QCon LONDON

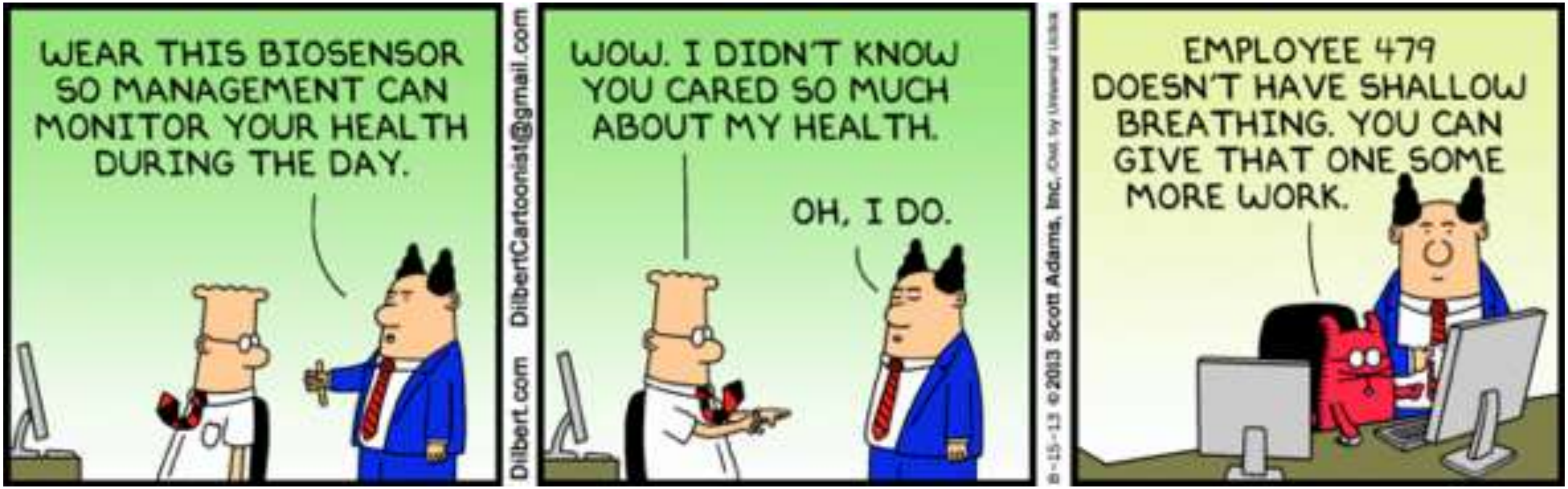
Your Thing is pwnd

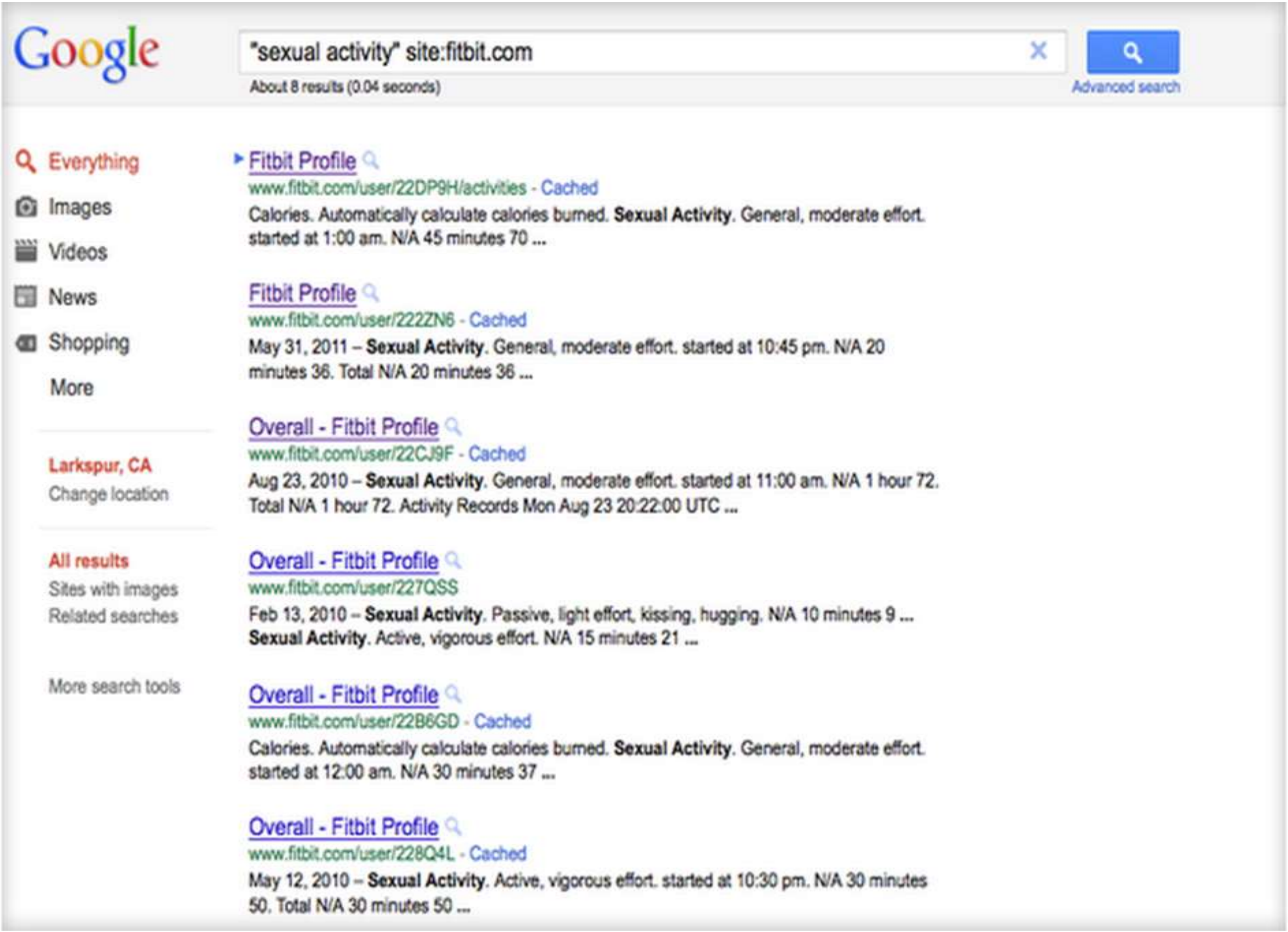
Security Challenges for the Internet of Things

Paul Fremantle
@pzfreo
PhD researcher
Portsmouth University
(paul.fremantle@port.ac.uk)

Co-Founder, WSO2

Firstly, does it even matter?


WEAR THIS BIOSENSOR SO MANAGEMENT CAN MONITOR YOUR HEALTH DURING THE DAY.
Dilbert.com DilbertCartoonist@gmail.com
WOW. I DIDN'T KNOW YOU CARED SO MUCH ABOUT MY HEALTH.
OH, I DO.
8-15-13 © 2013 Scott Adams, Inc. /Dist. by Universal Uclick
EMPLOYEE 479 DOESN'T HAVE SHALLOW BREATHING. YOU CAN GIVE THAT ONE SOME MORE WORK.



"sexual activity" site:fitbit.com

About 8 results (0.04 seconds)

Fitbit Profile
www.fitbit.com/user/22DP9H/activities - Cached
Calories. Automatically calculate calories burned. **Sexual Activity**. General, moderate effort. started at 1:00 am. N/A 45 minutes 70 ...

Fitbit Profile
www.fitbit.com/user/222ZN6 - Cached
May 31, 2011 – **Sexual Activity**. General, moderate effort. started at 10:45 pm. N/A 20 minutes 36. Total N/A 20 minutes 36 ...

Overall - Fitbit Profile
www.fitbit.com/user/22CJ9F - Cached
Aug 23, 2010 – **Sexual Activity**. General, moderate effort. started at 11:00 am. N/A 1 hour 72. Total N/A 1 hour 72. Activity Records Mon Aug 23 20:22:00 UTC ...

Overall - Fitbit Profile
www.fitbit.com/user/227QSS
Feb 13, 2010 – **Sexual Activity**. Passive, light effort, kissing, hugging. N/A 10 minutes 9 ... **Sexual Activity**. Active, vigorous effort. N/A 15 minutes 21 ...

Overall - Fitbit Profile
www.fitbit.com/user/22B6GD - Cached
Calories. Automatically calculate calories burned. **Sexual Activity**. General, moderate effort. started at 12:00 am. N/A 30 minutes 37 ...

Overall - Fitbit Profile
www.fitbit.com/user/228Q4L - Cached
May 12, 2010 – **Sexual Activity**. Active, vigorous effort. started at 10:30 pm. N/A 30 minutes 50. Total N/A 30 minutes 50 ...

My three rules for IoT security

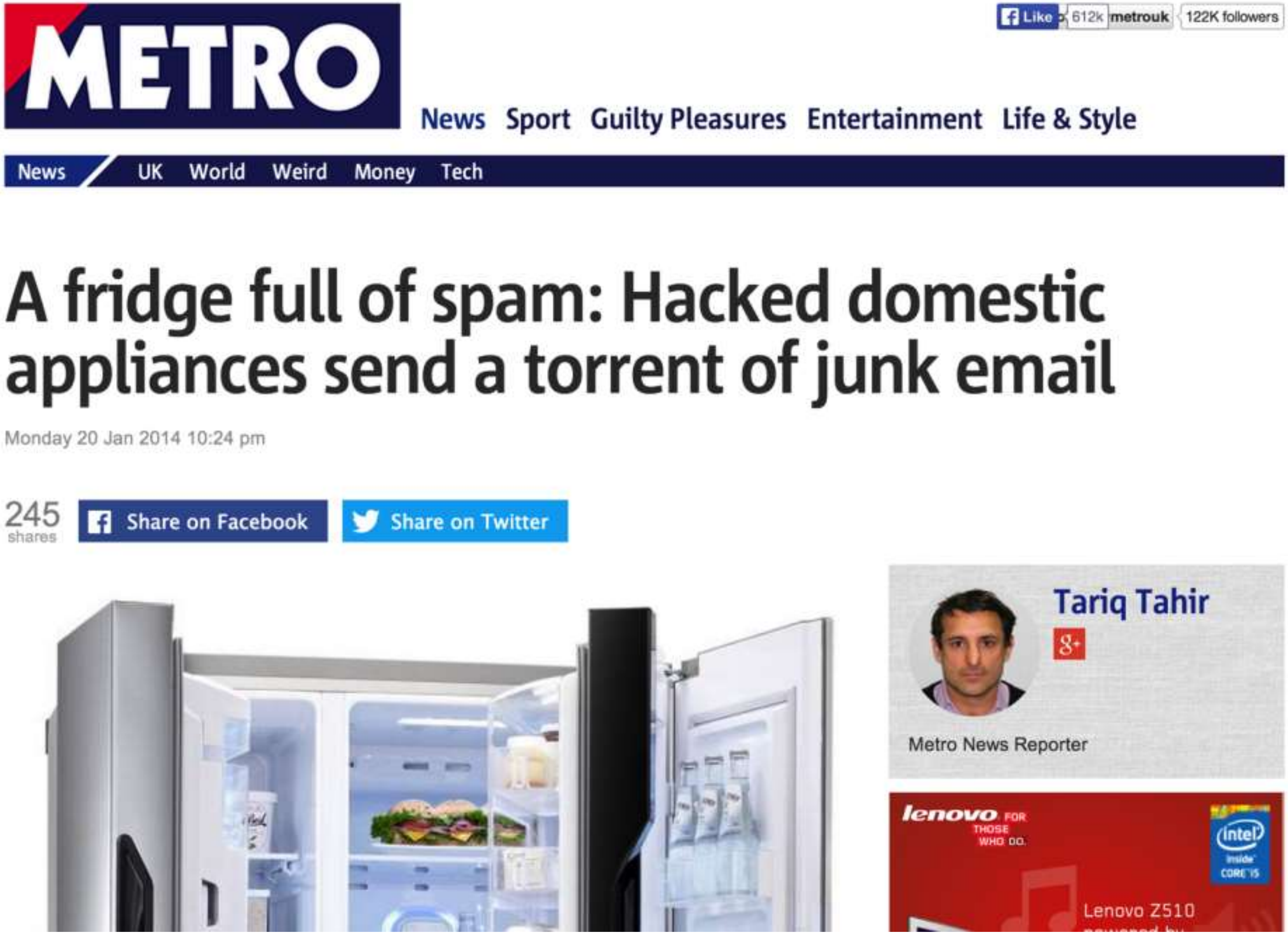
- 1. Don’t be stupid

- 2. Be smart

- 3. Think about what’s different

My three rules for IoT security

- 1. Don’t be stupid
  - The basics of Internet security haven’t gone away
- 2. Be smart
  - Use the best practice from the Internet
- 3. Think about what’s different
  - What are the unique challenges of your device?

