

17

Embedded Internet & Security Overview

18-649 Distributed Embedded Systems

Philip Koopman

Presented by Milda Zizyte

November 4, 2015

**Carnegie
Mellon**

Lame Passwords Are Everywhere!

◆ PC World 2012 Top 20 passwords

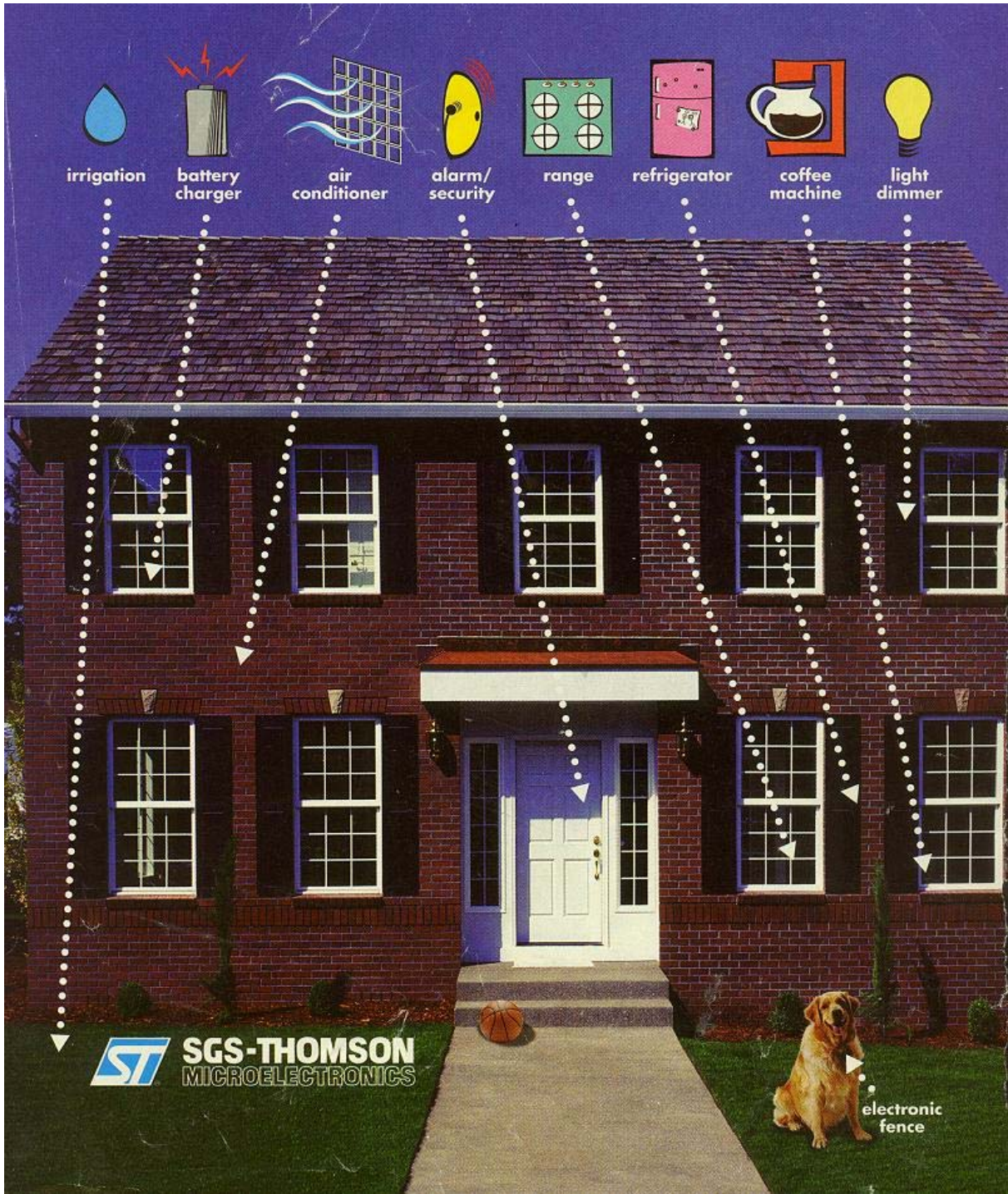
password
123456
12345678
abc123
qwerty
monkey
letmein
dragon
111111
baseball
iloveyou
trustno1
1234567
sunshine
master
123123
welcome
shadow
ashley
football

<http://www.zdnet.com/top-25-common-attackable-passwords-stop-using-ninja-and-jesus-7000006373/>

