RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-W03

When Worlds Collide: IoT meets ICS

Larry Pesce

Director of Research &
Sr. Managing Security Consultant
InGuardians
@haxorthematrix

A Little Background

Back in my day…

Welcome to the New Reality

- IoT gives me that “get off my lawn” moment
- In only a few short years, access to the internet has gone from a privilege to a right
- It has also spilled from our PC to our phone to our toys and even our homes
- No, not in our homes, the *actual* home.

Toys

Advanced Toys

High Tech Toys

Change the temperature?

High tech temperature change

Getting money from the bank?

Or this?

InGuardians™ Advanced Persistent Testing

High Tech Queues

Medicine?

High Tech Medicine

We’ve grown up

- We have come so far in so little time!
- Think about those same scenarios *today*.
- How about a refresher?

What about the now?

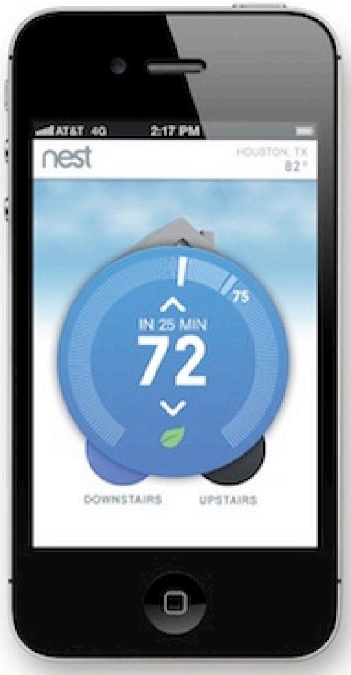
Damned kids, get off my lawn!

My Kid’s Toys

InGuardians™
Advanced Persistent Testing

Go outside!

Turn up the heat!

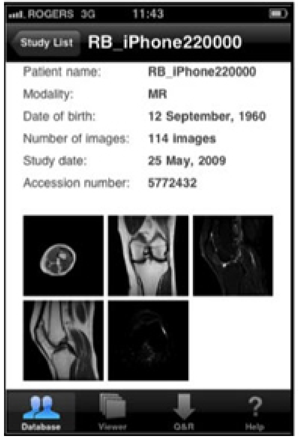


Banking?

Citizens Bank is a brand name of Citizens, N.A. and Citizens Bank of Pennsylvania

InGuardians™
Advanced Persistent Testing

Medicine


ROGERS 3G 11:43

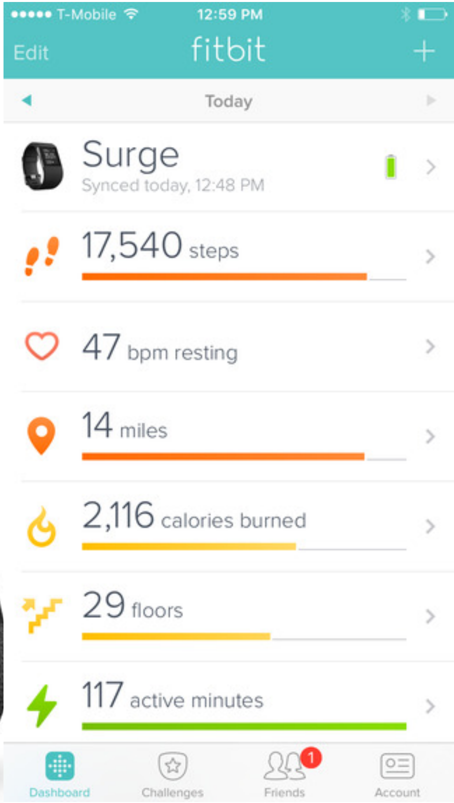
Study List RB_iPhone220000

Patient name: RB_iPhone220000
Modality: MR
Date of birth: 12 September, 1960
Number of images: 114 images
Study date: 25 May, 2009
Accession number: 5772432

ROGERS 3G 11:44

RB_iPhone220000

WL: 807 WW: 2767
Zoom: 96%


T-Mobile 12:59 PM

Edit fitbit +

Today

Surge
Synced today, 12:48 PM

17,540 steps

47 bpm resting

14 miles

2,116 calories burned

29 floors

117 active minutes

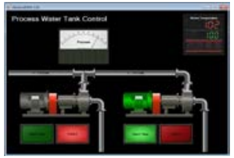
But, Larry…

- How does all this new fangled tech hurt us?
- More importantly how are these IoT devices impacting ICS?
- I don’t want this to sound like FUD, but this is a little forward looking into some perceived threats.
  - I’m of the opinion all of the parts are there
  - Attackers just need to put the parts together

Lets examine a few scenarios!