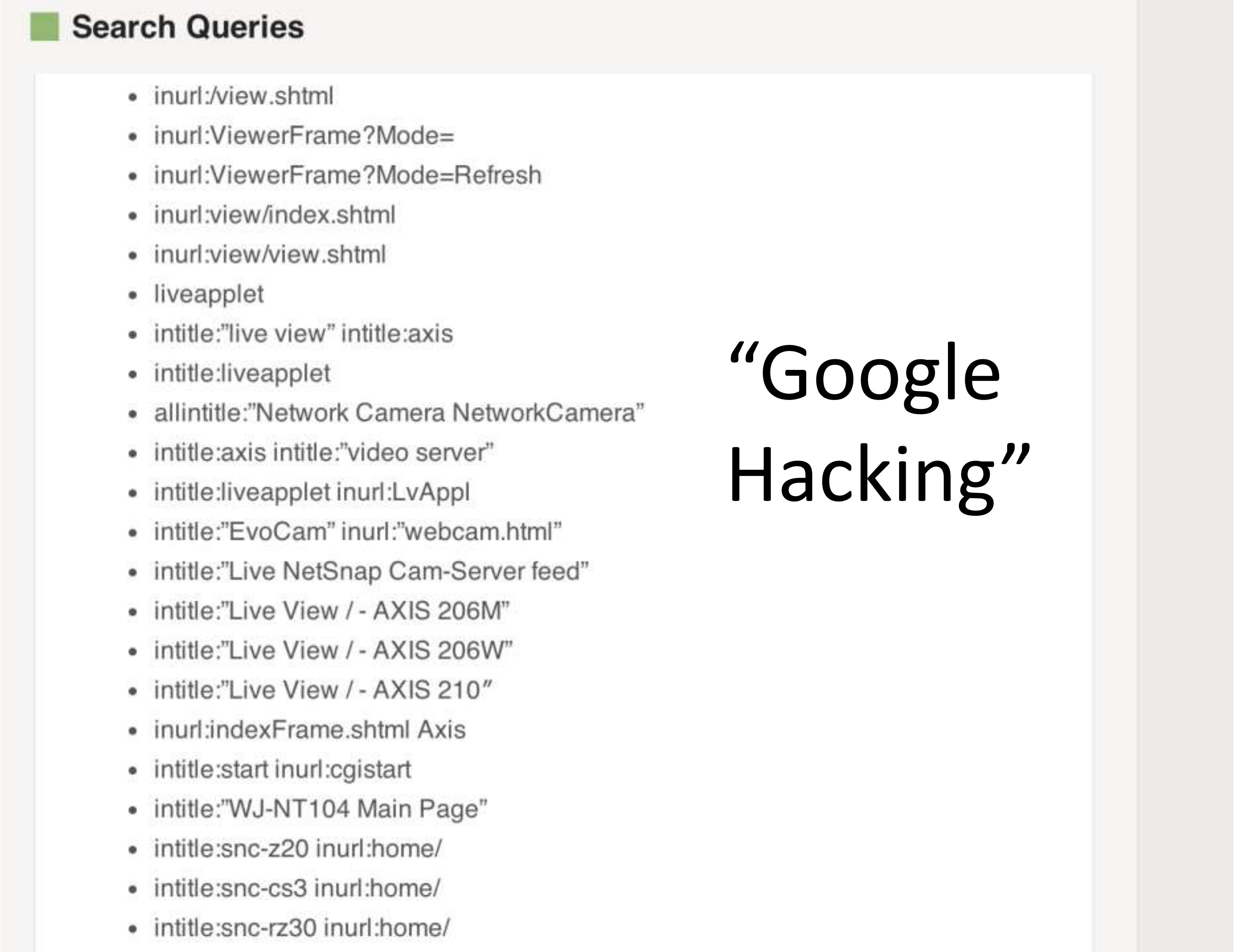


A fridge full of spam: Hacked domestic appliances send a torrent of junk email

Monday 20 Jan 2014 10:24 pm

Tariq Tahir

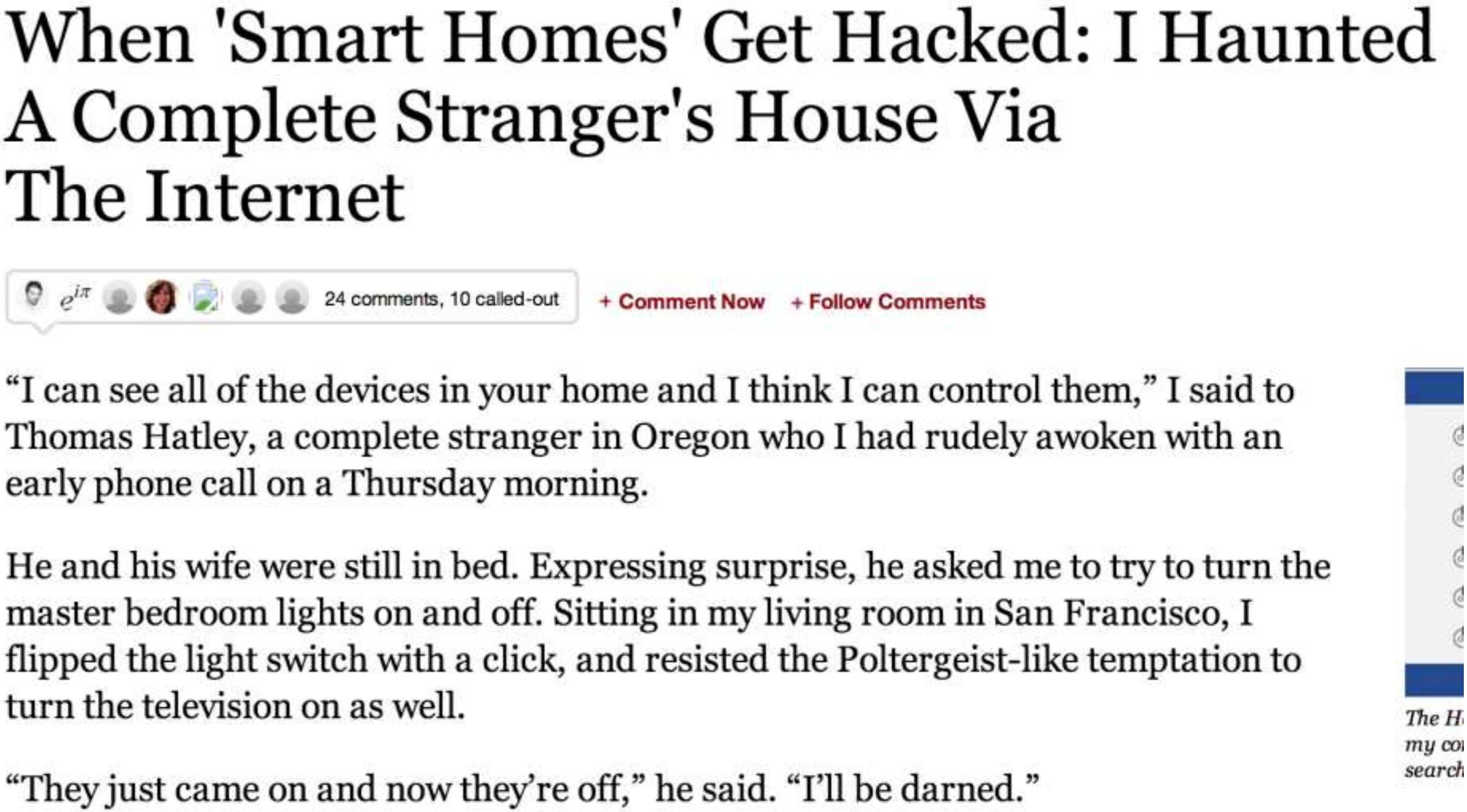
Metro News Reporter



Search Queries

- inurl:/view.shtml
- inurl:ViewerFrame?Mode=
- inurl:ViewerFrame?Mode=Refresh
- inurl:view/index.shtml
- inurl:view/view.shtml
- liveapplet
- intitle:"live view" intitle:axis
- intitle:liveapplet
- allintitle:"Network Camera NetworkCamera"
- intitle:axis intitle:"video server"
- intitle:liveapplet inurl:LvAppl
- intitle:"EvoCam" inurl:"webcam.html"
- intitle:"Live NetSnap Cam-Server feed"
- intitle:"Live View / - AXIS 206M"
- intitle:"Live View / - AXIS 206W"
- intitle:"Live View / - AXIS 210″
- inurl:indexFrame.shtml Axis
- intitle:start inurl:cgistart
- intitle:"WJ-NT104 Main Page"
- intitle:snc-z20 inurl:home/
- intitle:snc-cs3 inurl:home/
- intitle:snc-rz30 inurl:home/

“Google Hacking”



When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet

"I can see all of the devices in your home and I think I can control them," I said to Thomas Hatley, a complete stranger in Oregon who I had rudely awoken with an early phone call on a Thursday morning.

He and his wife were still in bed. Expressing surprise, he asked me to try to turn the master bedroom lights on and off. Sitting in my living room in San Francisco, I flipped the light switch with a click, and resisted the Poltergeist-like temptation to turn the television on as well.

"They just came on and now they're off," he said. "I'll be darned."

http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/

1998

- Realized that session cookies needed to be tied to user sessions
  - Scenario: Attacker has a valid login, but changes their cookie
  - Gets access to another user’s account

February 2015

Mosquitto 1.4 Release Notes

- When a durable client reconnects, its queued messages are now checked against ACLs in case of a change in username/ACL state since it last connected.

CONRAD
FUNKTION
PROG
Mo Di Mi Do Fr Sa So
16:52
08.02
Prog
Auto
Manu
22.5 °C
0 6 12 18 24
A2

So what is different about IoT?

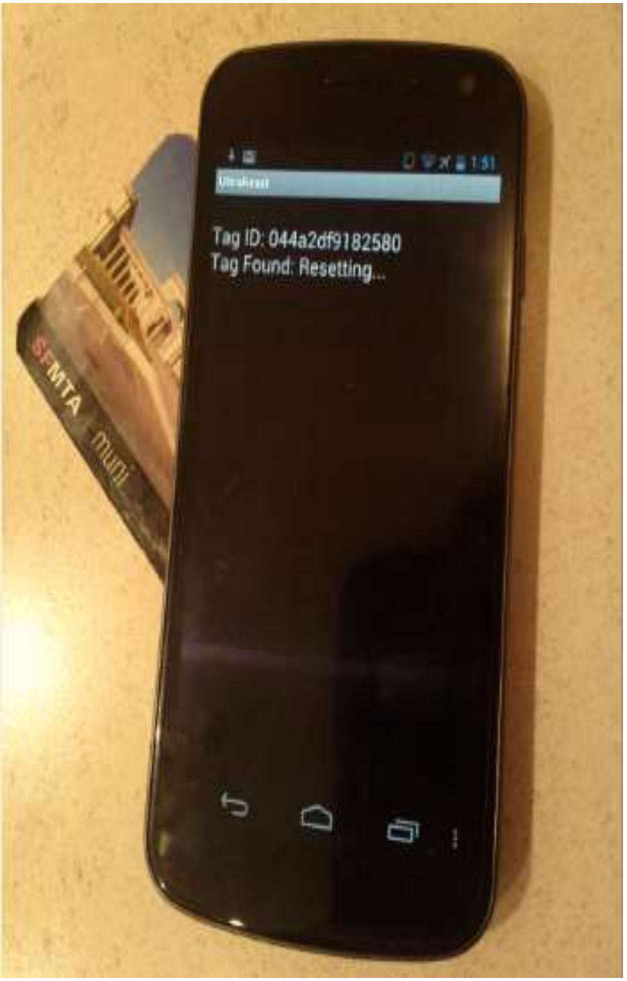
- The longevity of the device
  - Updates are harder (or impossible)
- The size of the device
  - Capabilities are limited – especially around crypto
- The fact there *is* a device
  - Usually no UI for entering userids and passwords
- The data
  - Often highly personal
- The mindset
  - Appliance manufacturers don’t think like security experts
  - Embedded systems are often developed by grabbing existing chips, designs, etc

Physical Hacks

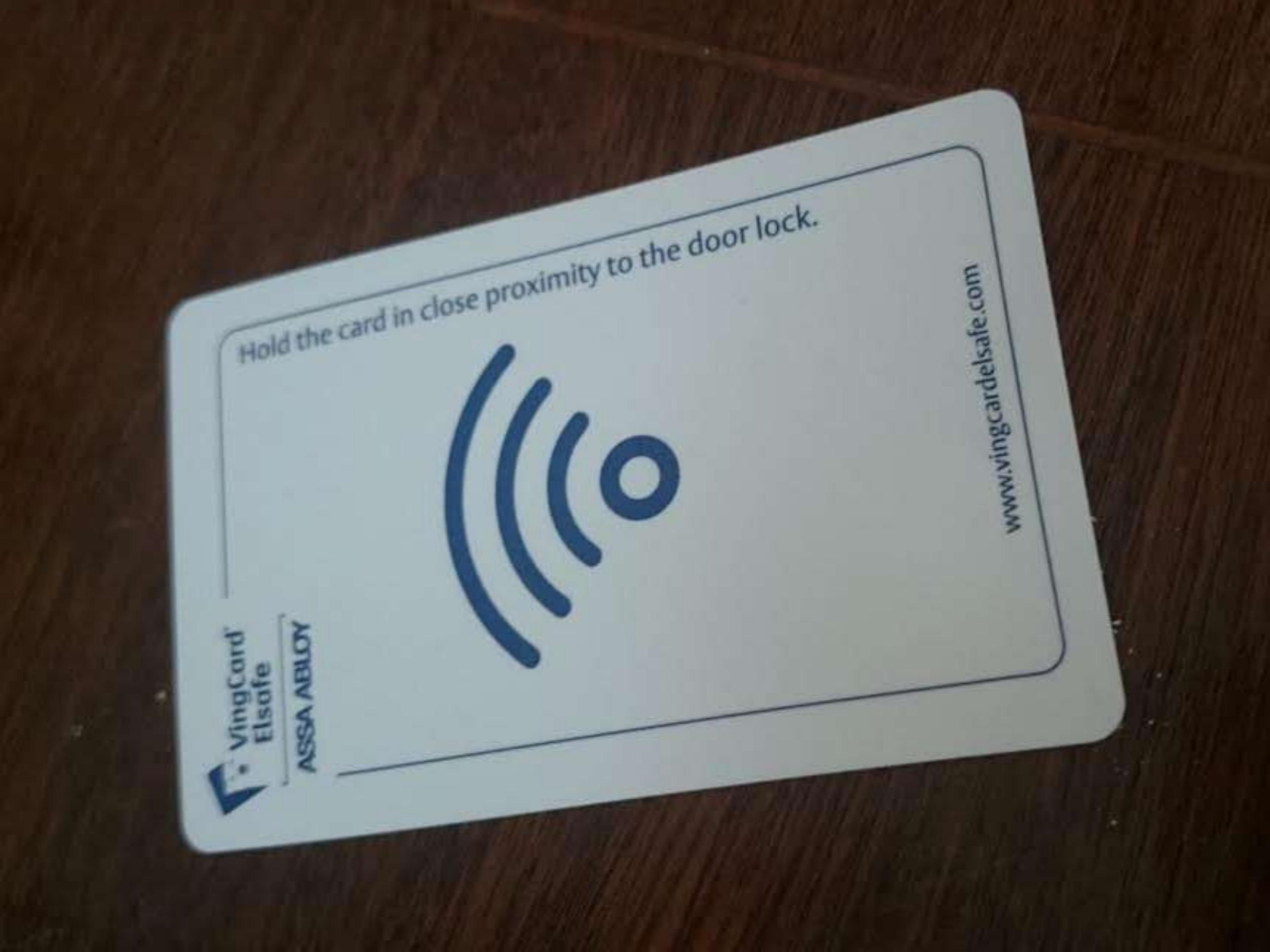
A Practical Attack on the MIFARE Classic:
http://www.cs.ru.nl/~flaviog/publications/Attack.MIFARE.pdf
Karsten Nohl and Henryk Plotz. MIFARE, Little Security, Despite Obscurity

UltraReset

https://intrepidusgroup.com/insight/2012/09/ultrareset-bypassing-nfc-access-control-with-your-smartphone/