◆ Top 30 cracked LinkedIn Passwords

link
1234
work
god
job
12345
angel
the
ilove
sex
jesus
connect
fu*k
monkey
123456
master
b*tch
d*ck
michael
jordan

<http://mashable.com/2012/06/08/linkedin-stolen-passwords-list/>



irrigation

battery
charger

air
conditioner

alarm/
security

range

refrigerator

coffee
machine

light
dimmer



SGS-THOMSON
MICROELECTRONICS

electronic
fence

Other Possible Internet Home Appliances

◆ A microwave oven that knows how to cook food

- Feed UPC to oven's barcode reader and it looks up recipe

◆ An Internet washing machines

- Control & Monitor laundry from smart phone App

<http://www.samsung.com/uk/consumer/home-appliances/laundry/washing-machine/WF12F9E6P4W/EU>



◆ Internet fridge

- Contacts grocery store to re-order

◆ Internet sewing machine

- Design stitch patterns on an iPad
- Or download patterns from Web



<http://www.sewingmachines.com.au/janome-memorycraft-horizon-15000-sewing-machine.html>

Smart Homes/Offices – A good idea?

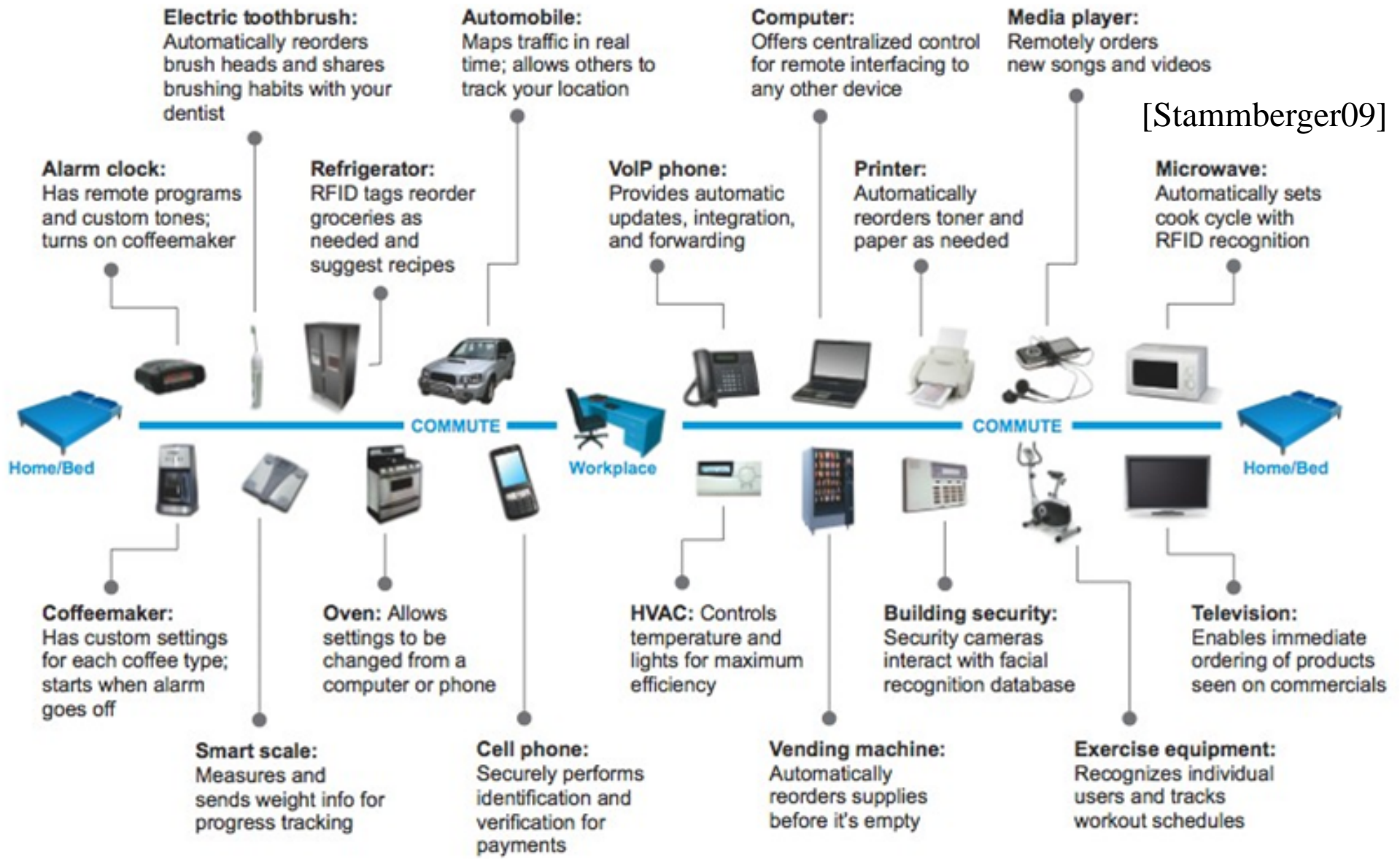


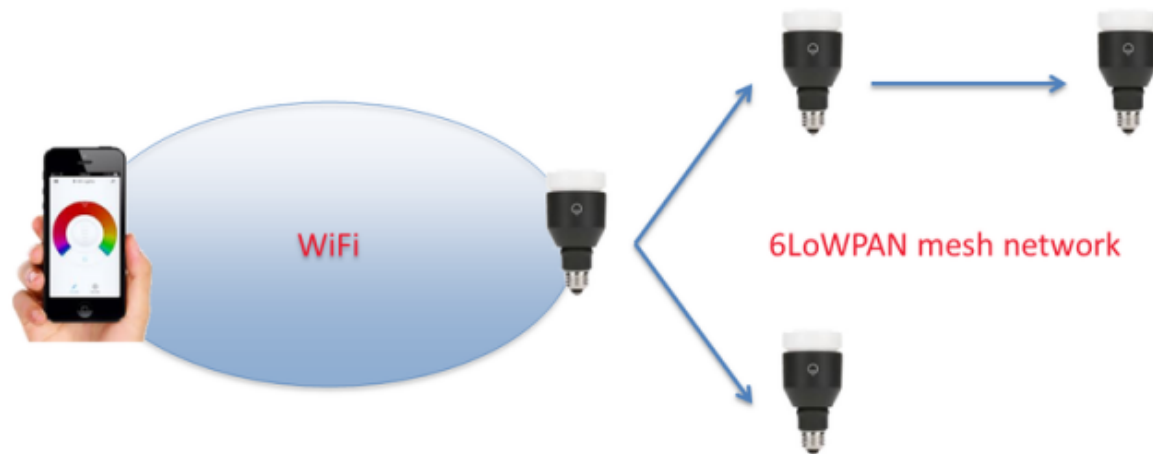
Figure 1: Connected devices already outnumber PCs by at least 5 to 1, and their numbers are growing

Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords

More evidence the Internet of things treats security as an afterthought.

by Dan Goodin - Jul 7, 2014 3:20pm EDT

[Share](#) [Tweet](#) 90



Context

In the latest cautionary tale involving the so-called Internet of things, white-hat hackers have devised an attack against network-connected lightbulbs that exposes Wi-Fi passwords to anyone in proximity to one of the LED devices.