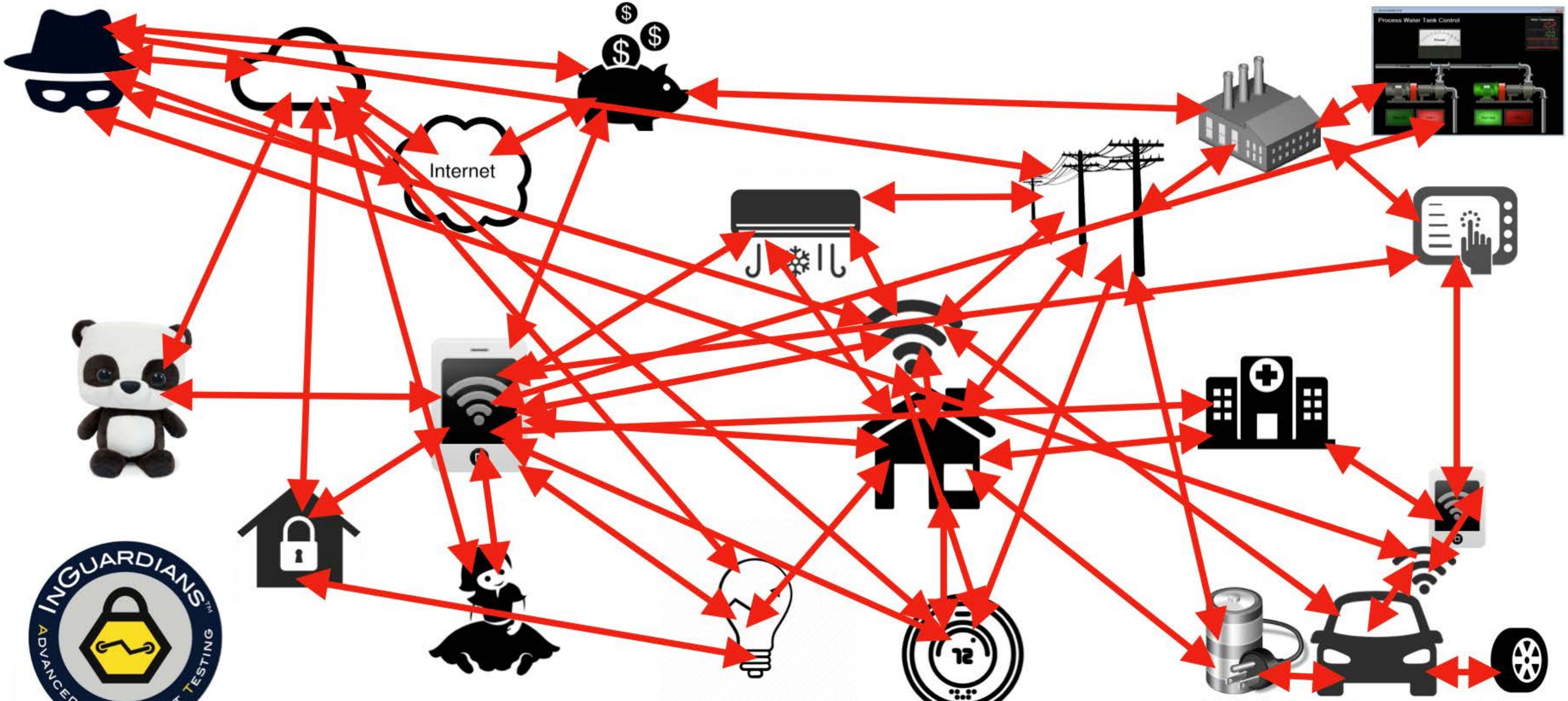
Services

Internet


Process Water Tank Control

INGUARDIANS™
ADVANCED PERSISTENT TESTING

Services



INGUARDIANS™
ADVANCED PERSISTENT TESTING

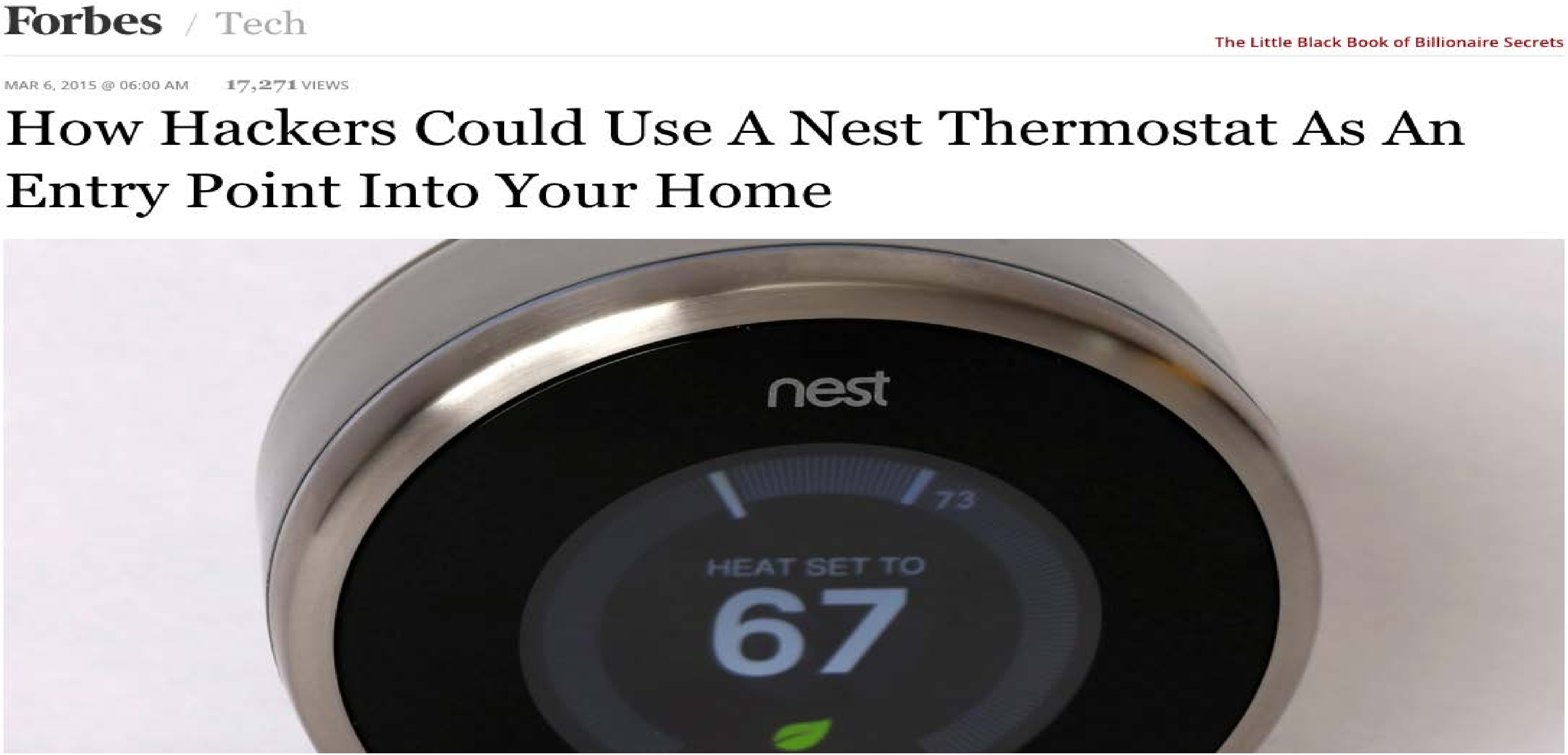
Attack Scenarios

Time to bring the pain

Scenario One

- “Hack” the grid with a “bump”
  - Shed, Demand, Shed, Demand
- Control of the A/C with a mobile app local with Bluetooth
- Needs large area to affect grid, maybe over multiple distribution
  - Go for a cloud controlled service
- Nest, IRIS all interact with Mobile, HAN, HAN devices
- How do we make this happen?

Nesting



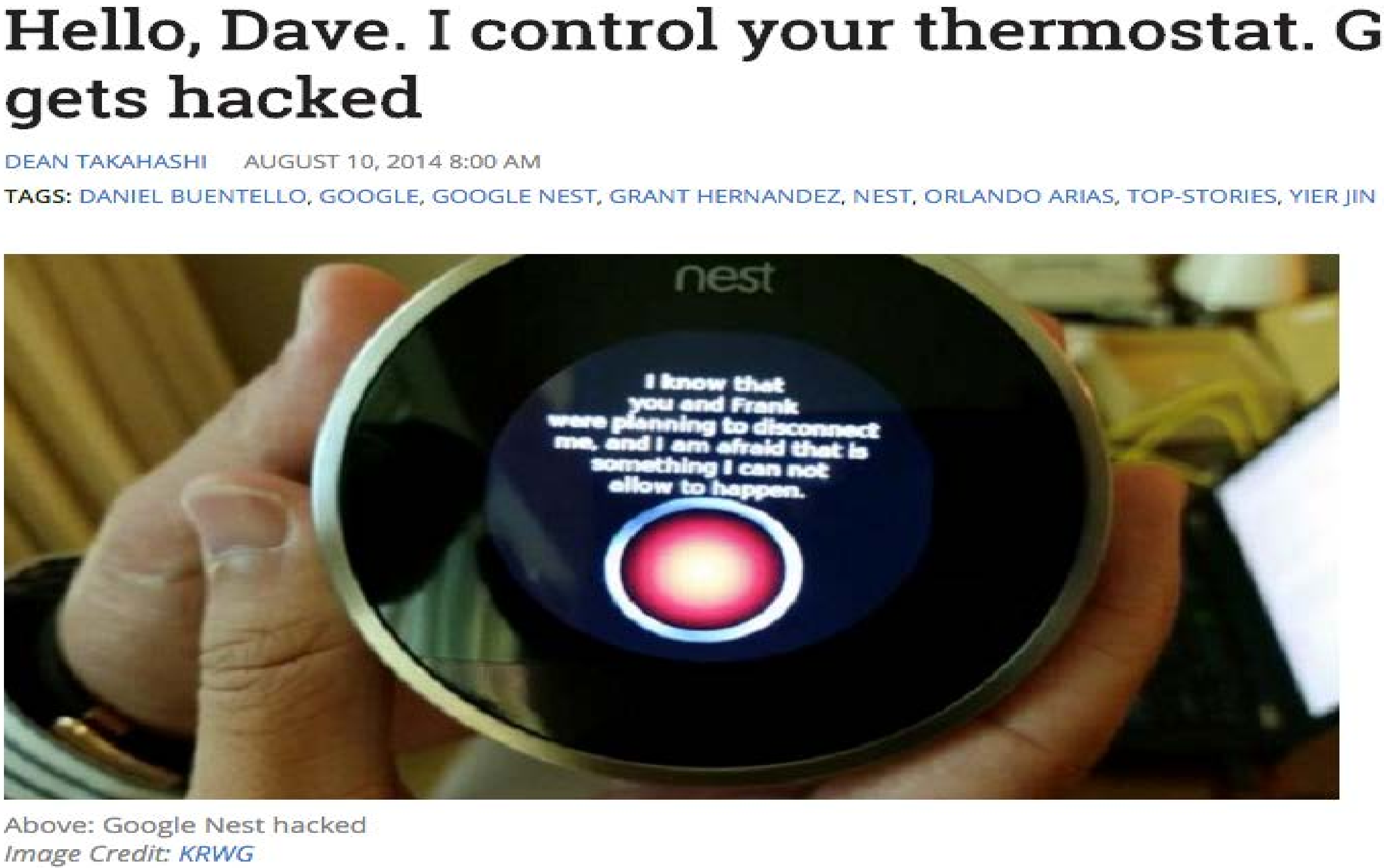
Forbes / Tech

The Little Black Book of Billionaire Secrets

MAR 6, 2015 @ 06:00 AM 17,271 VIEWS

How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home

Sorry Dave



Hello, Dave. I control your thermostat. Google's Nest gets hacked

DEAN TAKAHASHI AUGUST 10, 2014 8:00 AM

TAGS: DANIEL BUENTELLO, GOOGLE, GOOGLE NEST, GRANT HERNANDEZ, NEST, ORLANDO ARIAS, TOP-STORIES, YIER JIN

nest
I know that you and Frank were planning to disconnect me, and I am afraid that is something I can not allow to happen.

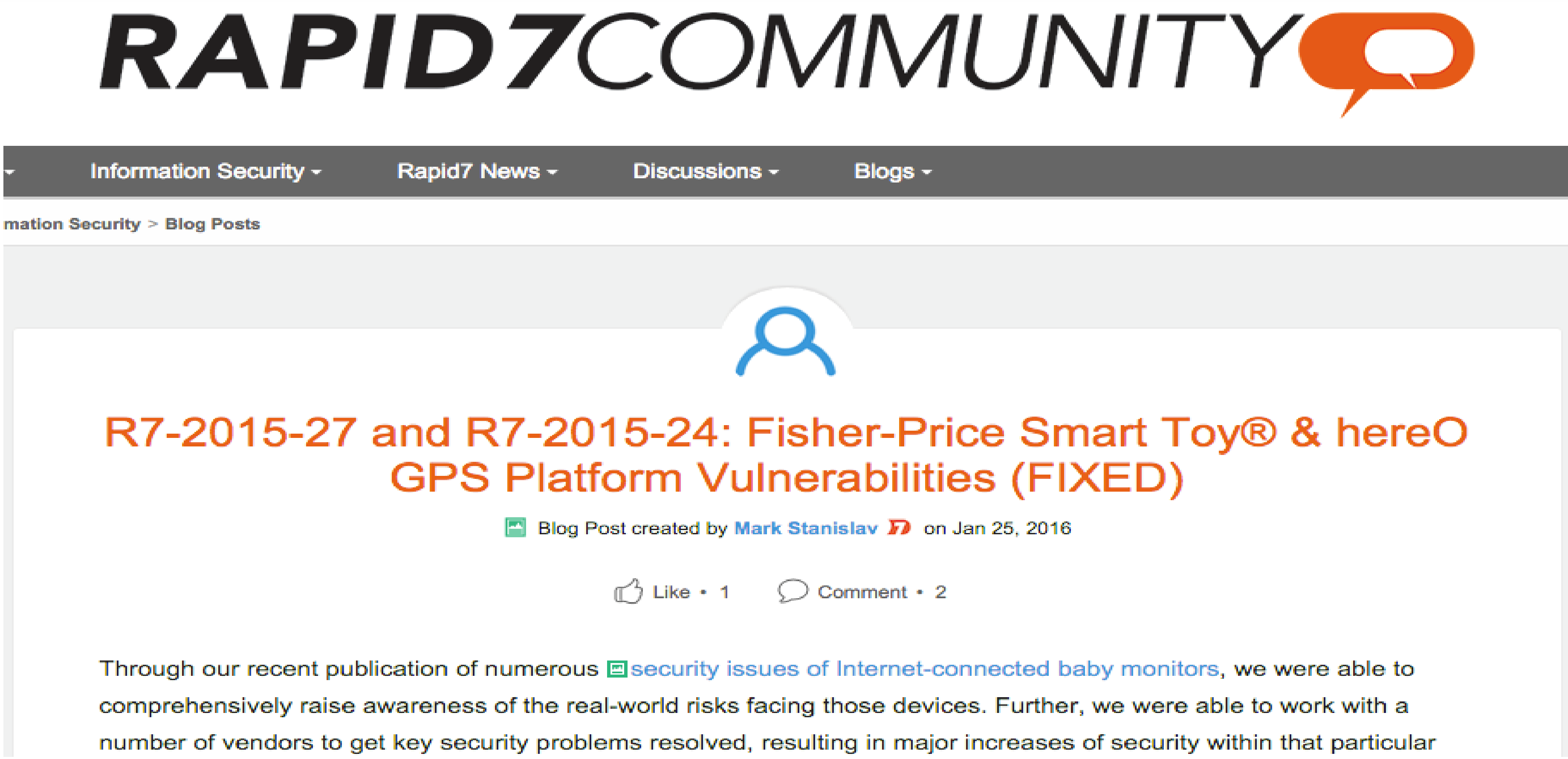
Above: Google Nest hacked

Image Credit: KRWG

Scenario Two (1)

- But where are the toys coming in to this?
- Smart Toy is an Android tablet wrapped in fluff
- Kayla and Hello Barbie can be used for shenanigans
- Heck, just go for the tablet!
  - Kids have less training on bad things
  - So many (shady) games, in app purchases and crazy permissions