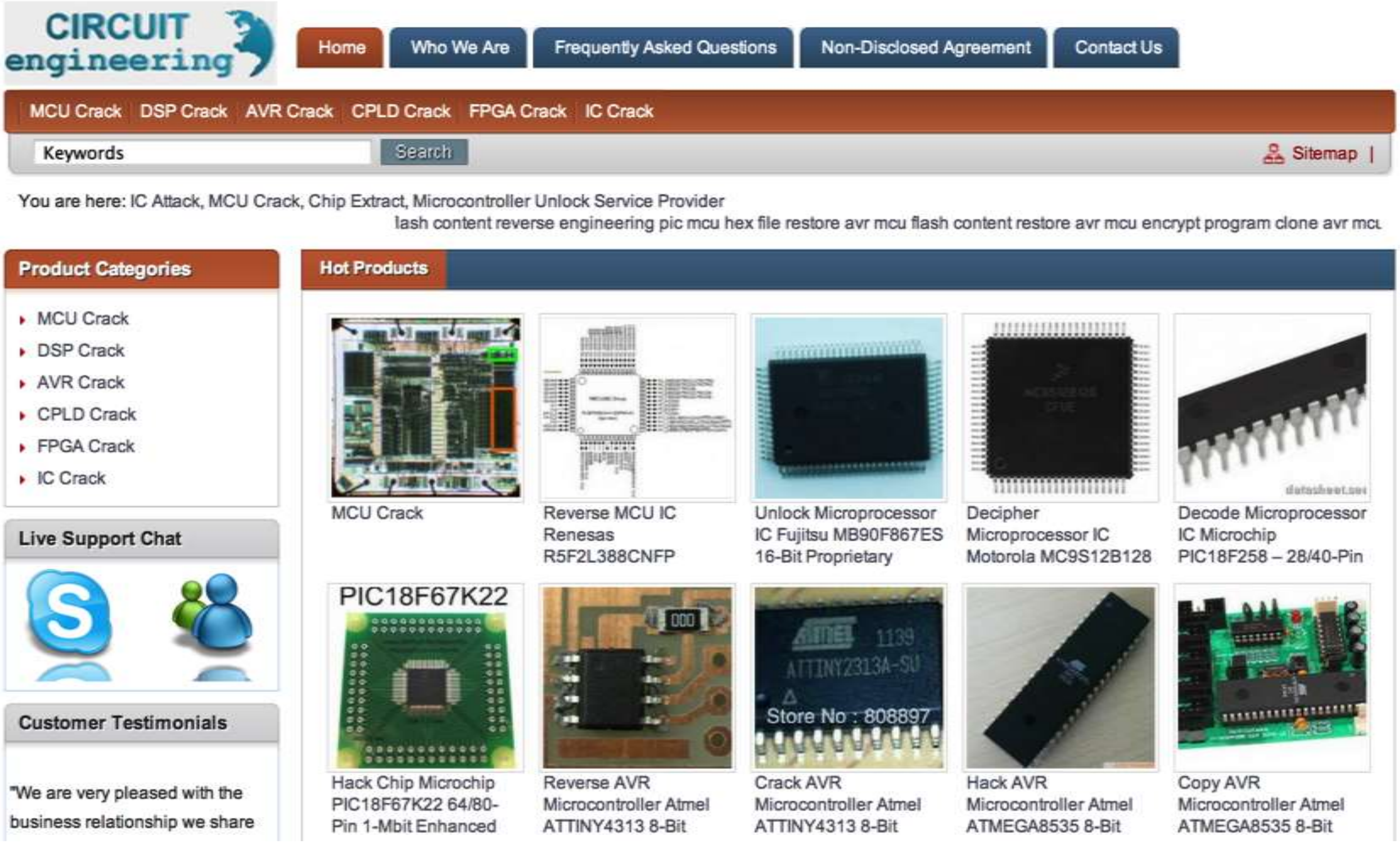

UltraReset

Tag ID: 044a2df9182580
Tag Found: Resetting...



Hold the card in close proximity to the door lock.

www.vingcardelsafe.com



You are here: IC Attack, MCU Crack, Chip Extract, Microcontroller Unlock Service Provider

lash content reverse engineering pic mcu hex file restore avr mcu flash content restore avr mcu encrypt program clone avr mcu

"We are very pleased with the business relationship we share

MCU Crack

Reverse MCU IC Renesas R5F2L388CNFP

Unlock Microprocessor IC Fujitsu MB90F867ES 16-Bit Proprietary

Decipher Microprocessor IC Motorola MC9S12B128

Decode Microprocessor IC Microchip PIC18F258 – 28/40-Pin

Hack Chip Microchip PIC18F67K22 64/80-Pin 1-Mbit Enhanced

Reverse AVR Microcontroller Atmel ATTINY4313 8-Bit

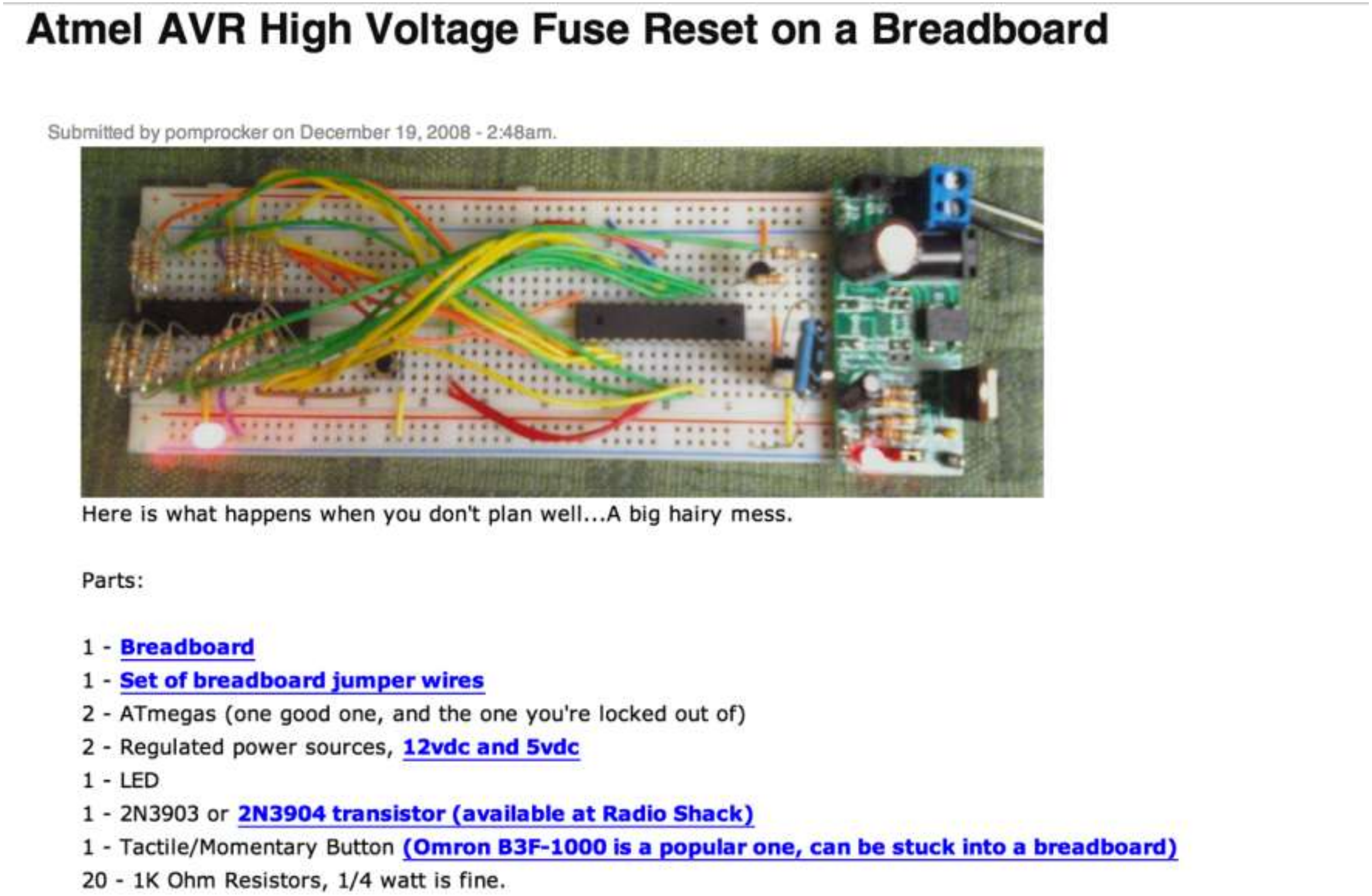
Crack AVR Microcontroller Atmel ATTINY4313 8-Bit

Hack AVR Microcontroller Atmel ATMEGA8535 8-Bit

Copy AVR Microcontroller Atmel ATMEGA8535 8-Bit

Or try this at home?

http://freo.me/1g15BiG



Atmel AVR High Voltage Fuse Reset on a Breadboard

Submitted by pomprocker on December 19, 2008 - 2:48am.

Here is what happens when you don't plan well...A big hairy mess.

Parts:

1 - **Breadboard**
1 - **Set of breadboard jumper wires**
2 - ATmegas (one good one, and the one you're locked out of)
2 - Regulated power sources, **12vdc and 5vdc**
1 - LED
1 - 2N3903 or **2N3904 transistor (available at Radio Shack)**
1 - Tactile/Momentary Button **(Omron B3F-1000 is a popular one, can be stuck into a breadboard)**
20 - 1K Ohm Resistors, 1/4 watt is fine.

Technical Report

UCAM-CL-TR-630
ISSN 1476-2986

Number 630

UNIVERSITY OF
CAMBRIDGE

Computer Laboratory

Semi-invasive attacks – A new approach to hardware security analysis

Sergei P. Skorobogatov

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.html

Hardware recommendations

- Don’t rely on obscurity

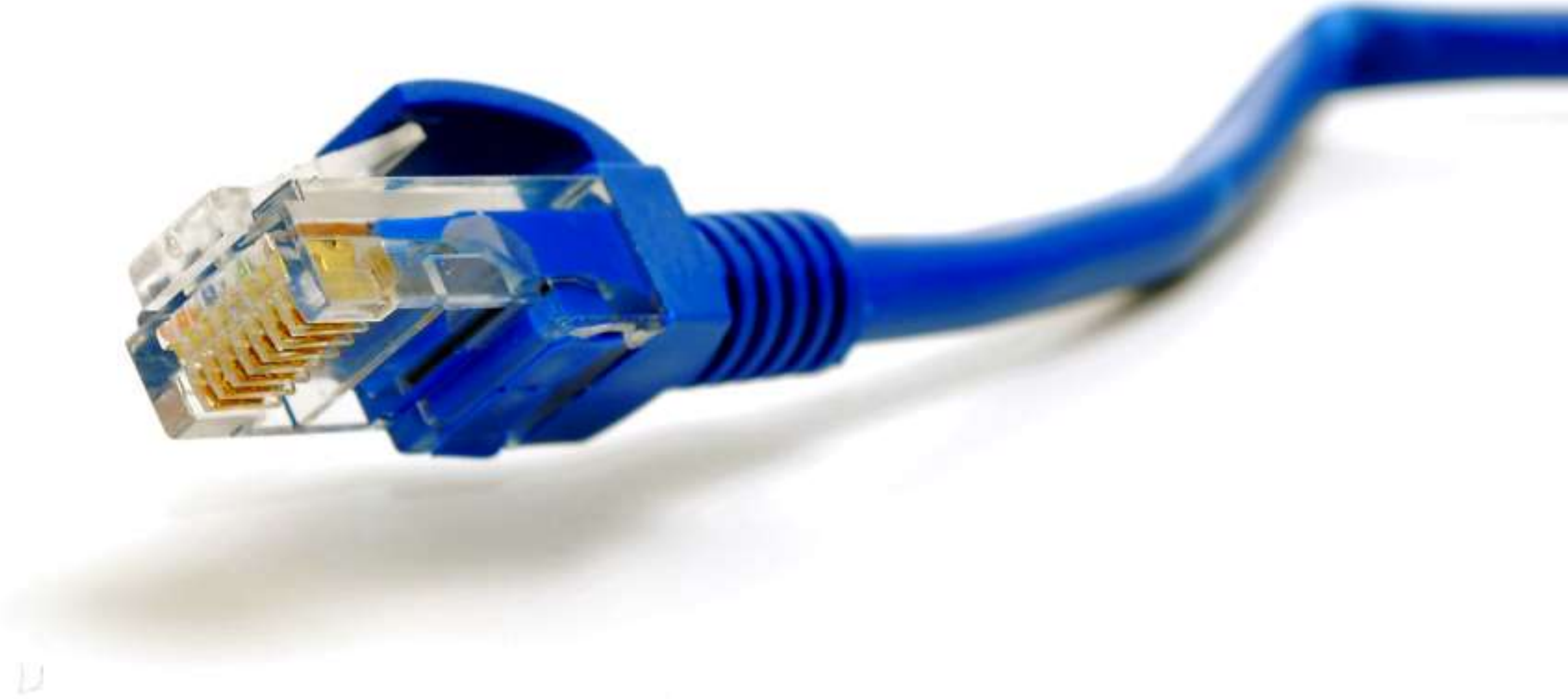
Hardware recommendations

- Don’t rely on obscurity
- Don’t rely on obscurity
- Don’t rely on obscurity
- Don’t rely on obscurity
- Don’t rely on obscurity
- Don’t rely on obscurity
- Don’t rely on obscurity

Hardware Recommendation #2

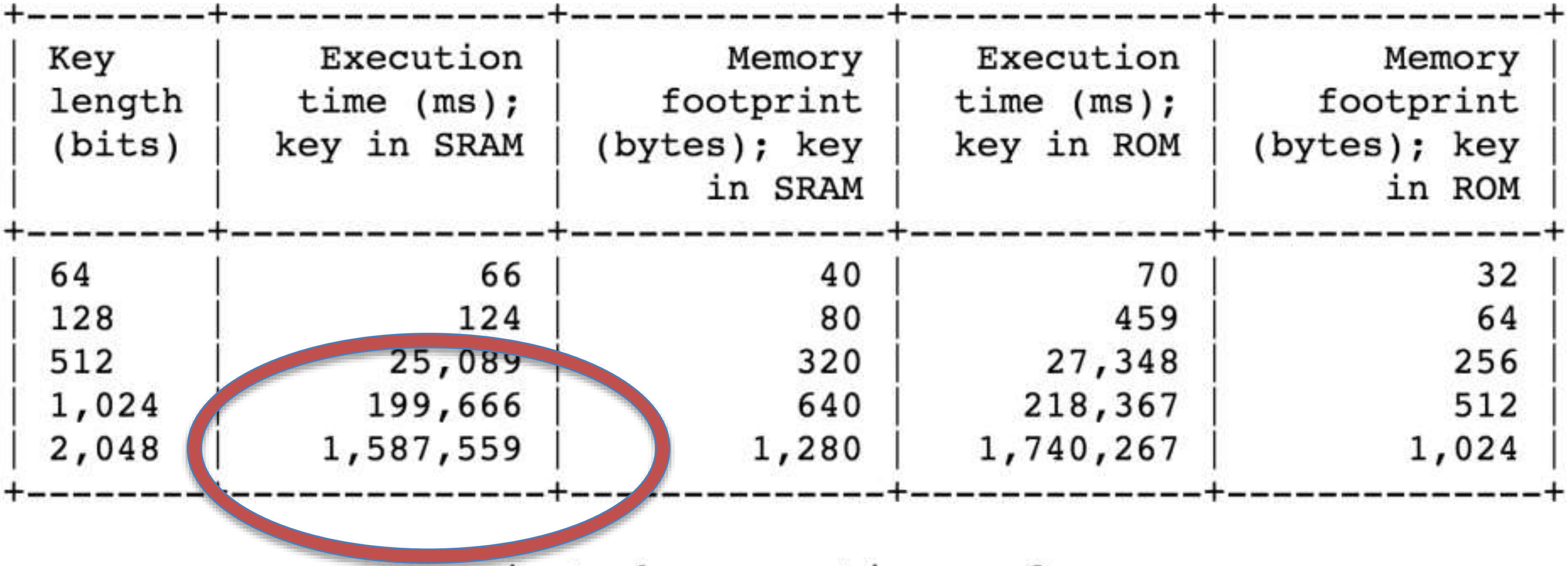
- Unlocking a single device should risk only that device’s data