The attack works against [LIFX smart lightbulbs](#), which can be turned on and off and adjusted using iOS- and Android-based devices. Ars Senior Reviews Editor Lee Hutchinson gave a [good overview here](#) of the Philips Hue lights, which are programmable, controllable LED-powered bulbs that compete with LIFX. The bulbs are part of a growing trend in which manufacturers add computing and networking capabilities to appliances so people can manipulate them remotely using smartphones, computers, and other network-connected devices. A [2012 Kickstarter campaign](#) raised more than \$1.3 million for LIFX, more than 13 times the original goal of \$100,000.

According to a [blog post published over the weekend](#), LIFX has updated the firmware used to control the bulbs after researchers discovered a weakness that allowed hackers within about 30 meters to obtain the passwords used to secure the connected Wi-Fi network. The credentials are passed from one networked bulb to another over a mesh network powered by [6LoWPAN](#), a wireless specification

<http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/>

DON'T BREW THAT CUPPA! Your kettle could be a SPAMBOT

Russian report says Chinese appliances hide Wifi slurping spam-spreaders

By Simon Sharwood, 29th October 2013



3,219 followers

http://www.theregister.co.uk/2013/10/29/dont_brew_that_cuppa_your_kettle_could_be_a_spam_bot/

[The Benefits and Significance of Private Platform as a Service](#)

Russian authorities have claimed that household appliances imported from China contain tiny computers that seek out open WiFi networks and then get to work sending spam and distributing malware.