Sad Panda

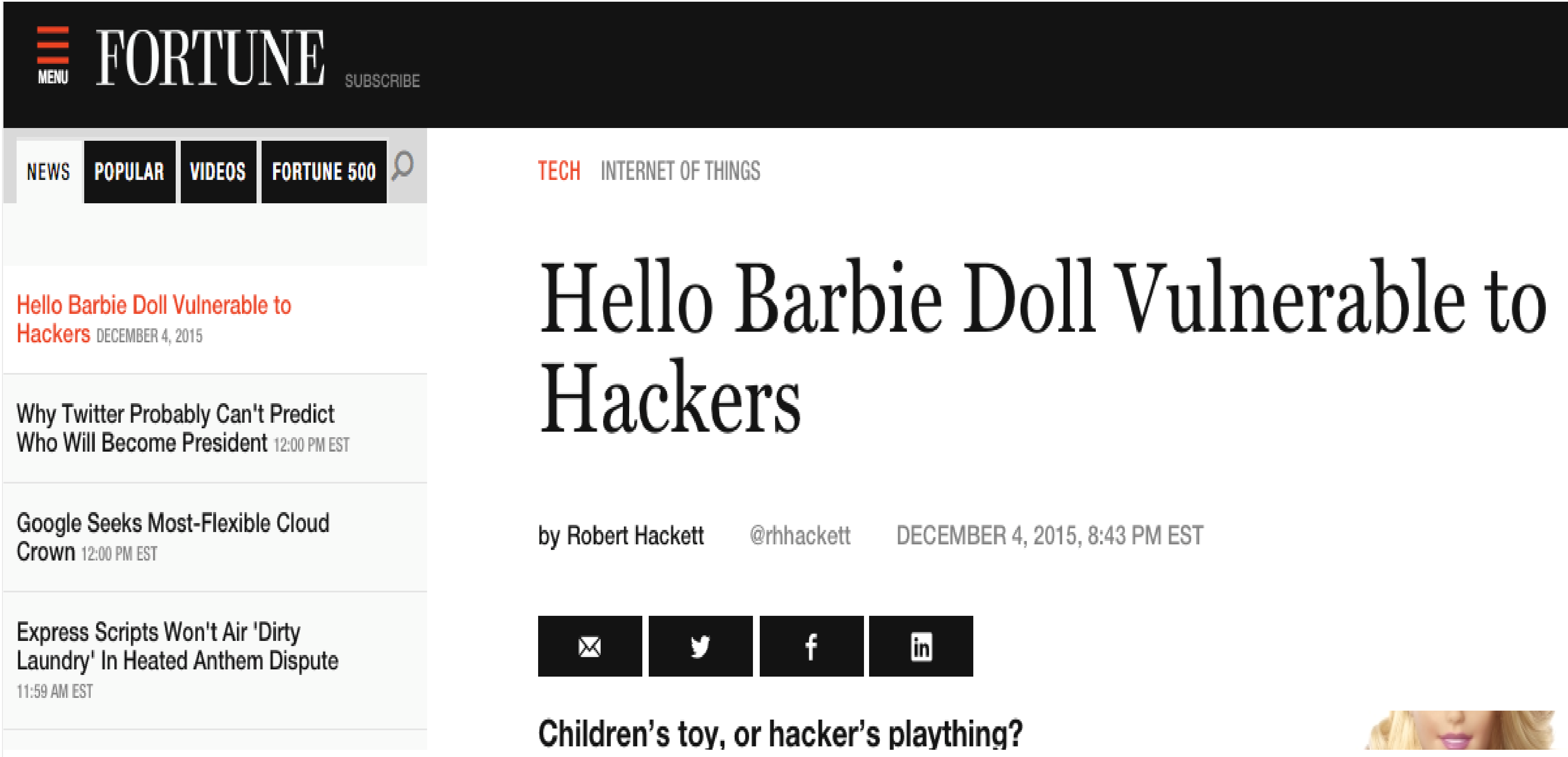


R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy® & hereO GPS Platform Vulnerabilities (FIXED)

Blog Post created by Mark Stanislav on Jan 25, 2016

Through our recent publication of numerous security issues of Internet-connected baby monitors, we were able to comprehensively raise awareness of the real-world risks facing those devices. Further, we were able to work with a number of vendors to get key security problems resolved, resulting in major increases of security within that particular

Hello, hacked Barbie



Hello Barbie Doll Vulnerable to Hackers DECEMBER 4, 2015

Why Twitter Probably Can't Predict Who Will Become President 12:00 PM EST

Google Seeks Most-Flexible Cloud Crown 12:00 PM EST

Express Scripts Won't Air 'Dirty Laundry' In Heated Anthem Dispute 11:59 AM EST

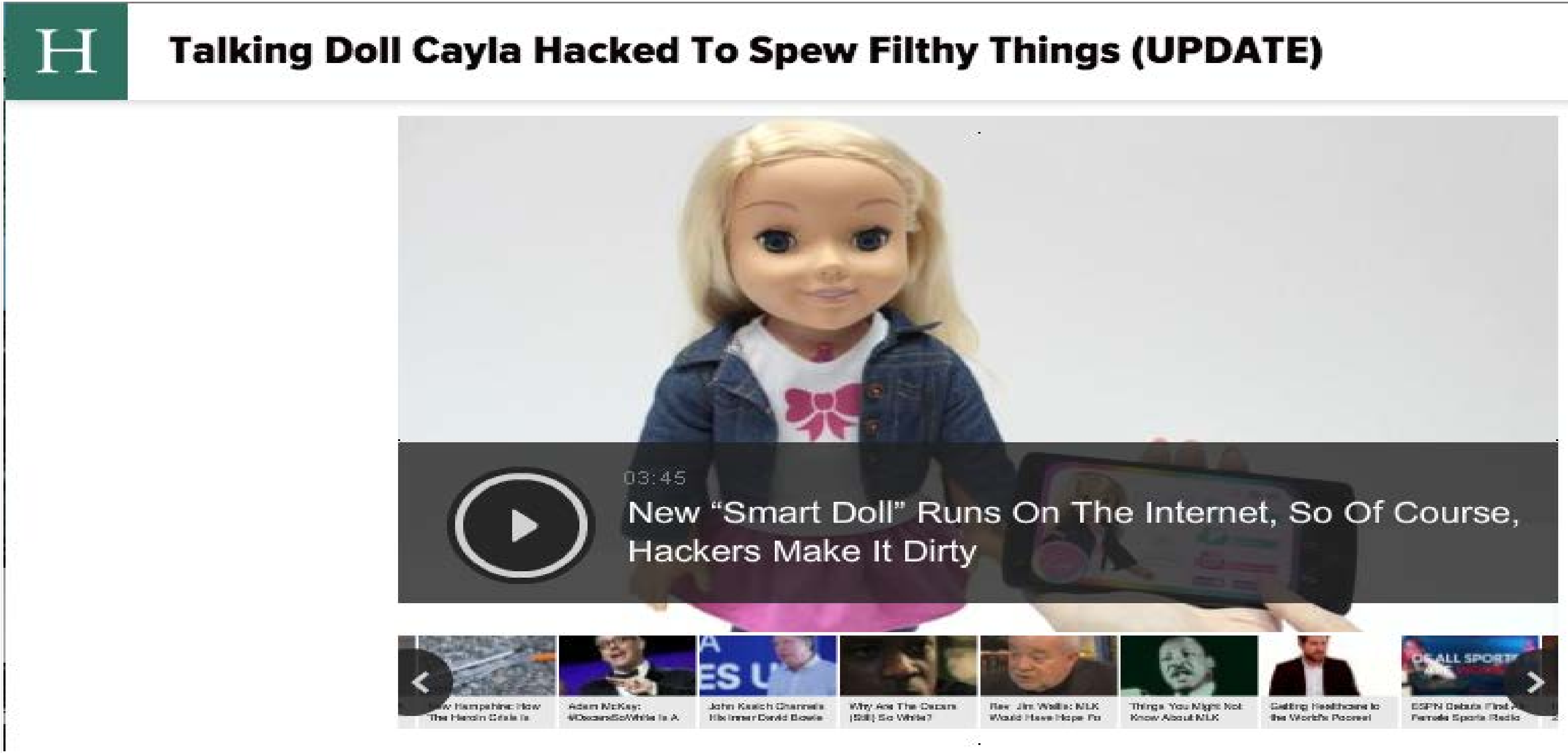
TECH INTERNET OF THINGS

Hello Barbie Doll Vulnerable to Hackers

by Robert Hackett @rhhackett DECEMBER 4, 2015, 8:43 PM EST

Children's toy, or hacker's plaything?