The Network



Crypto on small devices

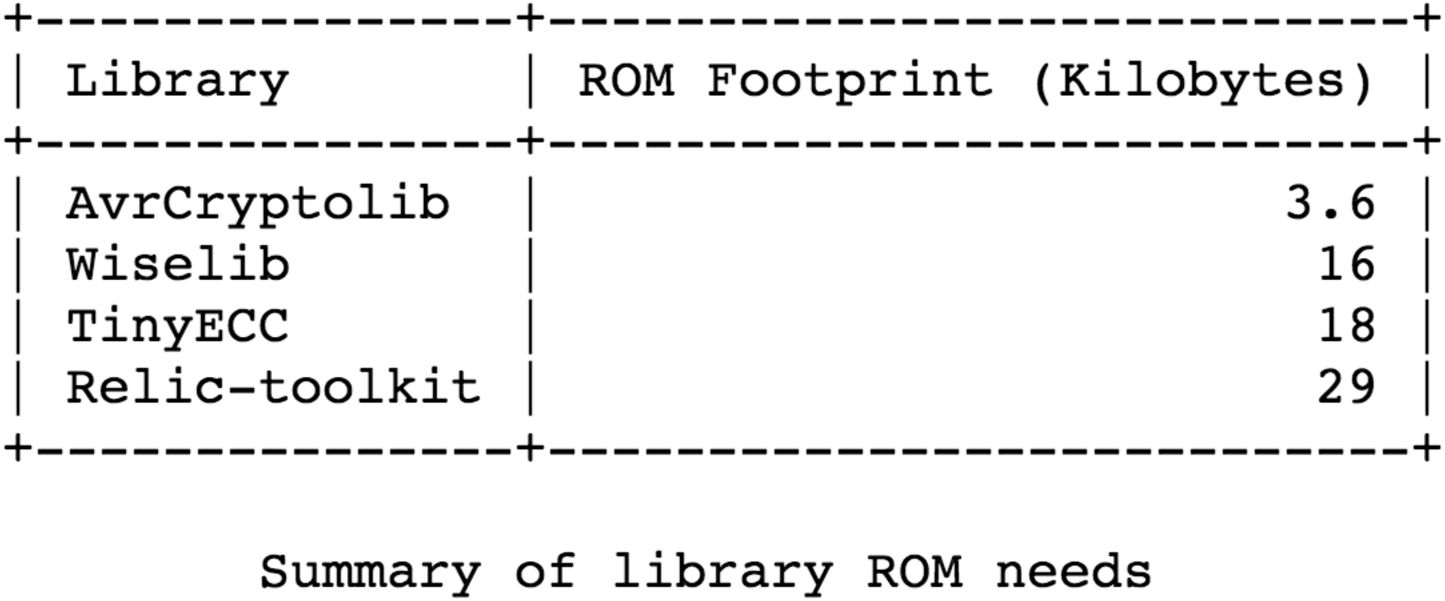
- Practical Considerations and Implementation Experiences in Securing Smart Object Networks
  - http://tools.ietf.org/html/draft-aks-crypto-sensors-02



Key length (bits)	Execution time (ms); key in SRAM	Memory footprint (bytes); key in SRAM	Execution time (ms); key in ROM	Memory footprint (bytes); key in ROM
64	66	40	70	32
128	124	80	459	64
512	25,089	320	27,348	256
1,024	199,666	640	218,367	512
2,048	1,587,559	1,280	1,740,267	1,024

RSA private key operation performance

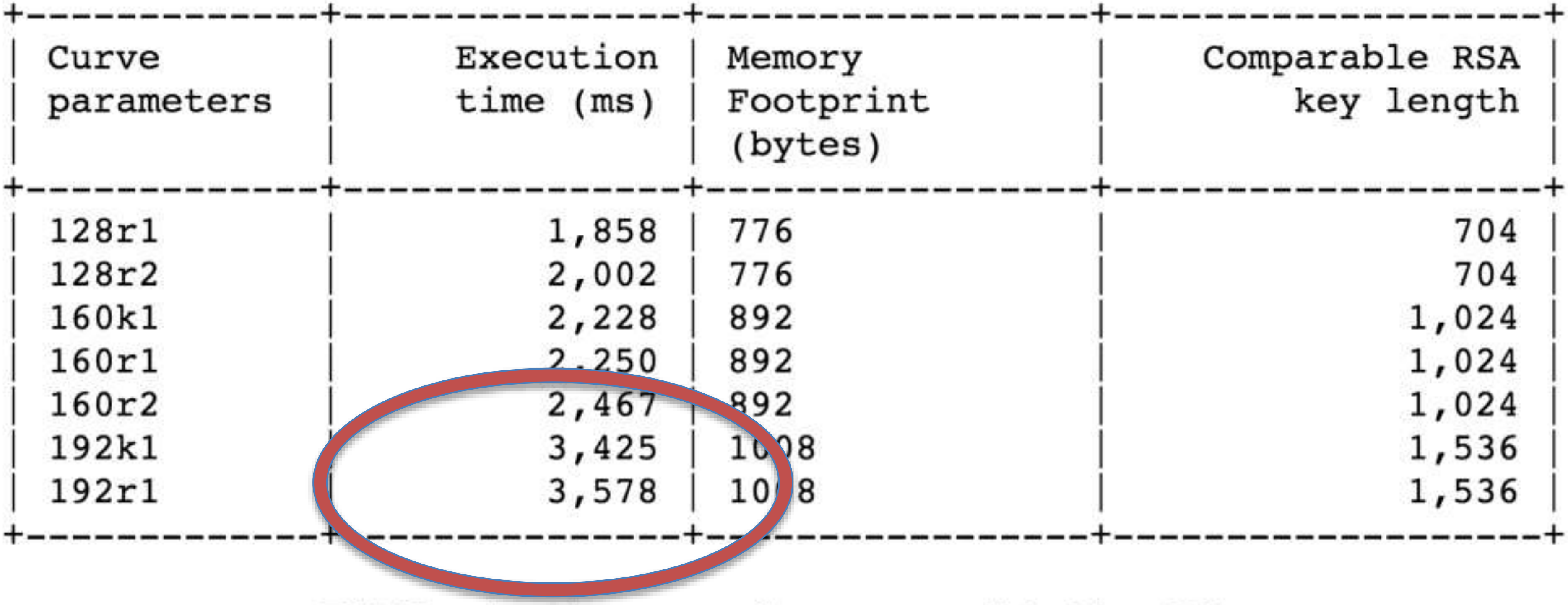
ROM requirements



Library	ROM Footprint (Kilobytes)
AvrCryptolib	3.6
Wiselib	16
TinyECC	18
Relic-toolkit	29

Summary of library ROM needs

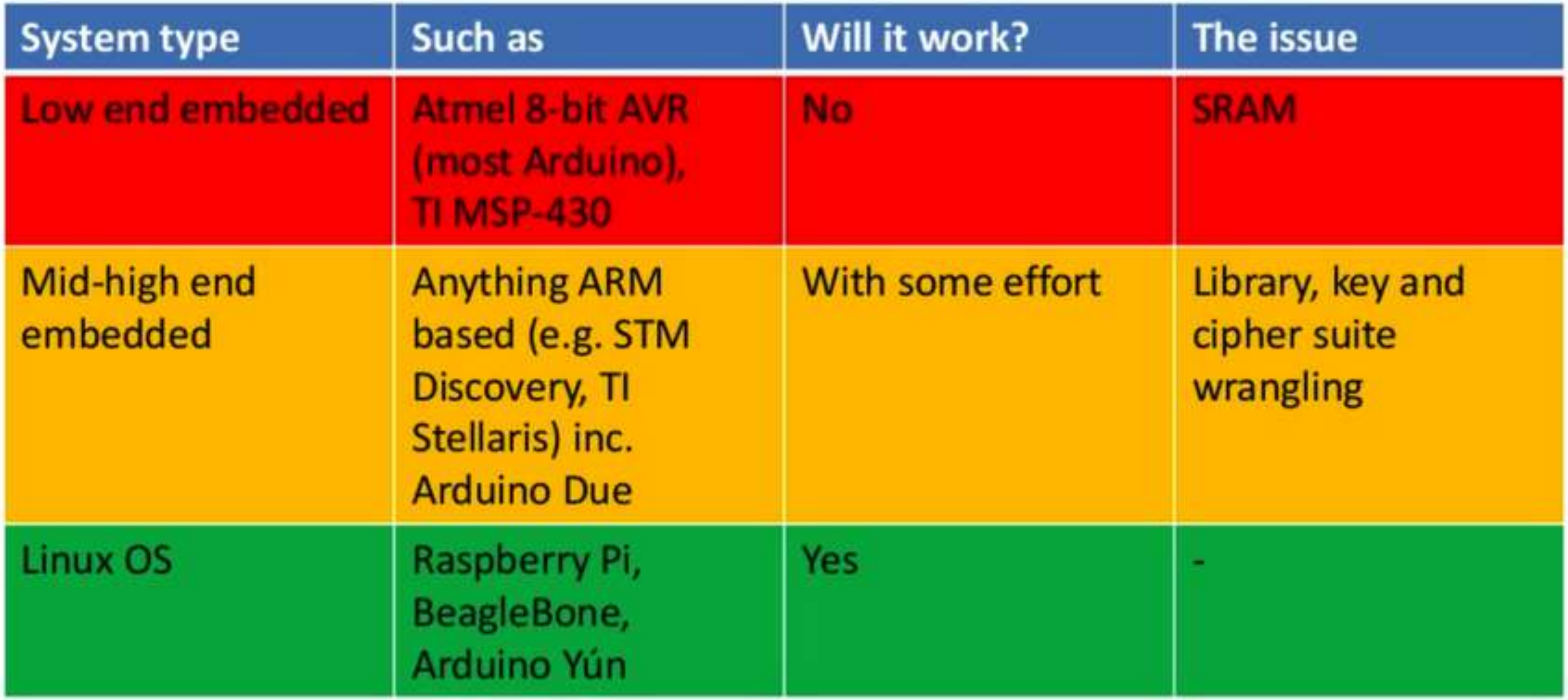
ECC is possible (and about fast enough)



Curve parameters	Execution time (ms)	Memory Footprint (bytes)	Comparable RSA key length
128r1	1,858	776	704
128r2	2,002	776	704
160k1	2,228	892	1,024
160r1	2,250	892	1,024
160r2	2,467	892	1,024
192k1	3,425	1008	1,536
192r1	3,578	1008	1,536

ECDSA signature performance with TinyECC

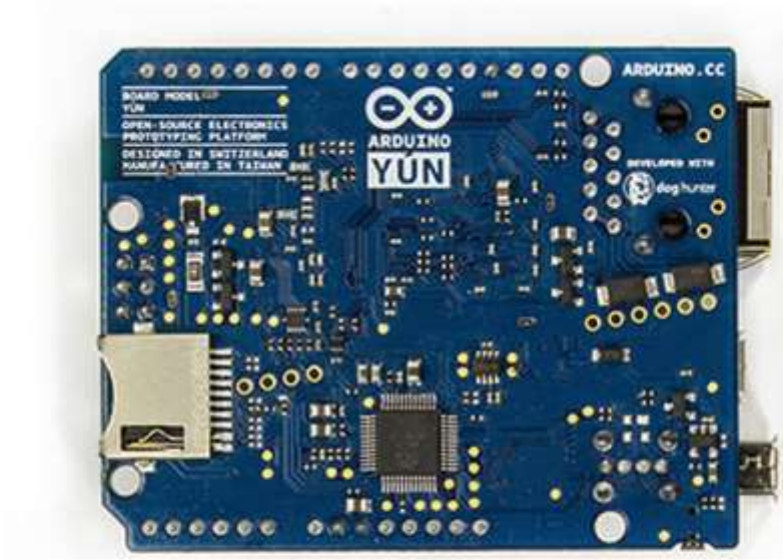
Crypto



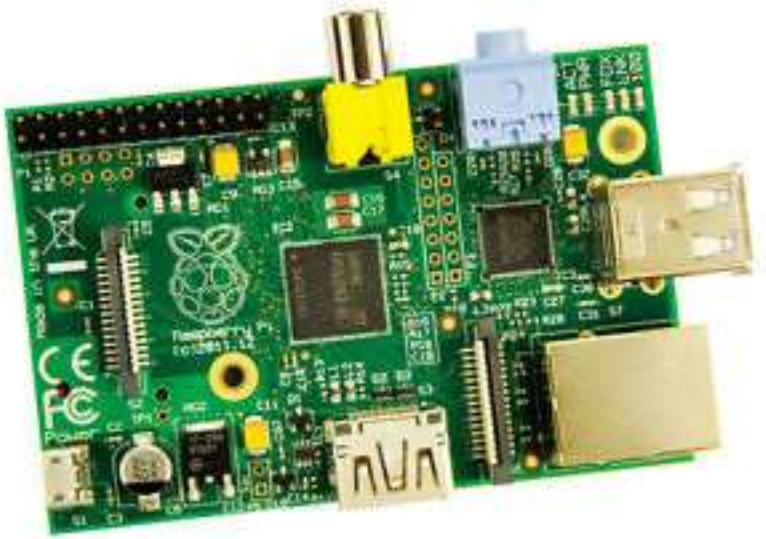
System type	Such as	Will it work?	The issue
Low end embedded	Atmel 8-bit AVR (most Arduino), TI MSP-430	No	SRAM
Mid-high end embedded	Anything ARM based (e.g. STM Discovery, TI Stellaris) inc. Arduino Due	With some effort	Library, key and cipher suite wrangling
Linux OS	Raspberry Pi, BeagleBone, Arduino Yún	Yes	-

Borrowed from Chris Swan:
http://www.slideshare.net/cpswan/security-protocols-in-constrained-environments/13

Won’t ARM just solve this problem?