St Petersburg news outlet *Rosbalt* reported last week that local authorities had examined kettles and irons and found "20 to 30 pieces of Chinese home appliance 'spy' microchips" that "sends some data to the foreign server".

Just what data is being sent and to where is not discussed, which had Vulture South thinking the report might be spurious.

A bit of digging suggests it is legitimate. One source the story mentions, Gleb Pavlov of customs broker [Panimport](#) can be found at the [link](#) we've popped in on the company's name. We've also been able to find [this link](#) to an appliances company called "Sable Ltd", the very name translation engines say is the employer of one Innokenty Fedorov whose company found the bugged appliances.



www.toprq.com/iphone
<https://www.flickr.com/photos/andybutkaj/1495901113>

Is Security An Issue For Embedded Systems?

◆ Potential problems are already there

- Modems that control embedded systems where “security” is an unlisted number
 - Example: an unprotected modem controlling a high-voltage power transmission line (Shiple & Garfinkel, 2001)
- Stories of insider attacks on critical systems
- User-modified critical systems
 - “Hot PROM” approach to modifying automotive engine controllers
- Mostly unpublicized – nobody wants to air their dirty laundry
 - Jul 2009: “Meticulously prepared” attack from N. Korea against S. Korea & US
 - Nov 2009: *60 Minutes* reports two Brazilian power outages due to attacks

◆ But, why will this be different than, say, bank security?

- Beyond them being mostly 8- & 16-bit CPUs with no OS?
- Beyond controlling safety critical systems?

[Home](#) > [Networking](#) > [Network Security](#)

News

Siemens: Stuxnet worm hit industrial systems

By Robert McMillan

September 14, 2010 01:17 PM ET

 [Comments \(4\)](#)

 [Recommended \(21\)](#)



[Share](#)

IDG News Service - A sophisticated worm designed to steal industrial secrets and disrupt operations has infected at least 14 plants, according to Siemens.

Called Stuxnet, [the worm was discovered in July](#) when researchers at VirusBlokAda found it on computers in Iran. It is one of the most sophisticated and unusual pieces of malicious software ever created -- the worm leveraged a previously unknown Windows vulnerability (now patched) that allowed it to spread from computer to computer, typically via USB sticks.

The worm, designed to attack Siemens industrial control systems, has not spread widely. However, it has affected a number of Siemens plants, according to company spokesman Simon Wieland. "We detected the [virus](#) in the SCADA [supervisory control and data acquisition] systems of 14 plants in operation but without any malfunction of process and production and without any damage," he said in an e-mail message.

Direct Attacks On Infrastructure

- ◆ **SCADA systems** – “*Supervisory Control And Data Acquisition*”
 - Embedded computers that control factories, refineries, power plants, etc.
 - Mostly they are Internet-Connected via a firewall

- 2003 – Slammer worm disables a safety monitoring system at Davis-Besse nuclear power plant in Ohio
 - Access via contractor network connection that bypassed firewall

2012 released SCADA exploit scorecard

<http://www.wired.com/2012/01/scada-exploits/>

					
Firmware					
Ladder Logic					
Backdoors					
Fuzzing					
Web			N/A	N/A	
Basic Config					
Exhaustion					
Undoc Features					

22 December 2014 Last updated at 08:01 ET

Hack attack causes 'massive damage' at steel works



The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

Details of the incident emerged in the annual report of the German Federal Office for Information Security (BSI).

It said attackers used booby-trapped emails to steal logins that gave them access to the mill's control systems.