Naughty Cayla



H

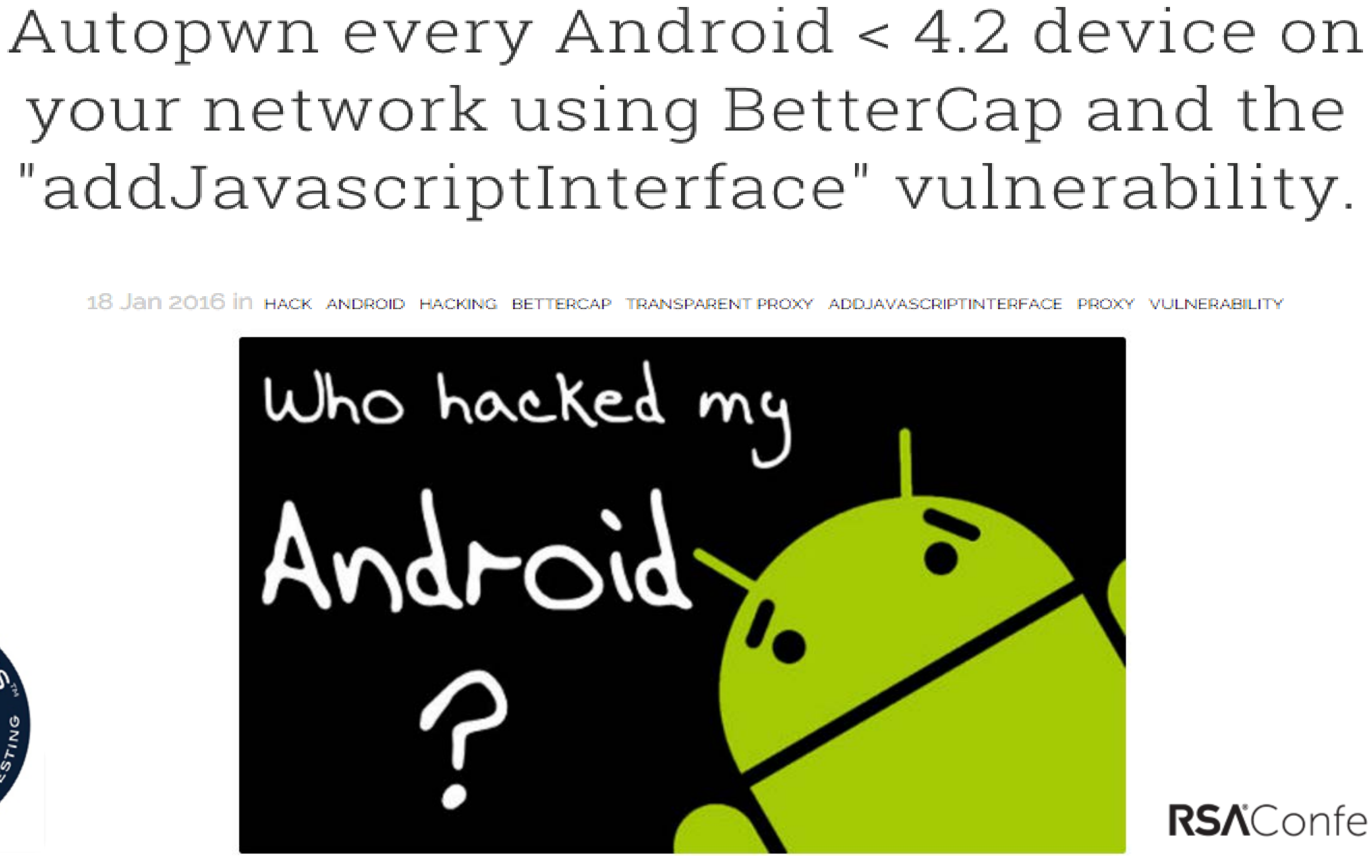
Talking Doll Cayla Hacked To Spew Filthy Things (UPDATE)

03:45

New “Smart Doll” Runs On The Internet, So Of Course, Hackers Make It Dirty

w Hampshire: How The Heroin Crisis Is
Adam McKay: #OscarsSoWhite Is A
John Kasich Channels His Inner David Bowie
Why Are The Oscars (Still) So White?
Rev. Jim Wallis: MLK Would Have Hope Fo
Things You Might Not Know About MLK
Getting Healthcare to the World's Poorest
ESPN Debuts First A Female Sports Radio

Tablet time



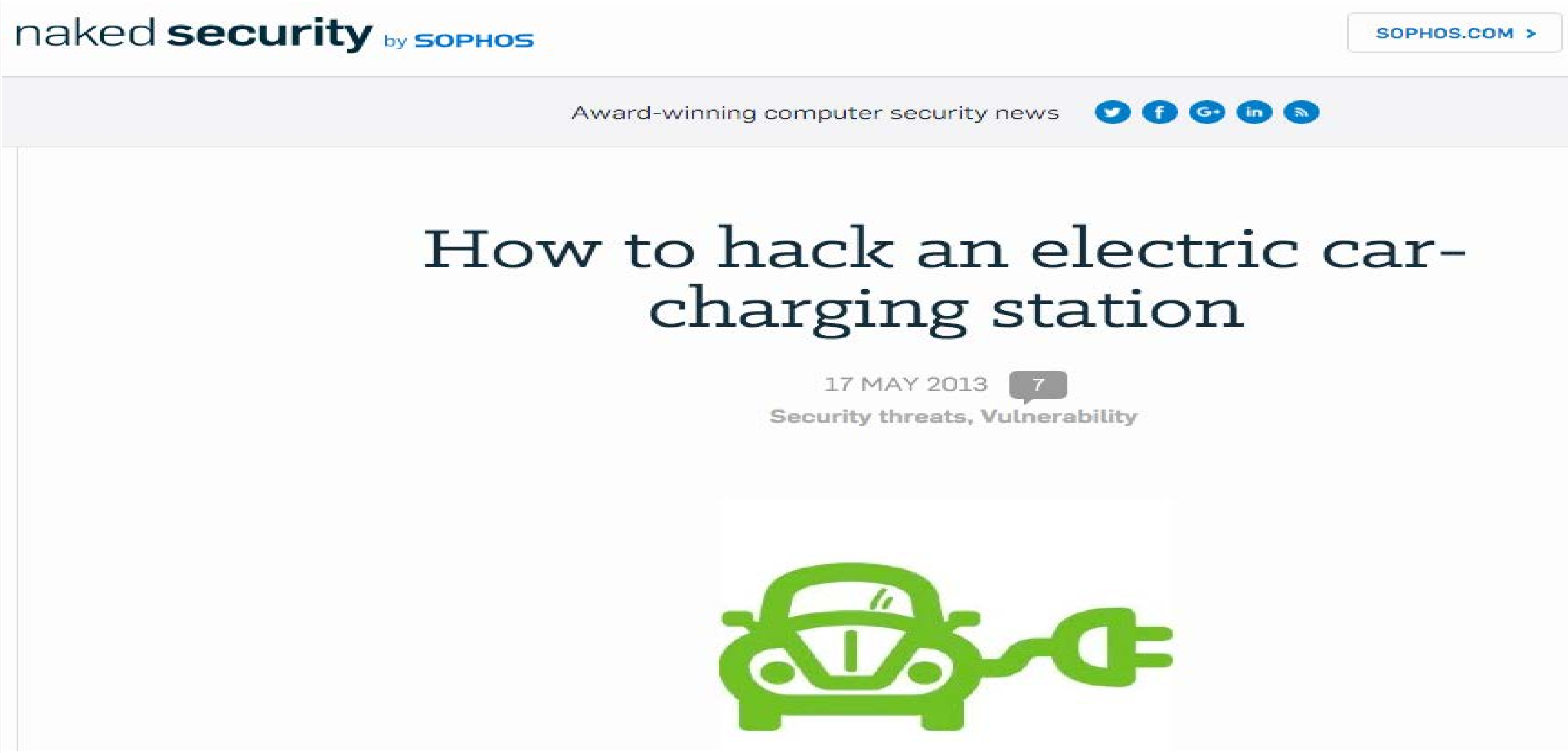
Autopwn every Android < 4.2 device on your network using BetterCap and the "addJavascriptInterface" vulnerability.

18 Jan 2016 in HACK ANDROID HACKING BETTERCAP TRANSPARENT PROXY ADDJAVASCRIPTINTERFACE PROXY VULNERABILITY

Scenario Two (2)

- All of these are just gateways to other devices
  - Home Security, car chargers, cars,
  - Amazon Echo anyone?
- So many additional interconnects!
  - None of these have issues…

Shocking



naked security by SOPHOS

SOPHOS.COM >

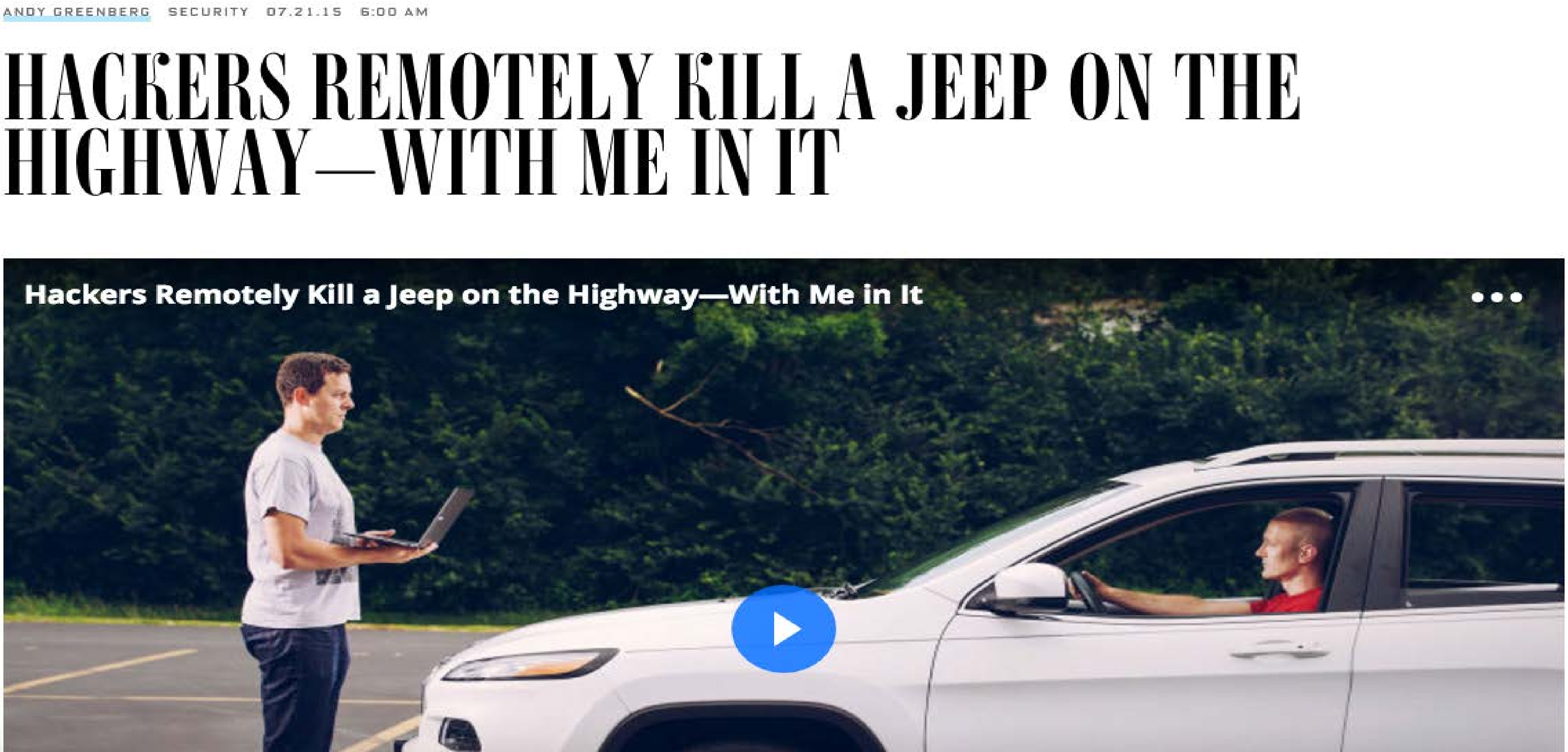
Award-winning computer security news

How to hack an electric car-charging station

17 MAY 2013 7

Security threats, Vulnerability

Zoom zoom!