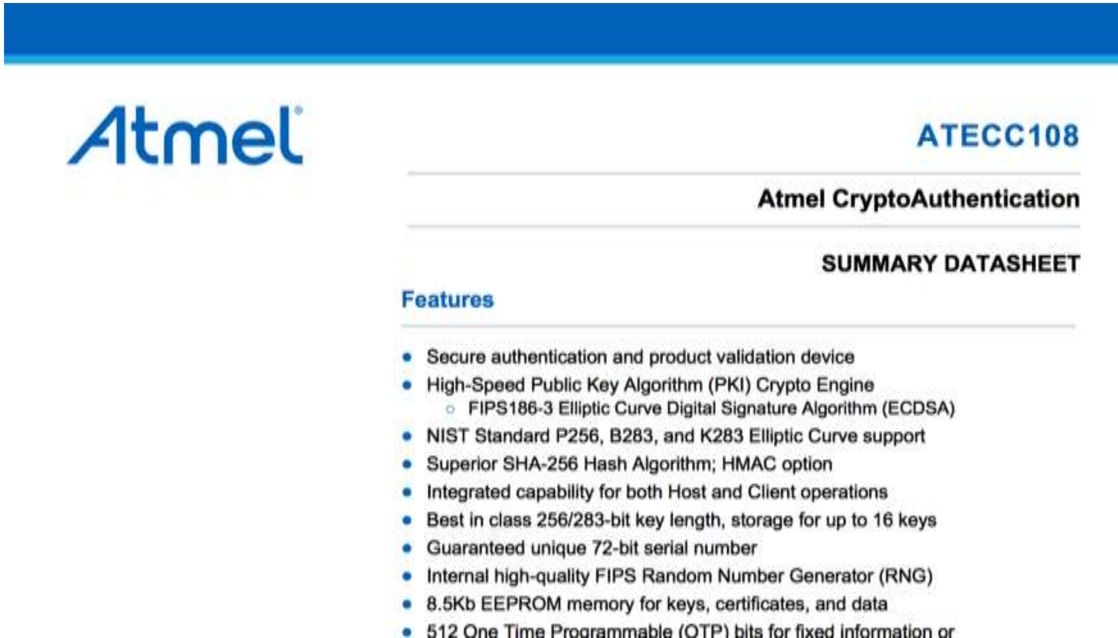
Cost matters



8 bits
$5 retail
$1 or less to embed

32 bits
$25 retail
$?? to embed

Another option?



Atmel

ATECC108

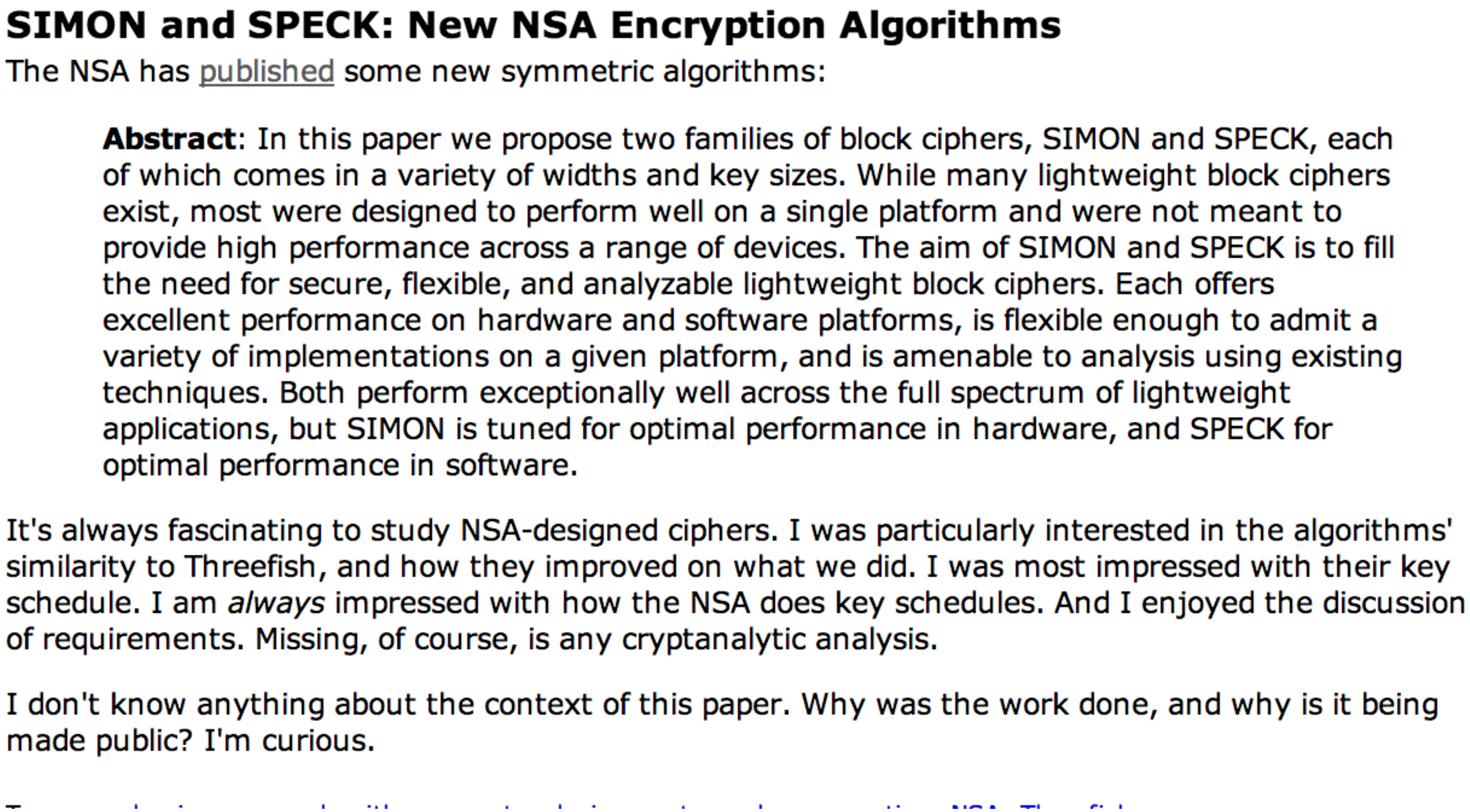
Atmel CryptoAuthentication

SUMMARY DATASHEET

Features

- Secure authentication and product validation device
- High-Speed Public Key Algorithm (PKI) Crypto Engine
  - FIPS186-3 Elliptic Curve Digital Signature Algorithm (ECDSA)
- NIST Standard P256, B283, and K283 Elliptic Curve support
- Superior SHA-256 Hash Algorithm; HMAC option
- Integrated capability for both Host and Client operations
- Best in class 256/283-bit key length, storage for up to 16 keys
- Guaranteed unique 72-bit serial number
- Internal high-quality FIPS Random Number Generator (RNG)
- 8.5Kb EEPROM memory for keys, certificates, and data
- 512 One Time Programmable (OTP) bits for fixed information or

SIMON and SPECK



SIMON and SPECK: New NSA Encryption Algorithms

The NSA has published some new symmetric algorithms:

> **Abstract**: In this paper we propose two families of block ciphers, SIMON and SPECK, each of which comes in a variety of widths and key sizes. While many lightweight block ciphers exist, most were designed to perform well on a single platform and were not meant to provide high performance across a range of devices. The aim of SIMON and SPECK is to fill the need for secure, flexible, and analyzable lightweight block ciphers. Each offers excellent performance on hardware and software platforms, is flexible enough to admit a variety of implementations on a given platform, and is amenable to analysis using existing techniques. Both perform exceptionally well across the full spectrum of lightweight applications, but SIMON is tuned for optimal performance in hardware, and SPECK for optimal performance in software.

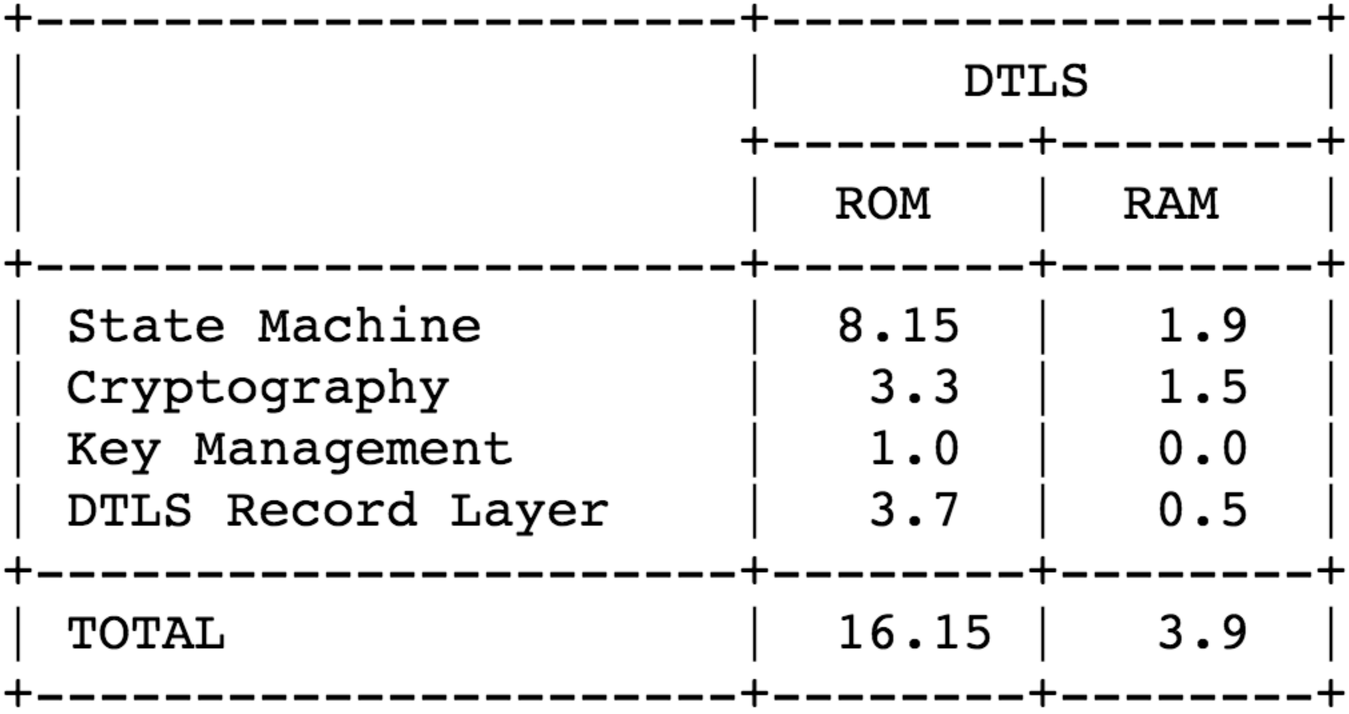
It's always fascinating to study NSA-designed ciphers. I was particularly interested in the algorithms' similarity to Threefish, and how they improved on what we did. I was most impressed with their key schedule. I am *always* impressed with how the NSA does key schedules. And I enjoyed the discussion of requirements. Missing, of course, is any cryptanalytic analysis.

I don't know anything about the context of this paper. Why was the work done, and why is it being made public? I'm curious.

https://www.schneier.com/blog/archives/2013/07/simon_and_speck.html

Datagram Transport Layer Security (DTLS)

- UDP based equivalent to TLS
- https://tools.ietf.org/html/rfc4347



	DTLS	
	ROM	RAM
State Machine	8.15	1.9
Cryptography	3.3	1.5
Key Management	1.0	0.0
DTLS Record Layer	3.7	0.5
TOTAL	16.15	3.9

Table 1: Memory Requirements in KB

Key distribution

How do you distribute keys to devices?

- Usually at manufacture time

- Complex to update

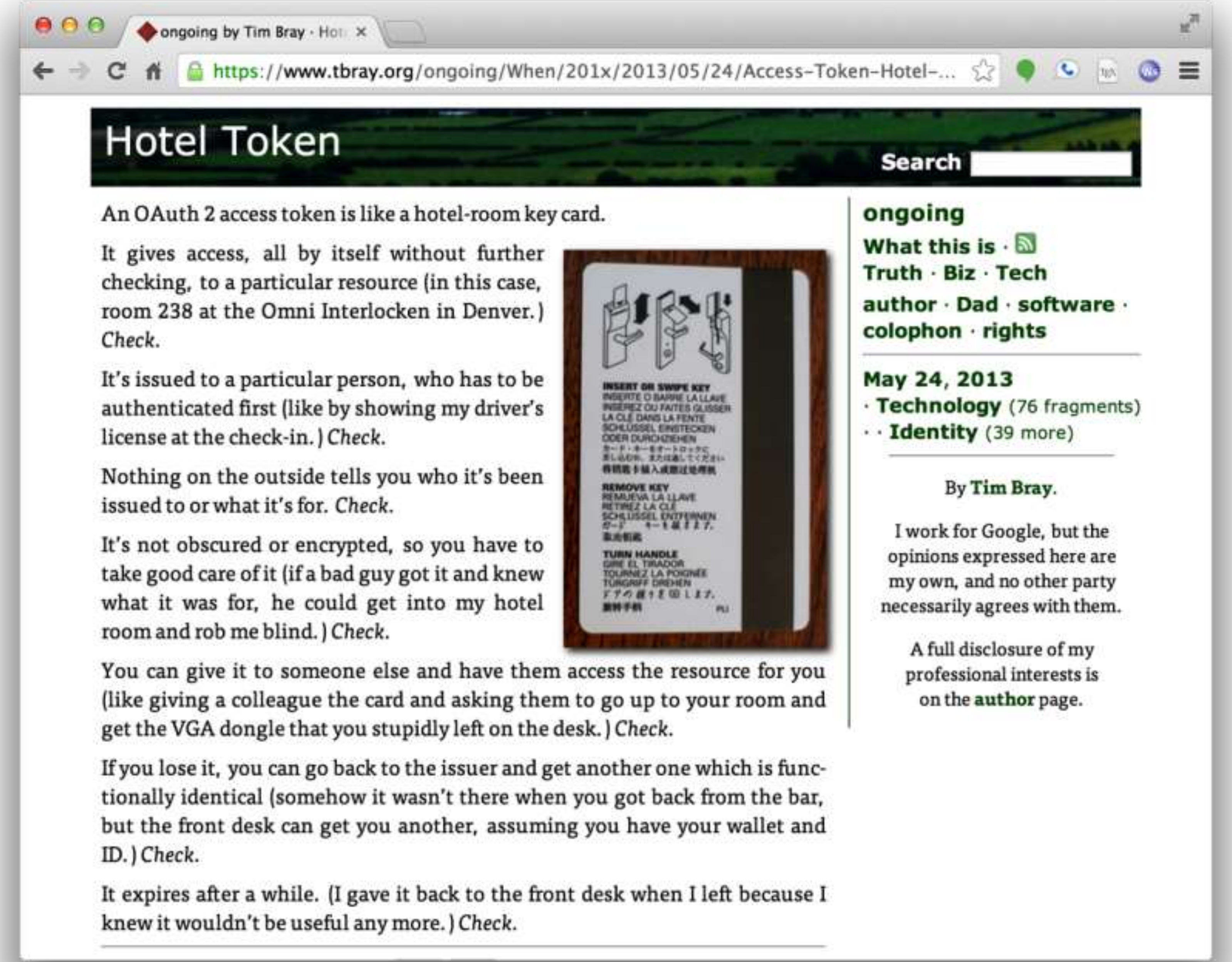
- What about expiration?

