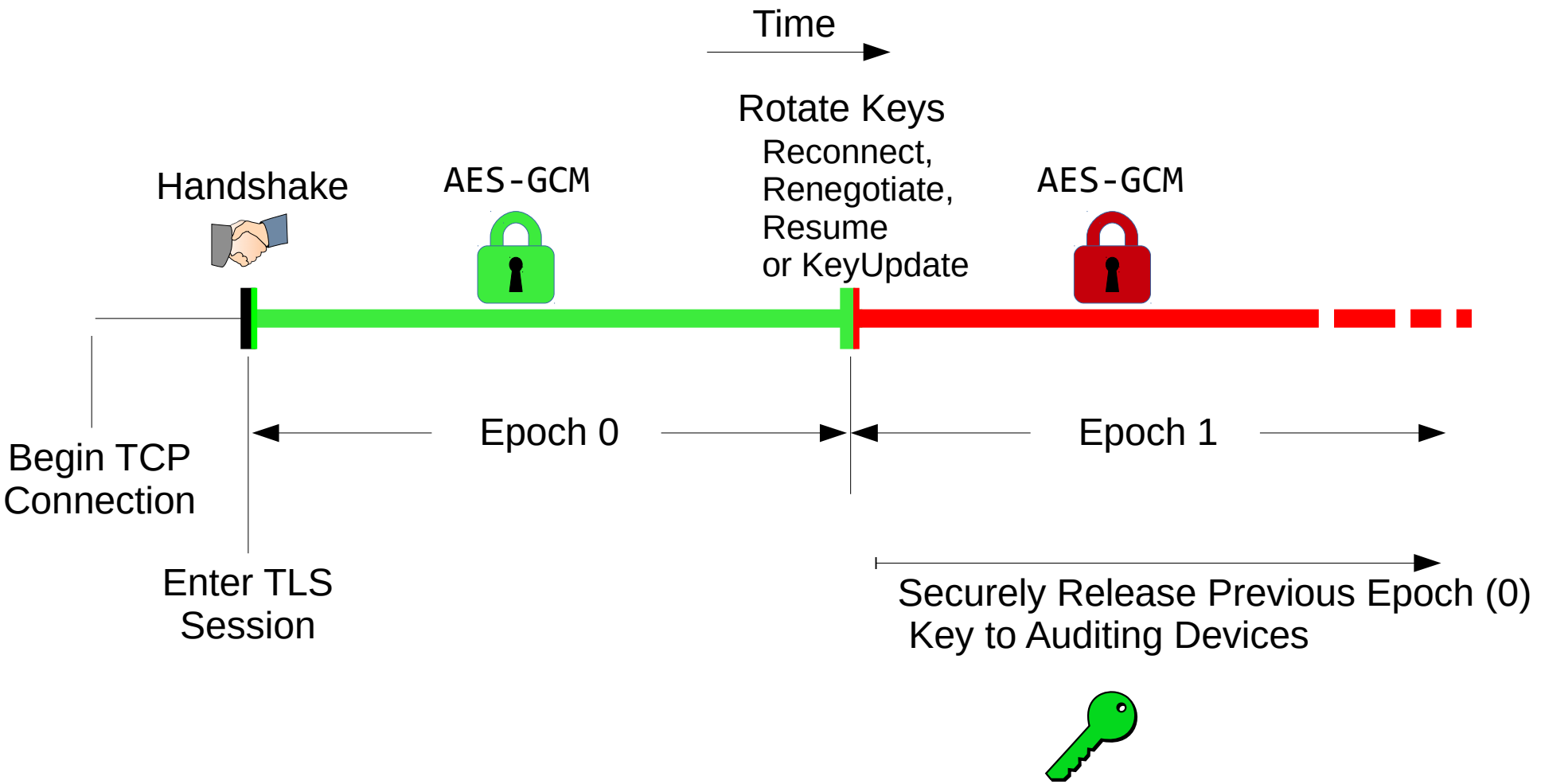
Solution: TLS-RaR

Use standard TLS features to **R**otate keys,



Solution: TLS-RaR

Use standard TLS features to **R**otate keys, **a**nd then securely **R**elease the previous keys to auditing devices.



Nice Properties

- **End-to-end integrity is preserved! (Unlike MITM)**
  - ➔ Guaranteed tamper-proof communication.

Nice Properties

- **End-to-end integrity is preserved! (Unlike MITM)**
  - Guaranteed tamper-proof communication.
- Audit box's decryption yields the same stream of data as endpoints' `SSL_read()` calls, but delayed
  - Audit matches what was received

Nice Properties

- **End-to-end integrity is preserved! (Unlike MITM)**
  - ➔ Guaranteed tamper-proof communication.
- Audit box's decryption yields the same stream of data as endpoints' `SSL_read()` calls, but delayed
  - ➔ Audit matches what was received
- Format of TLS on the wire is not changed
  - ➔ Easy to reason about security of the protocol

Nice Properties

- **End-to-end integrity is preserved! (Unlike MITM)**
  - Guaranteed tamper-proof communication.
- Audit box's decryption yields the same stream of data as endpoints' `SSL_read()` calls, but delayed
  - Audit matches what was received
- Format of TLS on the wire is not changed
  - Easy to reason about security of the protocol
- For some existing servers no change is necessary
  - Really easy to adopt

Nice Properties

- **End-to-end integrity is preserved! (Unlike MITM)**
  - → Guaranteed tamper-proof communication.
- Audit box's decryption yields the same stream of data as endpoints' `SSL_read()` calls, but delayed
  - → Audit matches what was received
- Format of TLS on the wire is not changed
  - → Easy to reason about security of the protocol
- For some existing servers no change is necessary
  - → Really easy to adopt
- Minimal change to OpenSSL on the device
  - → Easy to reason about security of the implementation
  - → Easy to adopt