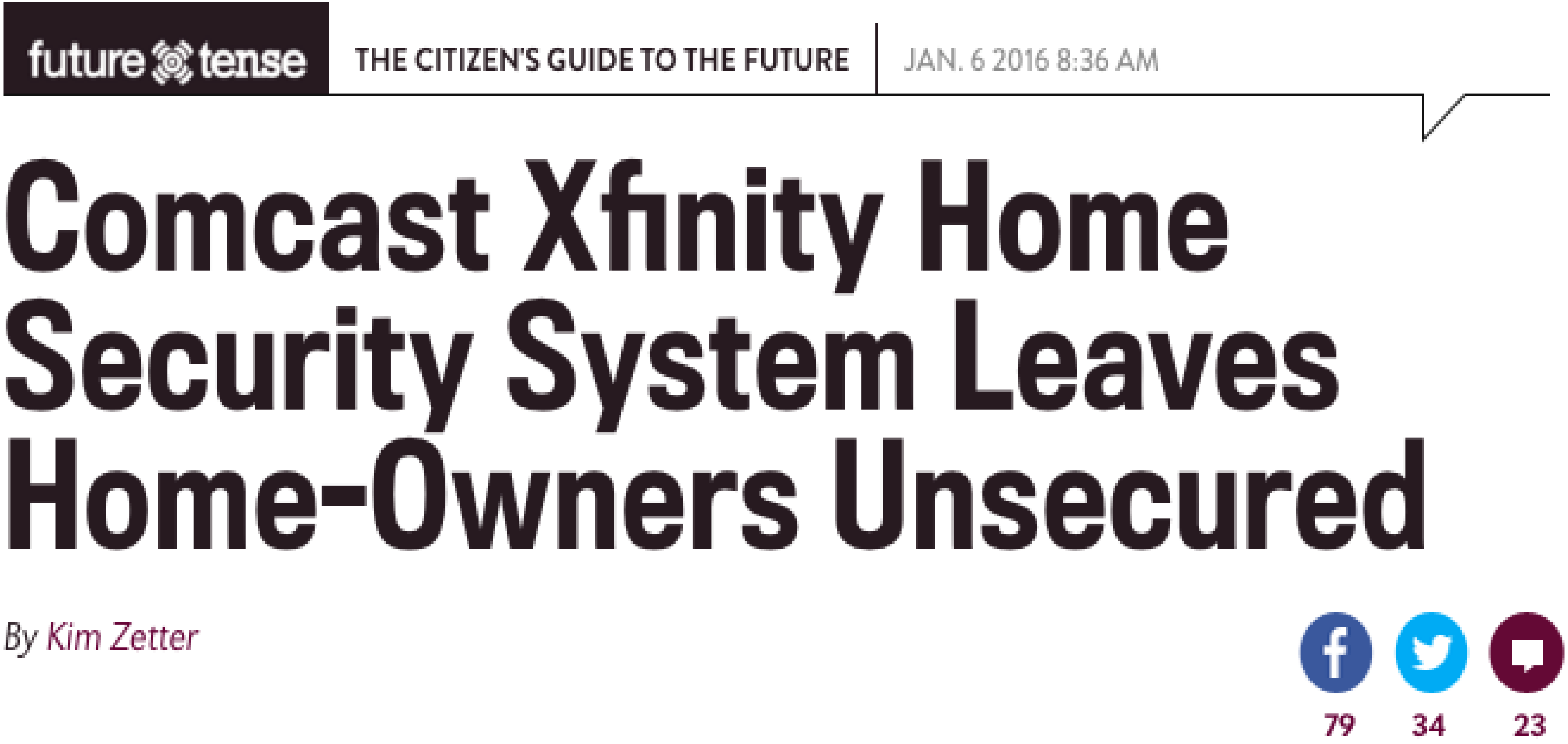


ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Home Security?

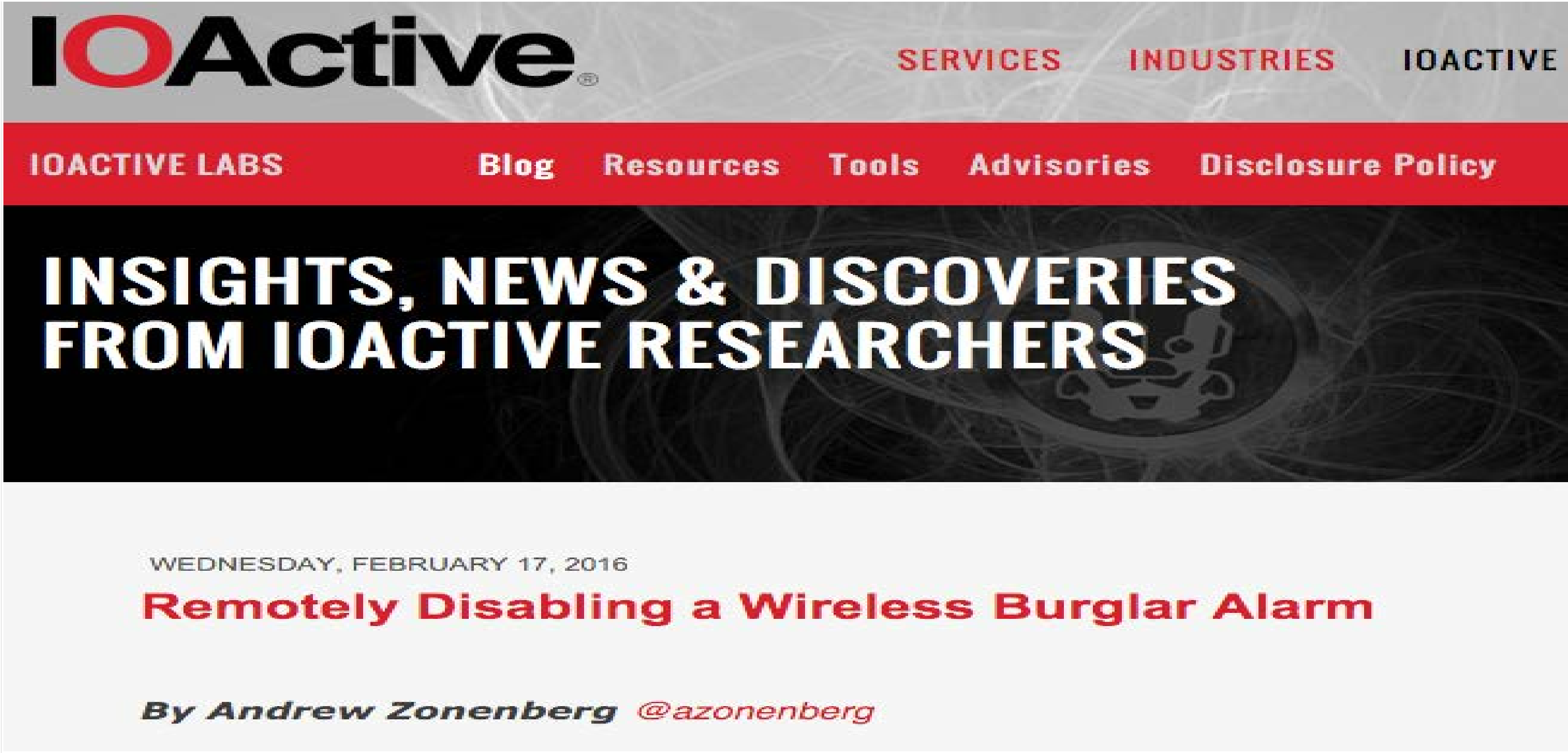


future tense THE CITIZEN'S GUIDE TO THE FUTURE JAN. 6 2016 8:36 AM

Comcast Xfinity Home Security System Leaves Home-Owners Unsecured

By Kim Zetter

Home Security Security?



INSIGHTS, NEWS & DISCOVERIES FROM IOACTIVE RESEARCHERS

WEDNESDAY, FEBRUARY 17, 2016

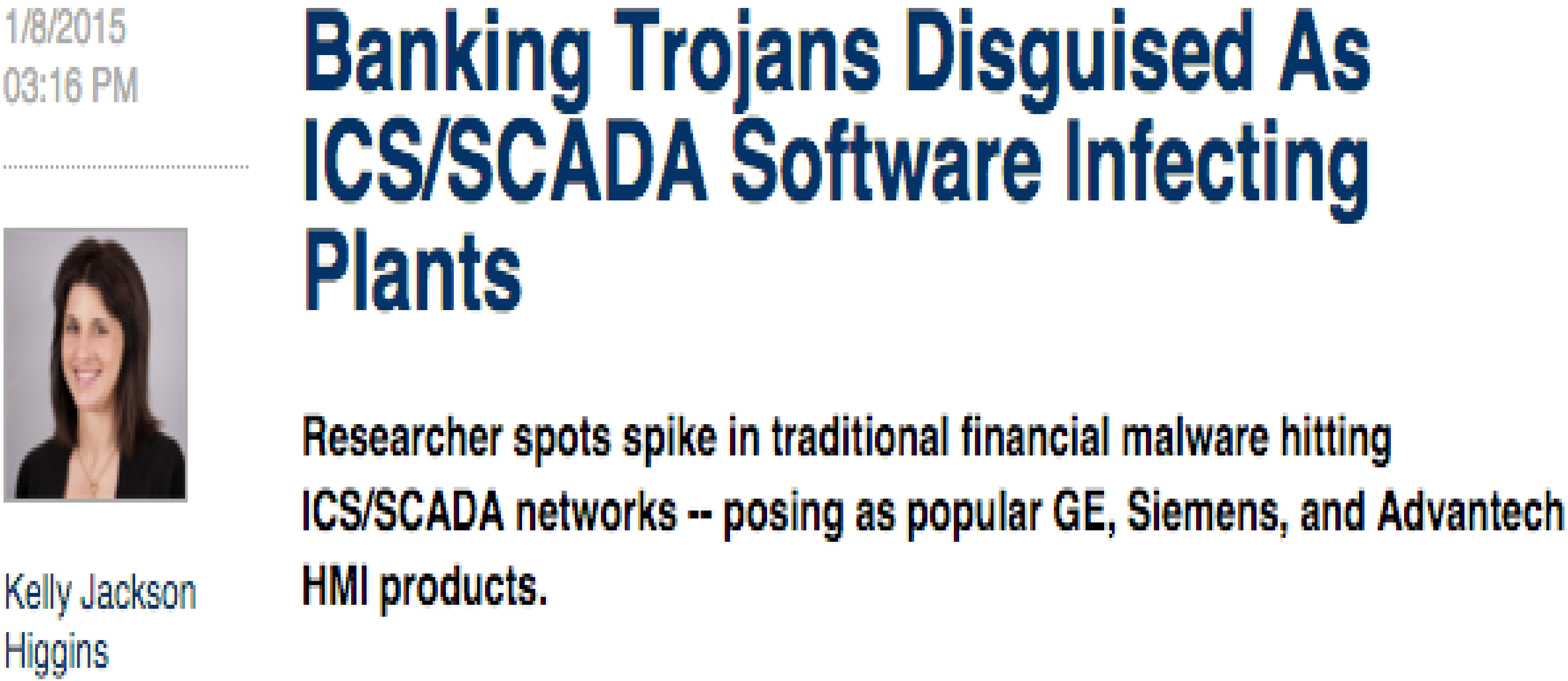
Remotely Disabling a Wireless Burglar Alarm

By Andrew Zonenberg @azonenberg

Banking

- Banking was a little harder
- Banking trojans abound, maybe compromising devices
- In a strange reversal of fortune…

Backwards!