Passwords

- Passwords suck for humans
- They suck even more for devices

OAUTH
2
OAUTH

OpenID
Connect


ongoing by Tim Bray · Hom
https://www.tbray.org/ongoing/When/201x/2013/05/24/Access-Token-Hotel-…
INSERT OR SWIPE KEY
INSERTE O BARRE LA LLAVE
INSEREZ OU FAITES GLISSER LA CLÉ DANS LA FENTE
SCHLÜSSEL EINSTECKEN ODER DURCHZIEHEN
REMOVE KEY
REMUEVA LA LLAVE
RETIREZ LA CLÉ
SCHLÜSSEL ENTFERNEN
TURN HANDLE
GIRE EL TIRADOR
TOURNEZ LA POIGNÉE
TÜRGRIFF DREHEN

Hotel Token

Search

An OAuth 2 access token is like a hotel-room key card.

It gives access, all by itself without further checking, to a particular resource (in this case, room 238 at the Omni Interlocken in Denver.) *Check*.

It's issued to a particular person, who has to be authenticated first (like by showing my driver's license at the check-in.) *Check*.

Nothing on the outside tells you who it's been issued to or what it's for. *Check*.

It's not obscured or encrypted, so you have to take good care of it (if a bad guy got it and knew what it was for, he could get into my hotel room and rob me blind.) *Check*.

You can give it to someone else and have them access the resource for you (like giving a colleague the card and asking them to go up to your room and get the VGA dongle that you stupidly left on the desk.) *Check*.

If you lose it, you can go back to the issuer and get another one which is functionally identical (somehow it wasn't there when you got back from the bar, but the front desk can get you another, assuming you have your wallet and ID.) *Check*.

It expires after a while. (I gave it back to the front desk when I left because I knew it wouldn't be useful any more.) *Check*.

ongoing

What this is ·
Truth · **Biz** · **Tech**
author · **Dad** · **software** ·
colophon · **rights**

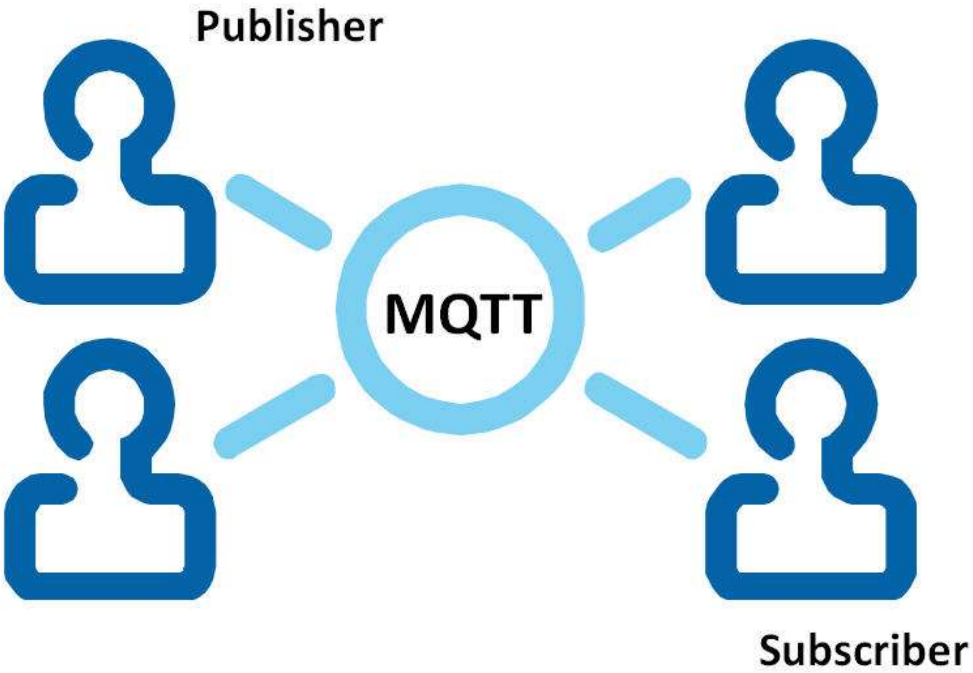
May 24, 2013
· **Technology** (76 fragments)
· · **Identity** (39 more)

By **Tim Bray**.

I work for Google, but the opinions expressed here are my own, and no other party necessarily agrees with them.

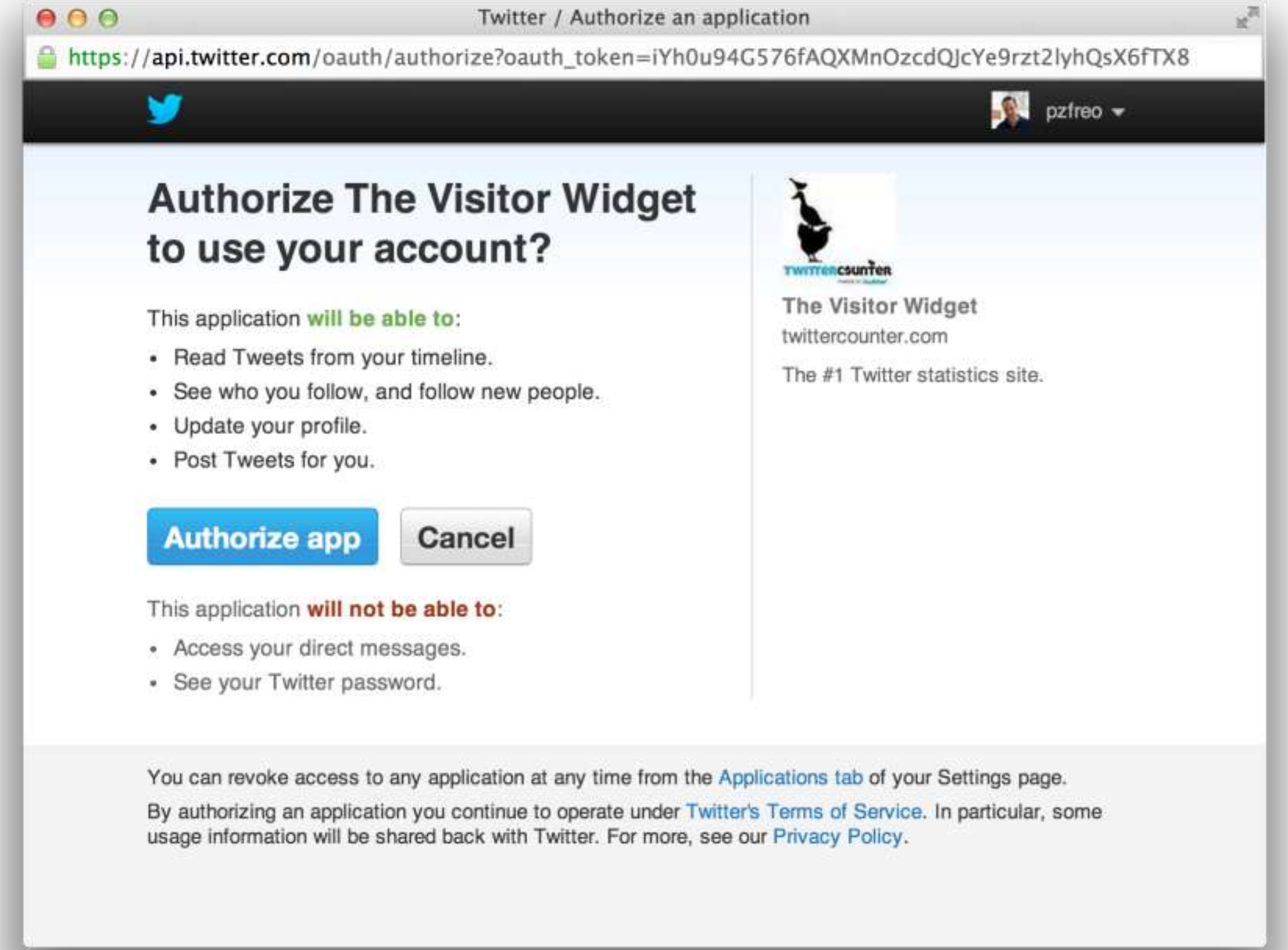
A full disclosure of my professional interests is on the **author** page.

MQTT



Messenger

Free texting from Facebook



Twitter / Authorize an application
https://api.twitter.com/oauth/authorize?oauth_token=iYh0u94G576fAQXMnOzcdQJcYe9rzt2lyhQsX6fTX8
pzfreo
TWITTERCOUNTER
Authorize app
Cancel

Authorize The Visitor Widget to use your account?

This application **will be able to**:

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.

This application **will not be able to**:

- Access your direct messages.
- See your Twitter password.

The Visitor Widget
twittercounter.com

The #1 Twitter statistics site.

You can revoke access to any application at any time from the Applications tab of your Settings page.

By authorizing an application you continue to operate under Twitter's Terms of Service. In particular, some usage information will be shared back with Twitter. For more, see our Privacy Policy.

Why Federated Identity for IoT?

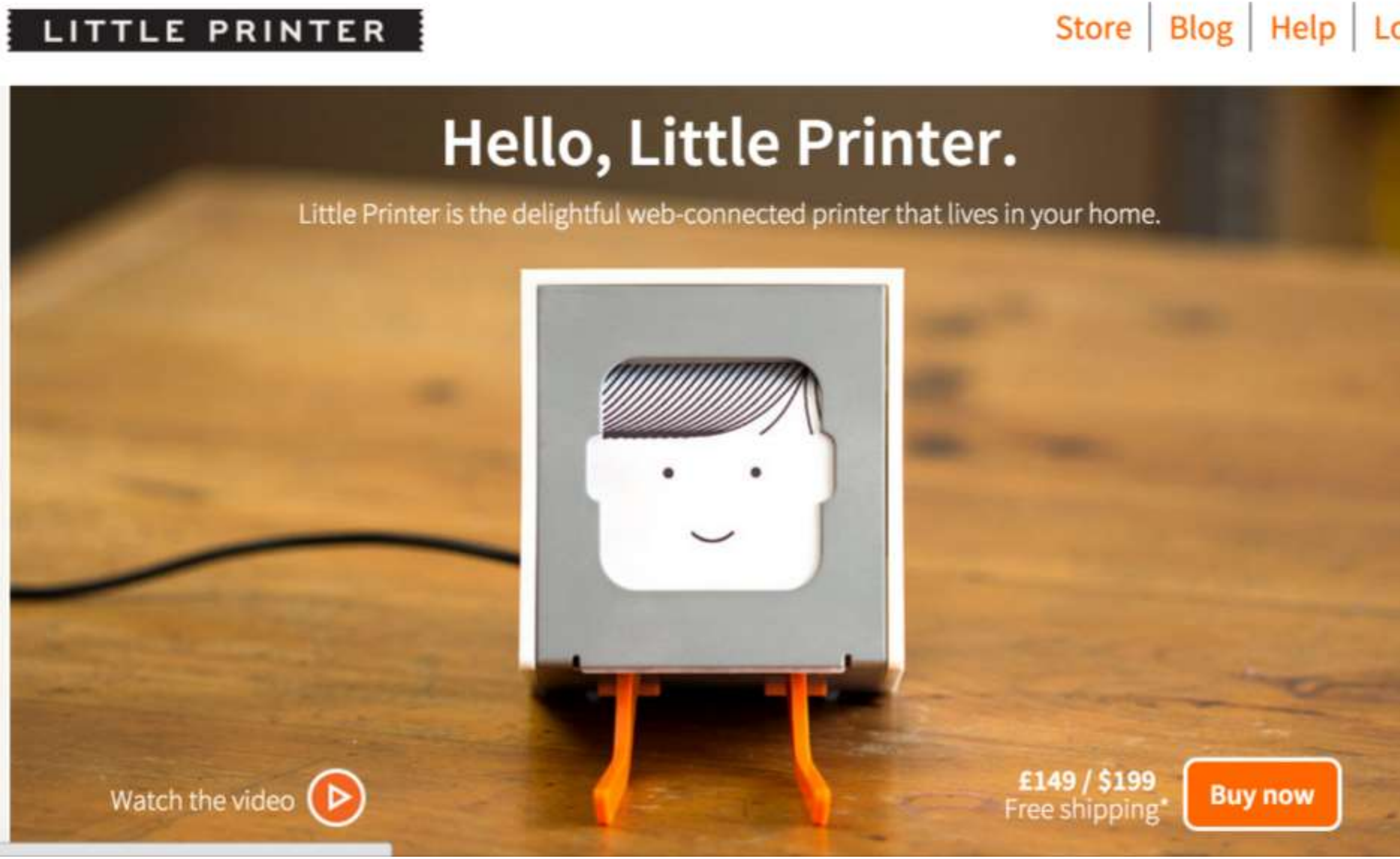
- Can enable a meaningful consent mechanism for sharing of device data
- Giving a device a token to use on API calls better than giving it a password
  - Revokable
  - Granular
- May be relevant for both
  - Device to cloud
  - Cloud to app

Why really?

Your IoT data privacy should not rely on the maker of a specific device

Relying on the maker of your device?