Nice Properties

- **End-to-end integrity is preserved! (Unlike MITM)**
  - Guaranteed tamper-proof communication.
- Audit box's decryption yields the same stream of data as endpoints' `SSL_read()` calls, but delayed
  - Audit matches what was received
- Format of TLS on the wire is not changed
  - Easy to reason about security of the protocol
- For some existing servers no change is necessary
  - Really easy to adopt
- Minimal change to OpenSSL on the device
  - Easy to reason about security of the implementation
  - Easy to adopt

Trust but Verify: Auditing the Secure Internet of Things

Judson Wilson Riad S. Wahby Henry Corrigan-Gibbs
Dan Boneh Philip Levis Keith Winstein
{judsonw, rsw, henrycg, dabo, pal, keithw}@cs.stanford.edu
Stanford University

ABSTRACT

Internet-of-Things devices often collect and transmit sensitive information like camera footage, health monitoring data, or whether someone is home. These devices protect data in transit with end-to-end encryption, typically using TLS connections between devices and associated cloud services.

But these TLS connections also prevent device owners from observing what their own devices are saying about them. Unlike in traditional Internet applications, where the end user controls one end of a connection (e.g., their web browser) and can observe its communication, Internet-of-Things vendors typically control the software in both the device and the cloud. As a result, owners have no way to audit the behavior of their own devices, leaving them little choice but to hope that these devices are transmitting only what they should.

This paper presents TLS–Rotate and Release (TLS-RaR), a system that allows device owners (e.g., consumers, security researchers, and consumer watchdogs) to authorize devices, called auditors, to decrypt and verify recent TLS traffic without compromising future traffic. Unlike prior work, TLS-RaR requires no changes to TLS's wire format or cipher suites, and it allows the device's owner to conduct a surprise inspection of recent traffic, without prior notice to the device that its communications will be audited.

1. INTRODUCTION

The Internet of Things (IoT) is notoriously insecure [34,65]. Recent exploits have shown a drone flying by a building to take control of its lights [56], and tens of thousands of compromised webcams were behind recent denial-of-service attacks against PayPal, Twitter, Netflix, and other prominent sites [14]. A recent study by HP Labs found that cleartext data, insecure firmware updates, and poor cryptographic practices mean that a substantial majority of devices had exploitable security flaws [38].

One well-accepted way to improve IoT security is to use Transport Layer Security (TLS). Products from Nest [3] and Samsung SmartThings, for example, use TLS to connect to their respective cloud services. TLS provides useful guarantees: message integrity and confidentiality, and mutual authentication of devices and servers.

However, the use of strong encryption on a locked-down consumer device has a worrisome effect for privacy: you, the device owner, cannot tell what your own devices are reporting about you. For example, if you install a Nest thermostat or camera in your home, you cannot observe the contents of its traffic to verify that it's only sending data of the kind the vendor has promised.

Internet-of-Things applications pose new security and privacy concerns because *both* ends of a secure connection are controlled by a single party: the vendor. While a Nest thermostat runs Linux, the owner cannot log in to it or otherwise control its operation. Because you cannot modify the thermostat's firmware, trace its applications, or intercept its unencrypted traffic, you cannot see what a device is reporting about you and your home.

The IoT therefore marks a break from the tradition, essentially as old as the Internet, of end users being able to inspect their own communications. Web browsers generally have a developer interface that lets end users see the contents of network traffic. And with local control of the operating system, one can look inside TLS streams by installing the public key of a trusted middlebox as a root certificate. IoT devices generally do not allow these.

While it may be rare that any given consumer will want to inspect the contents of their apps' encrypted traffic, the *ability* to do so has allowed consumer watchdogs and security researchers to uncover undisclosed exposures of personal information [5, 15, 25, 34, 67], and by reporting or publicizing these exposures, cause manufacturers to fix them.

At the same time, IoT manufacturers are understandably reluctant to provide a means to weaken a device's security by installing a new root certificate, which allows the holder to act as a man-in-the-middle between the device and the cloud, modifying traffic or impersonating one to the other. Manufacturers have also shown little interest in proposals, such as mcTLS [45], that diverge from the TLS protocol by adding additional keys and message-authentication codes to allow "read-only" middleboxes. These modified protocols are not supported by TLS terminators and load balancers in the cloud, which are often out of a vendor's control.

In this paper, we present a mechanism, TLS-Rotate and Release (TLS-RaR), which allows device owners to audit their devices' traffic without compromising application integrity, and without modifying the TLS format on the wire. Using

MobiSys '17, June 19–23, 2017, Niagara Falls, NY, USA.

ISBN 978-1-4503-4928-4/17/06…$15.00

DOI: http://dx.doi.org/10.1145/3081333.3081342

Trying to take TLS from Level 1 → Level 2

From: Stephen Farrell <stephen.farrell@cs.tcd.ie>
Date: Fri, 19 Aug 2016 22:29:50 +0100

The scope for an "auditor" (what is that?) actually being an attacker is IMO way too high to consider standardising that kind of feature and any idea that it'd involve informed consent of someone seems to me fictional.

I'd be opposed to that fwiw, as an individual participant.

As an AD, I'd look excruciatingly closely at the process for demonstrating that there's a real WG and IETF consensus for that kind of feature and that its potential for conflicting with other BCPs and well established IETF positions is very carefully considered.

Final thoughts

Robustness, Global and Local

Global: A device or software component that grows too popular can create systemic risk. Depending on manufacturers to support IoT devices forever is a long shot.

Local: Owners and anklebiters should be able to eavesdrop on what their own devices are saying about them—in order to understand and constrain what their devices are doing.

- TLS-Rotate and Release
- Secure Delegation
- Verification
- Serverless computing
- ...