1/8/2015
03:16 PM

Kelly Jackson Higgins

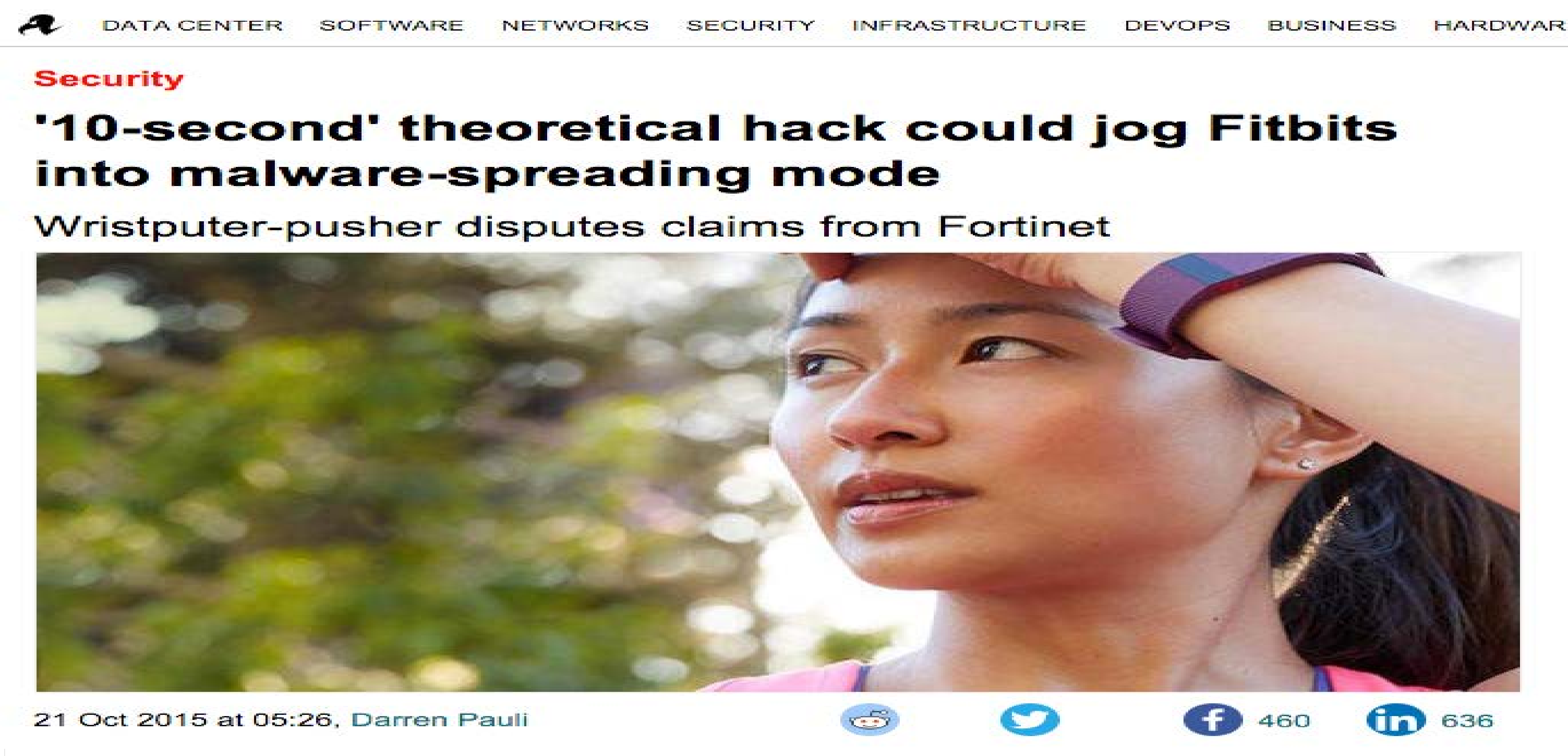
Banking Trojans Disguised As ICS/SCADA Software Infecting Plants

Researcher spots spike in traditional financial malware hitting ICS/SCADA networks -- posing as popular GE, Siemens, and Advantech HMI products.

Healthcare

- Connected “medical” devices?
  - Infusion pumps
  - Fitness trackers
  - MRI machines! (I can’t find the images, but check out @Viss’ twitter stream
- Now if these had issues, they could be used as additional vectors to interact with local or remote SCADA equipment…

Fitness Trackers



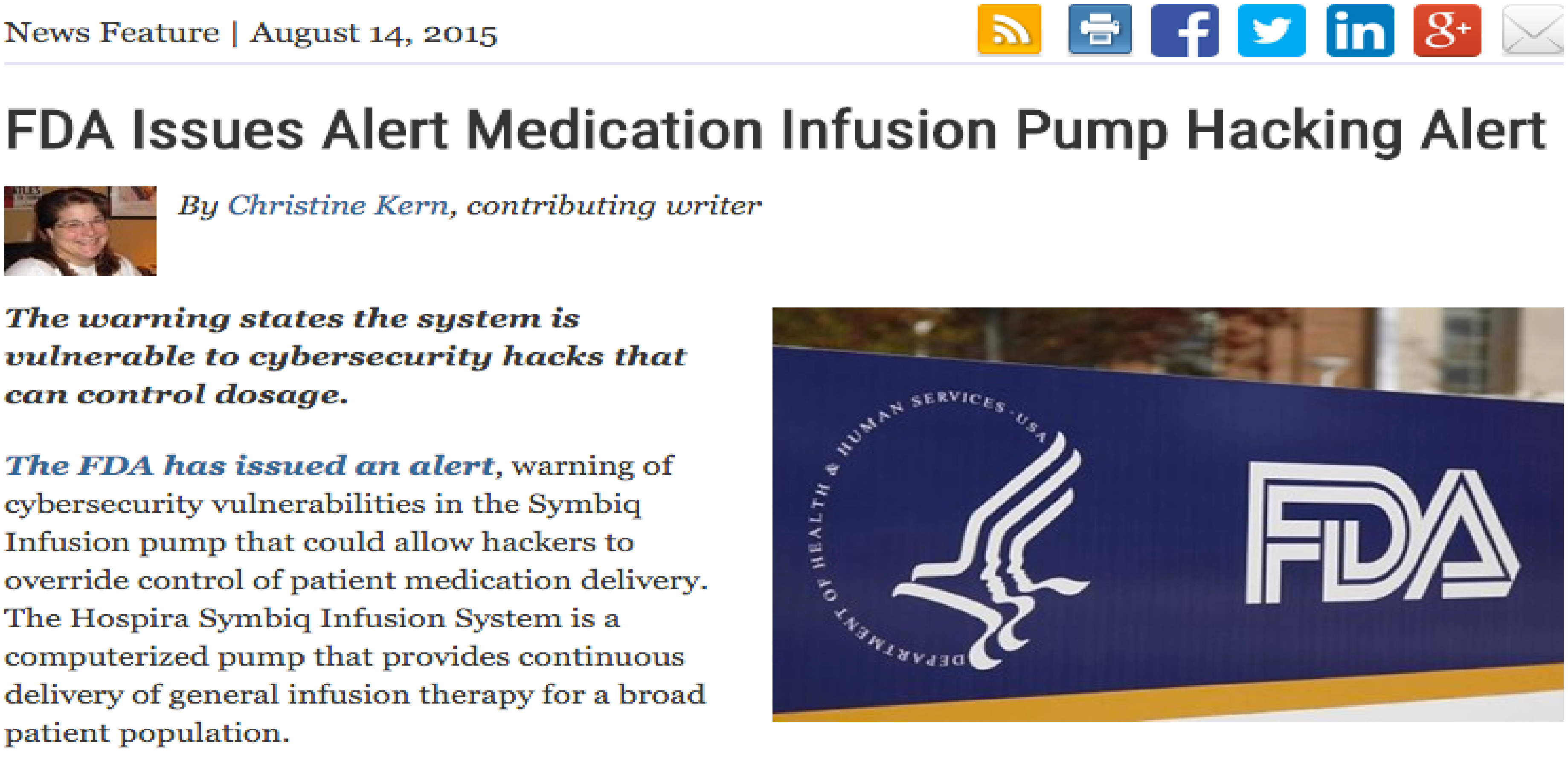
Security

'10-second' theoretical hack could jog Fitbits into malware-spreading mode

Wristputer-pusher disputes claims from Fortinet

21 Oct 2015 at 05:26, Darren Pauli

Medical Devices



News Feature | August 14, 2015

FDA Issues Alert Medication Infusion Pump Hacking Alert

By Christine Kern, contributing writer

The warning states the system is vulnerable to cybersecurity hacks that can control dosage.

The FDA has issued an alert, warning of cybersecurity vulnerabilities in the Symbiq Infusion pump that could allow hackers to override control of patient medication delivery. The Hospira Symbiq Infusion System is a computerized pump that provides continuous delivery of general infusion therapy for a broad patient population.