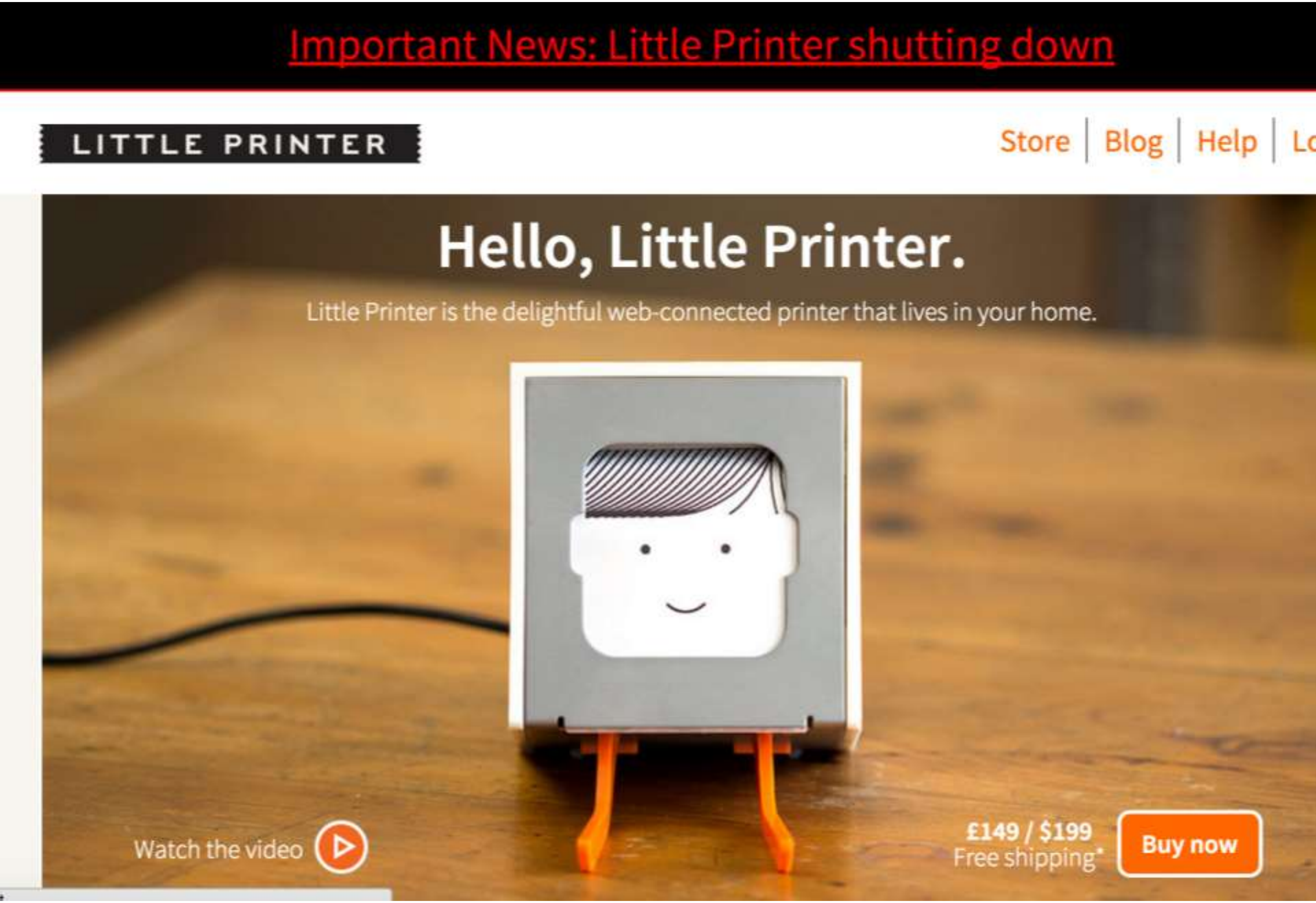
lenovo 联想
Superfish Malware
Kills HTTPS
Bad Guys!



Hello, Little Printer.

Little Printer is the delightful web-connected printer that lives in your home.

£149 / $199
Free shipping*

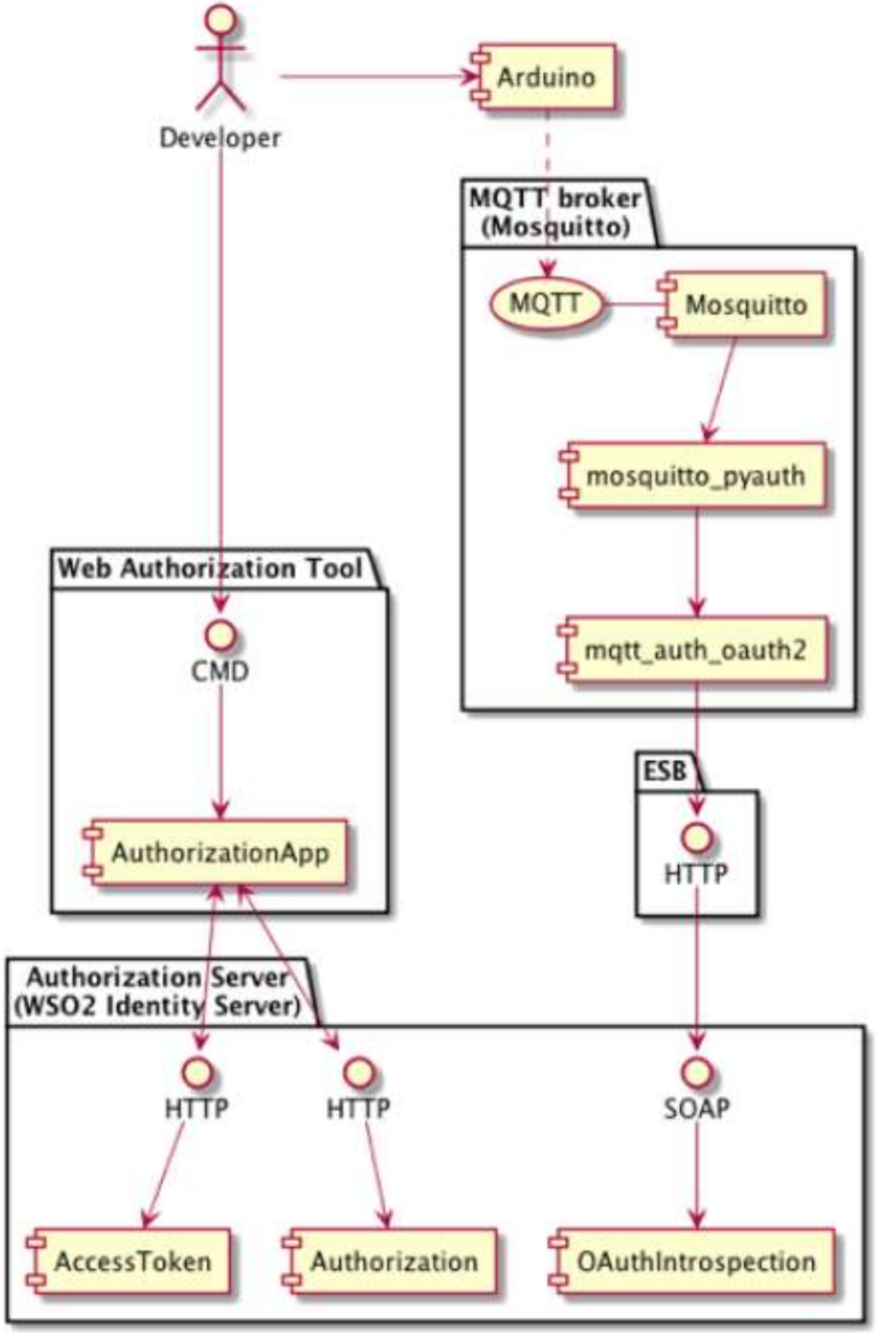


Important News: Little Printer shutting down

LITTLE PRINTER

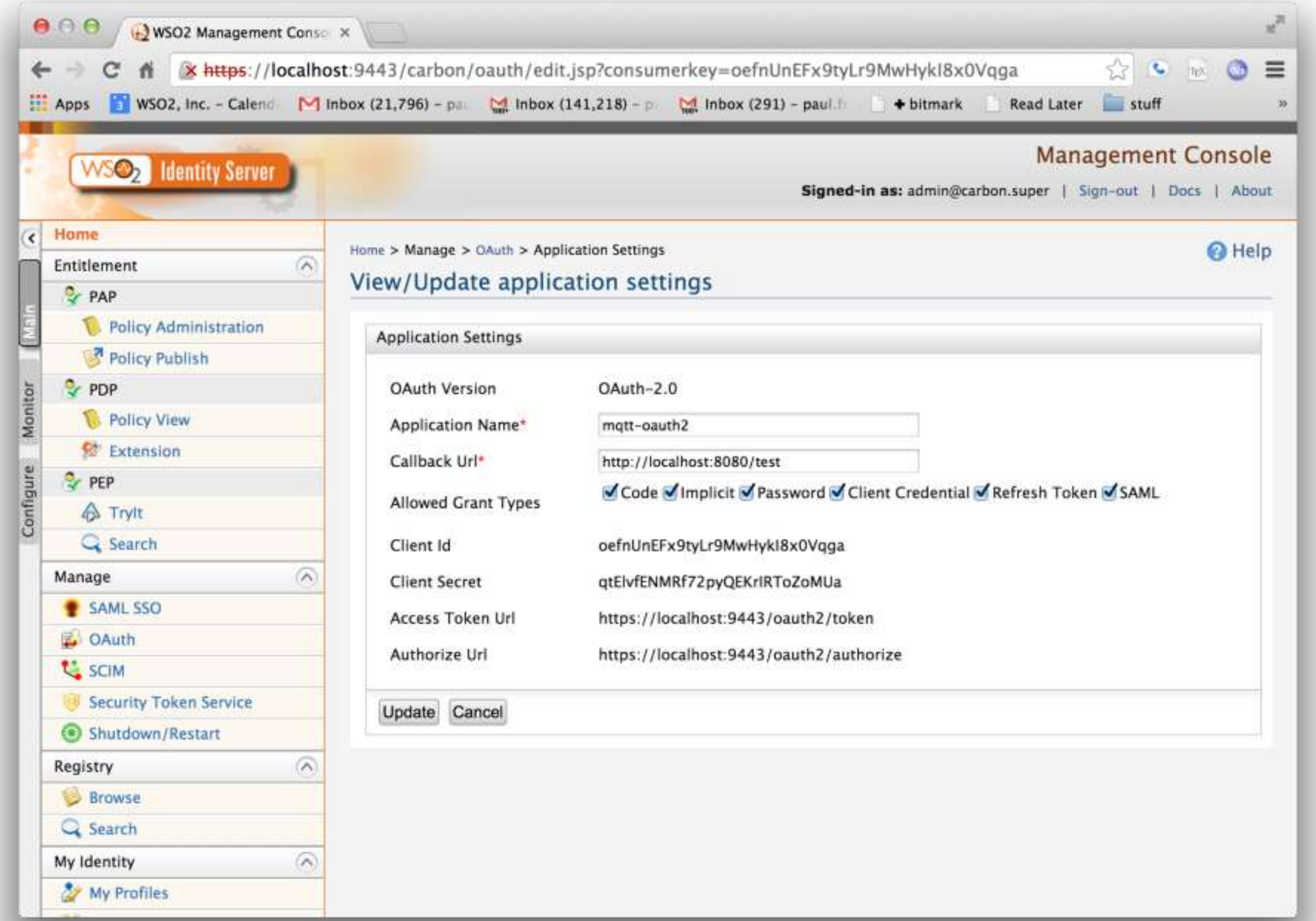
Hello, Little Printer.

Little Printer is the delightful web-connected printer that lives in your home.


Developer
Arduino
MQTT broker
(Mosquitto)
MQTT
Mosquitto
mosquitto_pyauth
mqtt_auth_oauth2
Web Authorization Tool
CMD
AuthorizationApp
ESB
HTTP
Authorization Server
(WSO2 Identity Server)
HTTP
HTTP
SOAP
AccessToken
Authorization
OAuthIntrospection

Device to Cloud

- Put an OAuth2 token on the device
- Set the “scope” to be limited
  - This device can publish to this topic
- Support refresh model



Home > Manage > OAuth > Application Settings

View/Update application settings

Application Settings

OAuth Version	OAuth-2.0
Application Name*	mqtt-oauth2
Callback Url*	http://localhost:8080/test
Allowed Grant Types	☑ Code ☑ Implicit ☑ Password ☑ Client Credential ☑ Refresh Token ☑ SAML
Client Id	oefnUnEFx9tyLr9MwHykI8x0Vqga
Client Secret	qtElvfENMRf72pyQEKrlRToZoMUa
Access Token Url	https://localhost:9443/oauth2/token
Authorize Url	https://localhost:9443/oauth2/authorize

Cloud to App

- The same technology can be used to enable some app to subscribe to a specific topic
- Much easier than with Arduino!

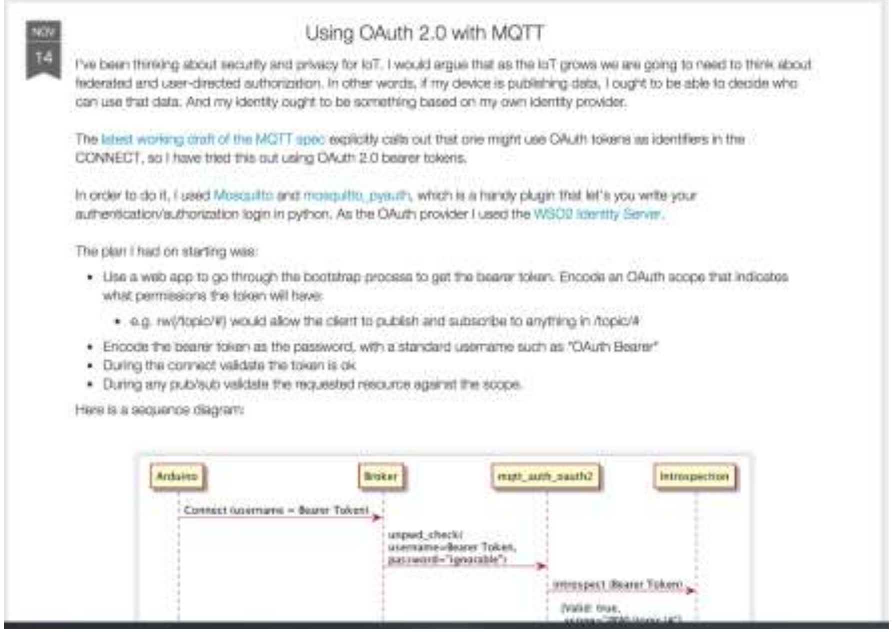
Lessons learnt

- OAuth2 Token lengths are usually ok (no promise though)
  - OpenId Connect much larger
- Registration is hard
- MQTT and MPU / I2C code is 97% of Duemilanove
  - Adding the final logic to do OAuth2 flow pushed it to 99%
  - No TLS in this demo is a big issue
- Different OAuth2 implementations behave differently
  - Need to disable updating the refresh token with every refresh
- Need to be able to update the scope of token if this will work for long term embedded devices
- MQTT needs some better designed patterns for RPC
  - Standardised

More information

http://pzf.fremantle.org/2013/11/using-oauth-20-with-mqtt.html

http://siot-workshop.org/



NOV
14

Using OAuth 2.0 with MQTT

I've been thinking about security and privacy for IoT. I would argue that as the IoT grows we are going to need to think about federated and user-directed authorization. In other words, if my device is publishing data, I ought to be able to decide who can use that data. And my identity ought to be something based on my own identity provider.

The latest working draft of the MQTT spec explicitly calls out that one might use OAuth tokens as identifiers in the CONNECT, so I have tried this out using OAuth 2.0 bearer tokens.

In order to do it, I used Mosquitto and mosquitto_pyauth, which is a handy plugin that let's you write your authentication/authorization login in python. As the OAuth provider I used the WSO2 Identity Server.