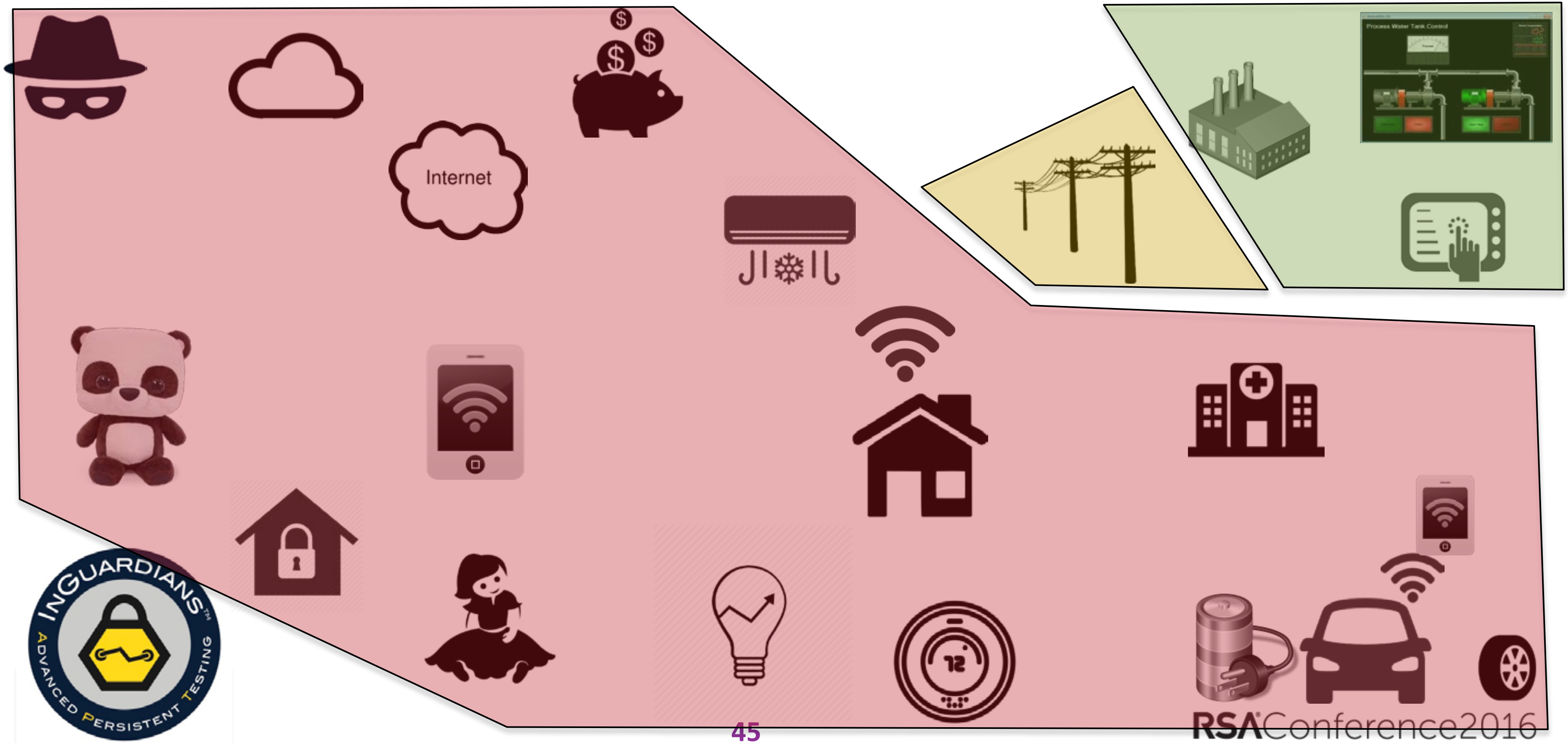
Threat Landscape?

Time to get the lawn mower

Critical mass

- Every one of these issues give yet another opportunity for interaction between a compromised device to
  - Other apps
  - HANs and HAN connected devices
  - By proxy, internal Corporate resources
    - BYOD
    - Possible connections to OT side?

Danger Zone!



InGuardians™
Advanced Persistent Testing

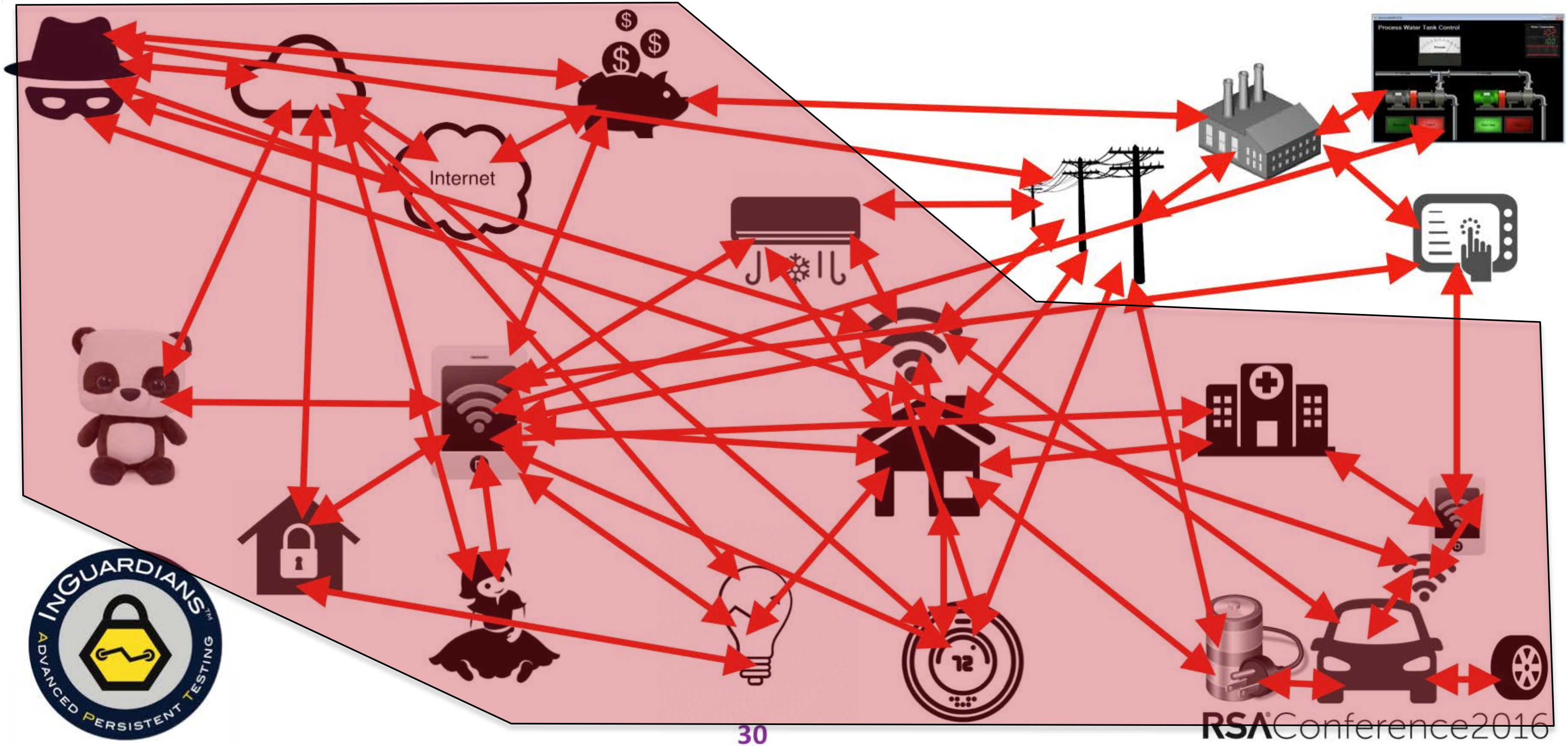
State of the Union

- Current attacks on ICS/SCADA start at the corporate side of the house
  - Phishing, Whaling
  - Office Macros, known vulnerabilities
  - 0-day requires significant resource commitment
- “Red zone” is the next opportunity!
  - So many opportunities!
  - So many MORE opportunities for 0-day with lower barrier to entry

Collision course

- Past attacks targeted the Corporate side and were stopped there
  - APT1, OpCleaver
- Others, bridged the gap
  - Havex, BlackEnergy3; “minor” intrusions and impact
  - German Iron Works, Stuxnet, Ukraine; major intrusions and impact

This will only get worse.



InGuardians™ Advanced Persistent Testing

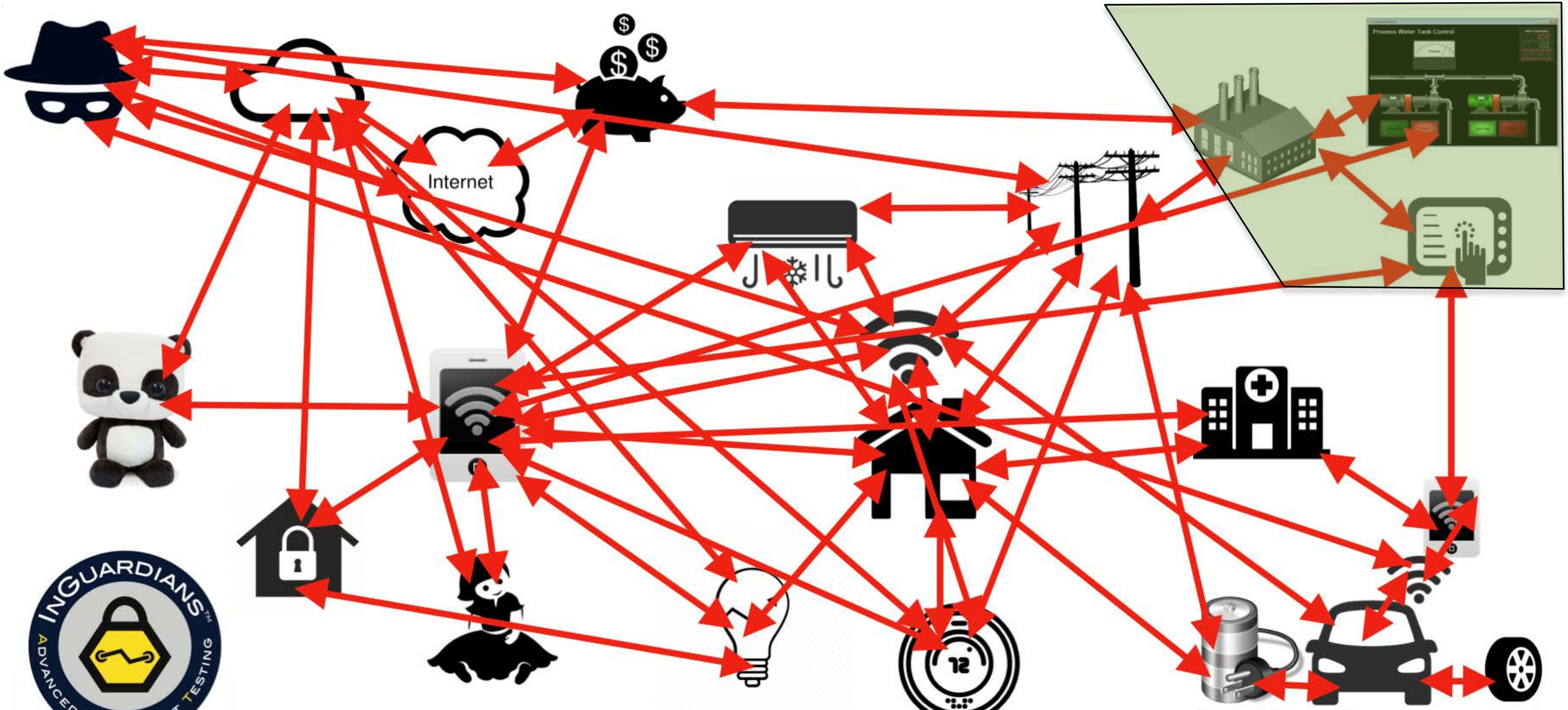
Room for Improvement

Tim Taylor says MOAR POWER!

Head for near miss?

- Instead of a collision, why not a near miss?
  - We will never be perfect, but that “near miss” might be just enough to avoid disaster
  - I use “near miss” as a metaphor, but we should do way better.
- How do we make this happen?
  - 3 approaches to 3 different problems: ICS/SCADA, HAN, IoT

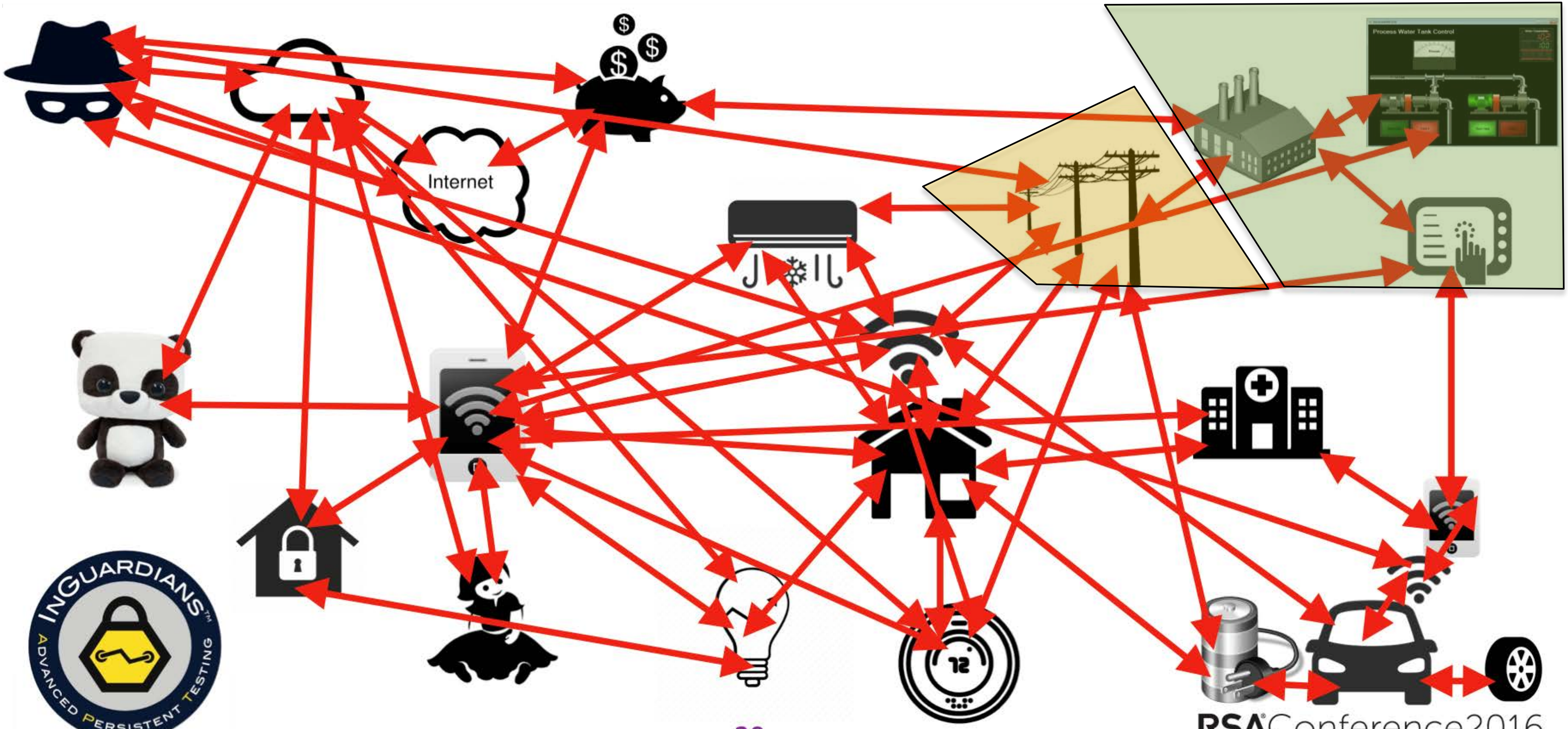
This part is hard!



A great place

- This is in many cases a great place to be
  - Air gapped networks, restricted network access, physical security
  - High level of redundancy, fail safes and manual overrides
- Significant amount of Industry regulations help.
- However traditional IT security has never been needed here before!
  - Times, they are a changing!
  - This is called “innovation”!
- Potential to add more traditional IT security for improvment
  - Detailed monitoring, inbound/outbound firewall

Let’s make this harder.



The not so Wild West (1)

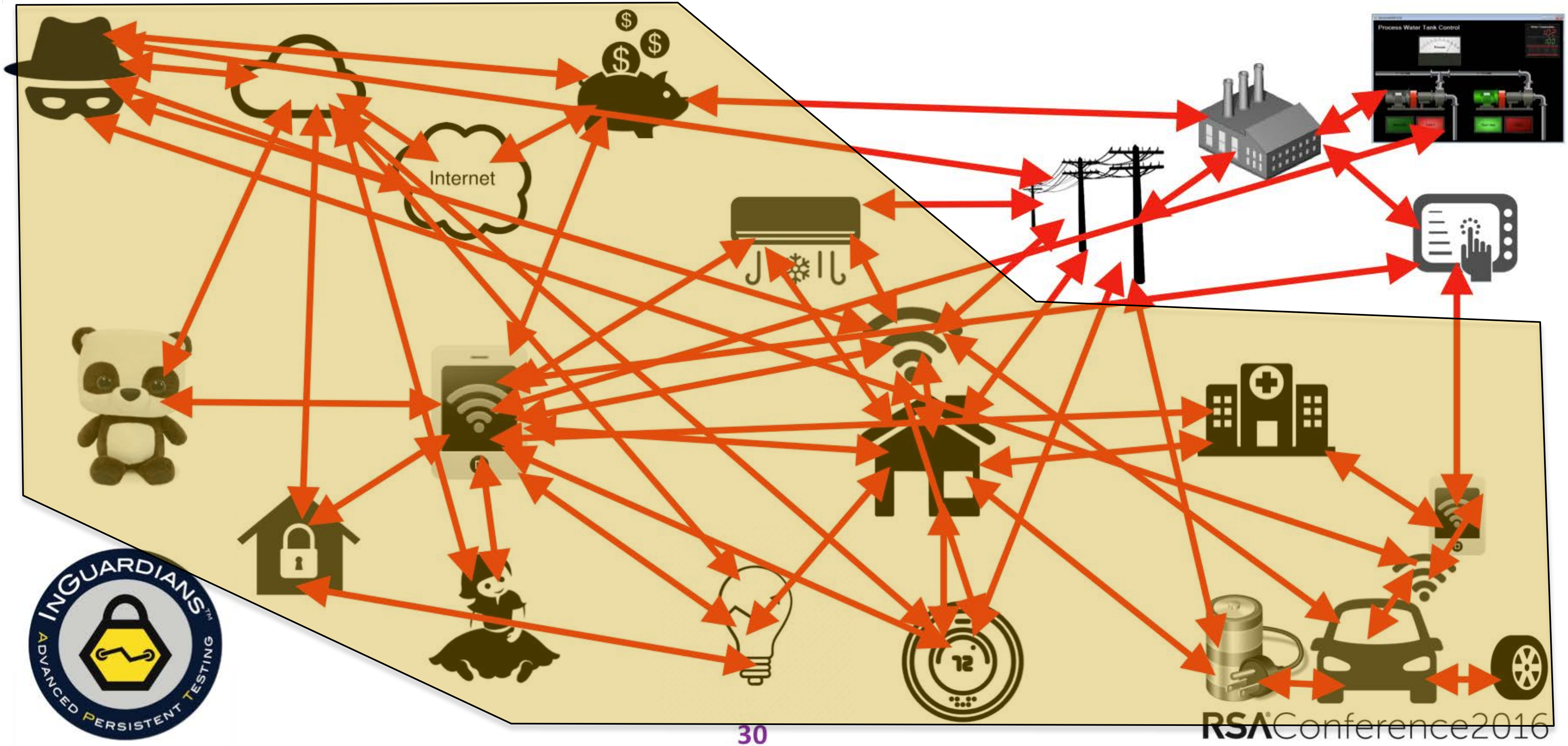
- HAN/Smart meter as an entry point to points beyond
  - So let’s lock that down and monitor the heck out of it!
- Not so fast…
  - This is where potential benefit comes to consumers and utilities so we WANT connections from customers
  - Should not be unknown devices, communication with utility to activate

The not so Wild West (2)

- I think we can improve this!
  - Protect the information used to autheinticate customers to the utility for adding home HAN devices
    - Social Engineering
    - Traditional IT/Corporate security programs.
  - HAN based firewall with device profiles with specific permitted protocols and individual commands on the gateways!
  - Read your logs and do IDS
- Yes, I’m talking Principle of Least Privilege (POLP)

InGuardians™ Advanced Persistent Testing

Beatings will continue until morale improves



Wrapping Up

Time to get the lawn mower

Disaster

- We have plenty of room for improvement here!
  - Embedded device design and security
  - Mobile App design and security
    - Good coding practices
    - Hard coded passwords
  - API access security
  - Wireless protocol implementation and selection
- These are endemic problems across multiple industries
  - Most are traditional IT problems

In Conclusion

- Rapid adoption of IoT massively increases attack surface and generates many incestuous attack paths
- All sides of the house have lots to learn from each other
- If we don’t improve we are doomed to fail, and fail hard
- We can get there!
  - Open communication
  - Education

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

Thank you!

Larry Pesce

Director of Research & Sr. Managing Security Consultant
InGuardians
@haxorthematrix

#RSAC