The plan I had on starting was:

- Use a web app to go through the bootstrap process to get the bearer token. Encode an OAuth scope that indicates what permissions the token will have:
  - e.g. rw(/topic/#) would allow the client to publish and subscribe to anything in /topic/#
- Encode the bearer token as the password, with a standard username such as "OAuth Bearer"
- During the connect validate the token is ok
- During any pub/sub validate the requested resource against the scope.

Here is a sequence diagram:

Arduino
Broker
mqtt_auth_oauth2
Introspection
Connect (username = Bearer Token)
unpwd_check(
username=Bearer Token,
password="ignorable")
introspect (Bearer Token)
{Valid: true,

Federated Identity and Access Management for the Internet of Things

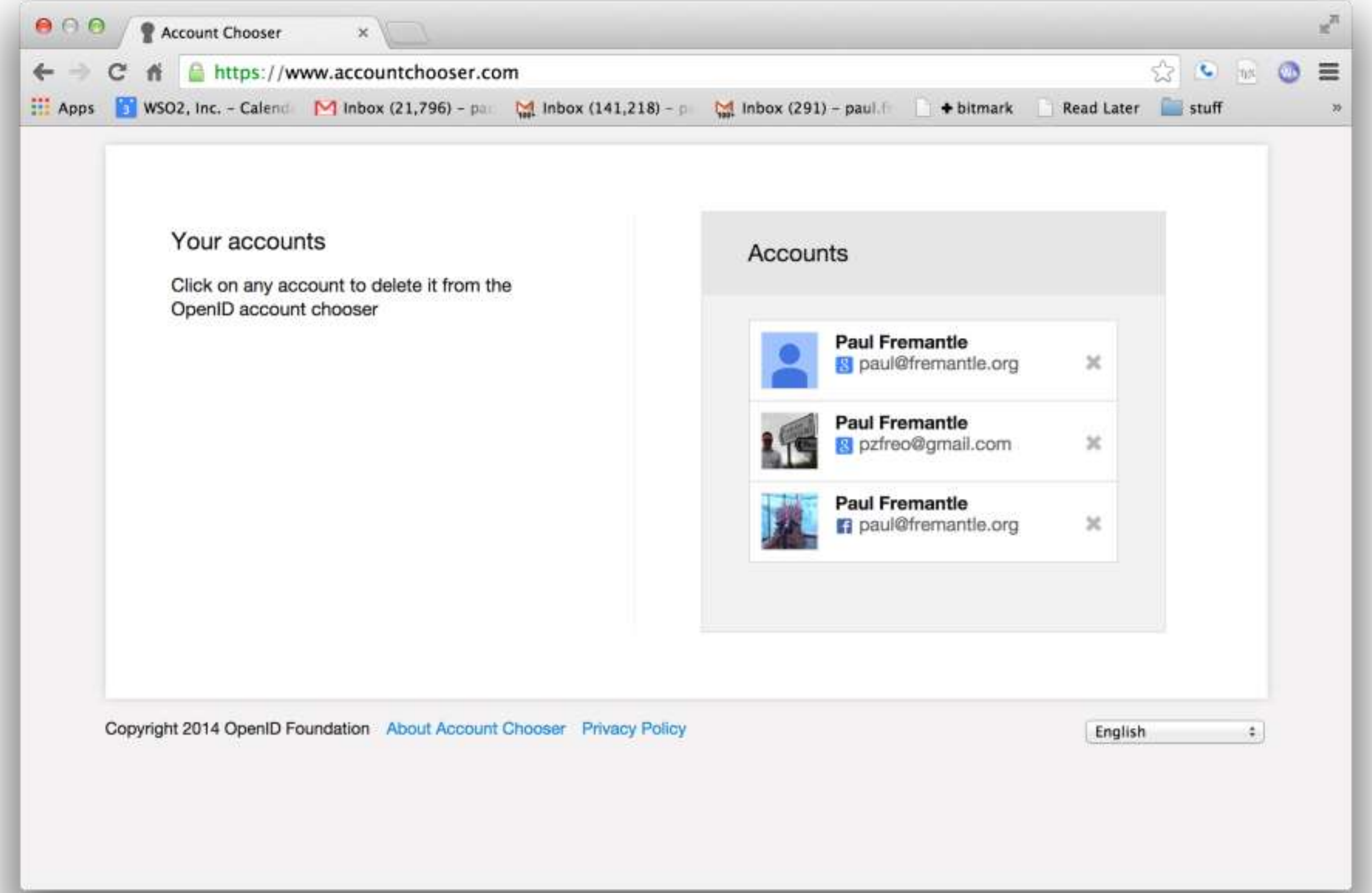
Paul Fremantle[12], Benjamin Aziz[1], Jacek Kopecký[1], and Philip Scott[1]

[1] School of Computing,
University of Portsmouth,
Portsmouth PO1 3HE, UK
{paul.fremantle,benjamin.aziz, jacek.kopecky, philip.scott}@port.ac.uk
[2] WSO2 Inc.
paul@wso2.com

Abstract. We examine the use of Federated Identity and Access Management (FIAM) approaches for the Internet of Things (IoT). We look at specific challenges that devices, sensors and actuators have, and look for approaches to address them. OAuth is a widely deployed protocol – built on top of HTTP – for applying FIAM to Web systems. We explore the use of OAuth for IoT systems that instead use the lightweight MQTT 3.1 protocol. In order to evaluate this area, we built a prototype that uses OAuth 2.0 to enable access control to information distributed via MQTT. We evaluate the results of this prototyping activity, and assess the strengths and weaknesses of this approach, and the benefits of using the FIAM approaches with IoT and Machine to Machine (M2M) scenarios. Finally we outline areas for further research.

1 Introduction

OpenId Connect



Your accounts

Click on any account to delete it from the OpenID account chooser

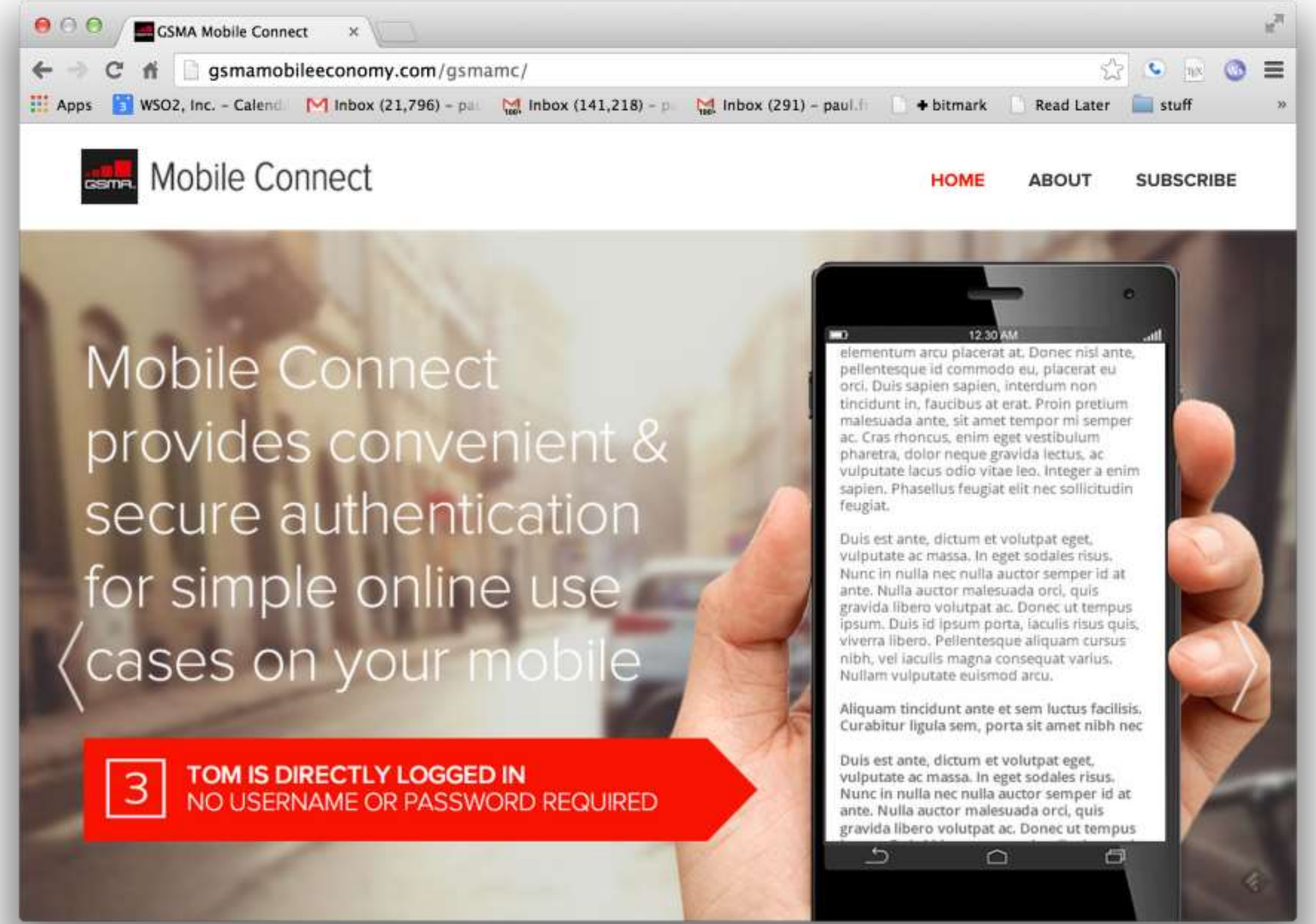
Accounts

Paul Fremantle
paul@fremantle.org

Paul Fremantle
pzfreo@gmail.com

Paul Fremantle
paul@fremantle.org

Copyright 2014 OpenID Foundation About Account Chooser Privacy Policy



Mobile Connect

Mobile Connect provides convenient & secure authentication for simple online use cases on your mobile

3 TOM IS DIRECTLY LOGGED IN
NO USERNAME OR PASSWORD REQUIRED

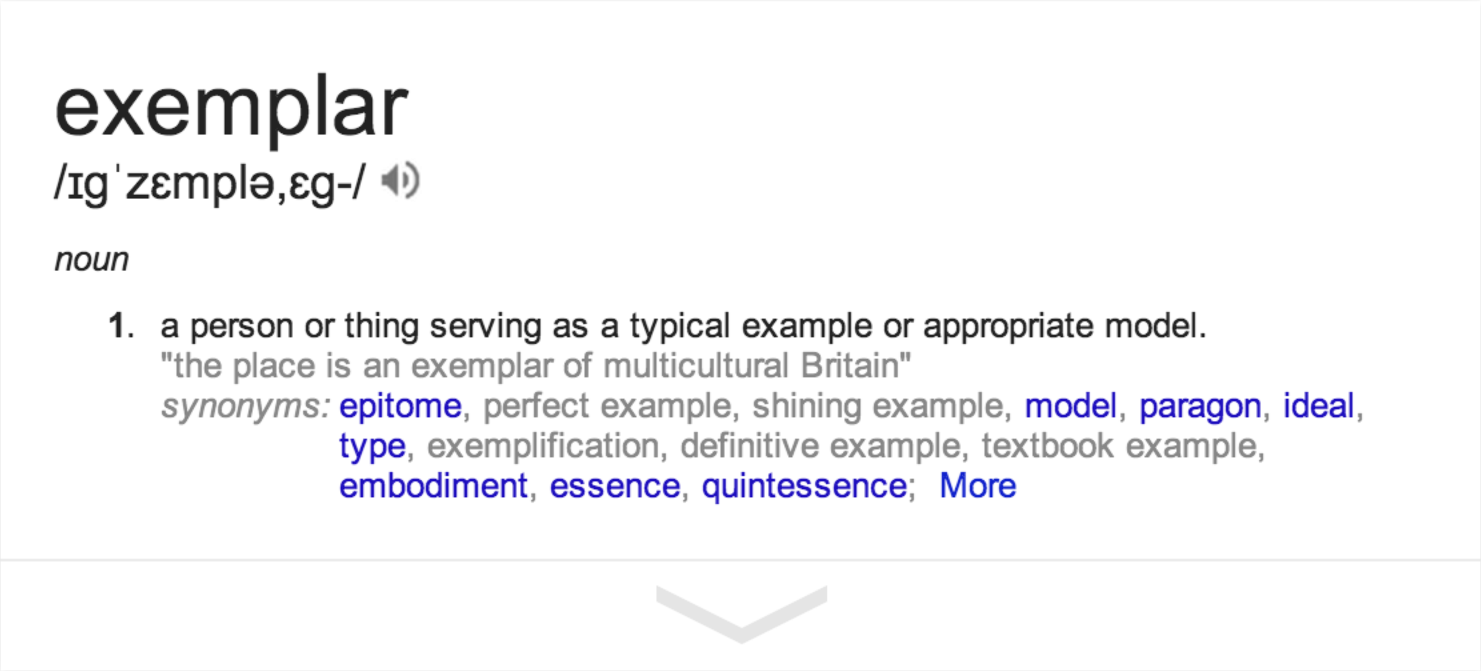
elementum arcu placerat at. Donec nisl ante, pellentesque id commodo eu, placerat eu orci. Duis sapien sapien, interdum non tincidunt in, faucibus at erat. Proin pretium malesuada ante, sit amet tempor mi semper ac. Cras rhoncus, enim eget vestibulum pharetra, dolor neque gravida lectus, ac vulputate lacus odio vitae leo. Integer a enim sapien. Phasellus feugiat elit nec sollicitudin feugiat.

Duis est ante, dictum et volutpat eget, vulputate ac massa. In eget sodales risus. Nunc in nulla nec nulla auctor semper id at ante. Nulla auctor malesuada orci, quis gravida libero volutpat ac. Donec ut tempus ipsum. Duis id ipsum porta, iaculis risus quis, viverra libero. Pellentesque aliquam cursus nibh, vel iaculis magna consequat varius. Nullam vulputate euismod arcu.

Aliquam tincidunt ante et sem luctus facilisis. Curabitur ligula sem, porta sit amet nibh nec

Duis est ante, dictum et volutpat eget, vulputate ac massa. In eget sodales risus. Nunc in nulla nec nulla auctor semper id at ante. Nulla auctor malesuada orci, quis gravida libero volutpat ac. Donec ut tempus

Are **you** creating the next privacy breach?



exemplar

/ɪɡˈzɛmplə,ɛɡ-/

noun

1. a person or thing serving as a typical example or appropriate model.
   "the place is an exemplar of multicultural Britain"
   synonyms: epitome, perfect example, shining example, model, paragon, ideal, type, exemplification, definitive example, textbook example, embodiment, essence, quintessence; More

Summary

- Think about security with your next device
- We as a community need to make sure that the next generation of IoT devices are secure
- We need to create exemplars
  - Shields
  - Libraries
  - Server software
  - Standards

http://upload.wikimedia.org/wikipedia/commons/c/c8/Thank_you_001.jpg