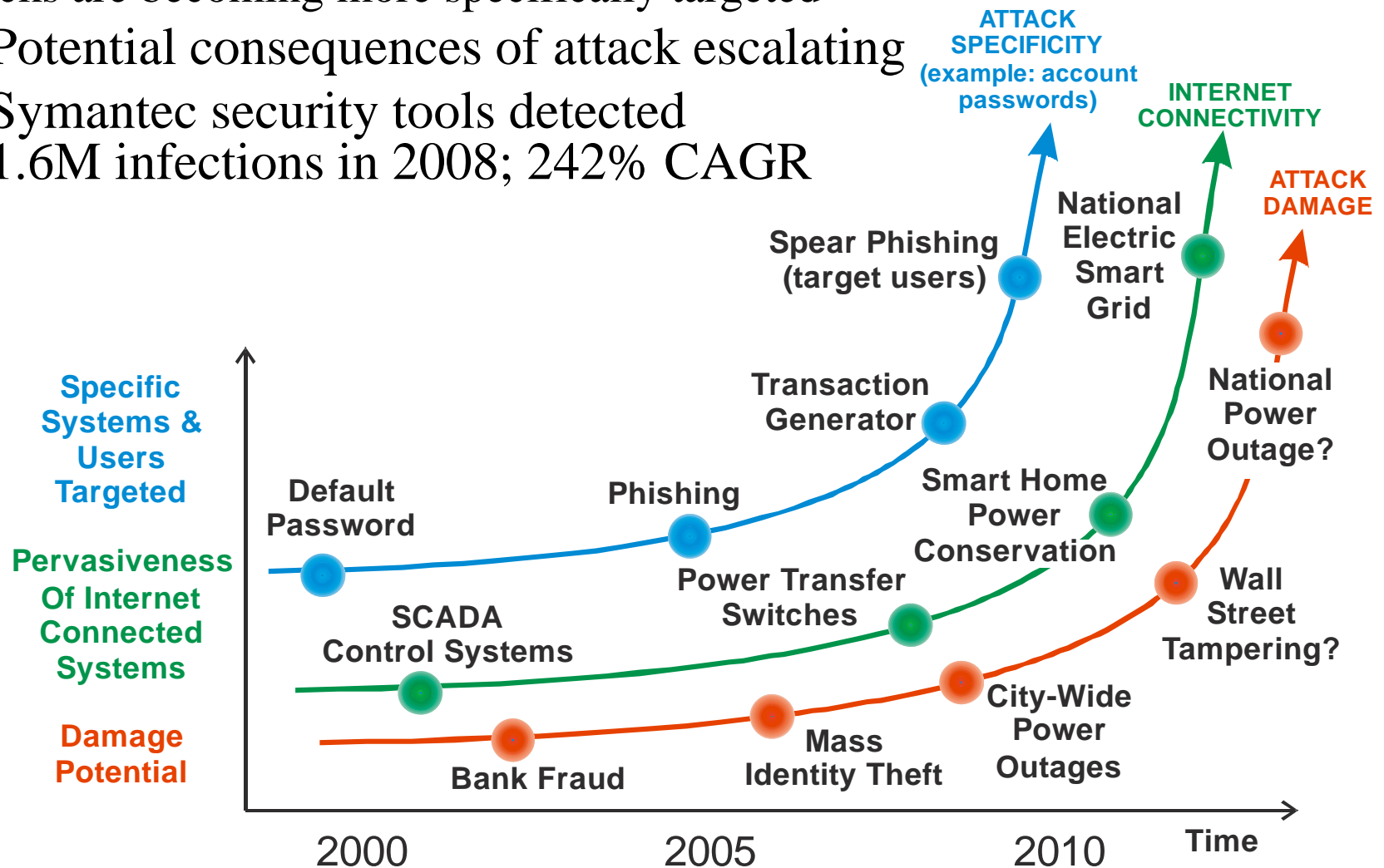
This led to parts of the plant failing and meant a blast furnace could not be shut down as normal.

The unscheduled shutdown of the furnace caused the damage, said the report.

<http://www.bbc.com/news/technology-30575104>

Risk Due To Attacks Is Increasing Over Time

- ◆ More systems are connected and possibly vulnerable [Emerson Electric, 2008]
- ◆ Attacks are becoming more specifically targeted
 - Potential consequences of attack escalating
 - Symantec security tools detected 1.6M infections in 2008; 242% CAGR



ATTACK SPECIFICITY AND DAMAGE INCREASING AS CONNECTIVITY RISES

◆ (2012 info)

US-CERT Security News

Source: United States Computer Emergency Readiness Team, <http://www.us-cert.gov/>



Energy

Flame Malware and SCADA Security: What are the impacts?
- May 29

"Over the weekend, a new super worm exploded onto the cyber security landscape. Known as Flame or skYlper, it appears to be targeting sites in the Middle East, just like the Stuxnet and Duqu worms did."



Factory

Emerson DeltaV multiple vulnerabilities
- May 30

"This Advisory identifies multiple vulnerabilities in the Emerson DeltaV application. This web release follows the earlier secure portal release."



Transport

North Korea implicated in malware attacks on airport
- June 5

"Agents from North Korea and a man from South Korea have been accused of using malware-laced games to conduct attacks on a South Korean airport."



Buildings

RuggedCom weak cryptography for password vulnerability
- May 25

"This Advisory details a default backdoor user account with a weak password encryption. This web release follows the earlier secure portal release."

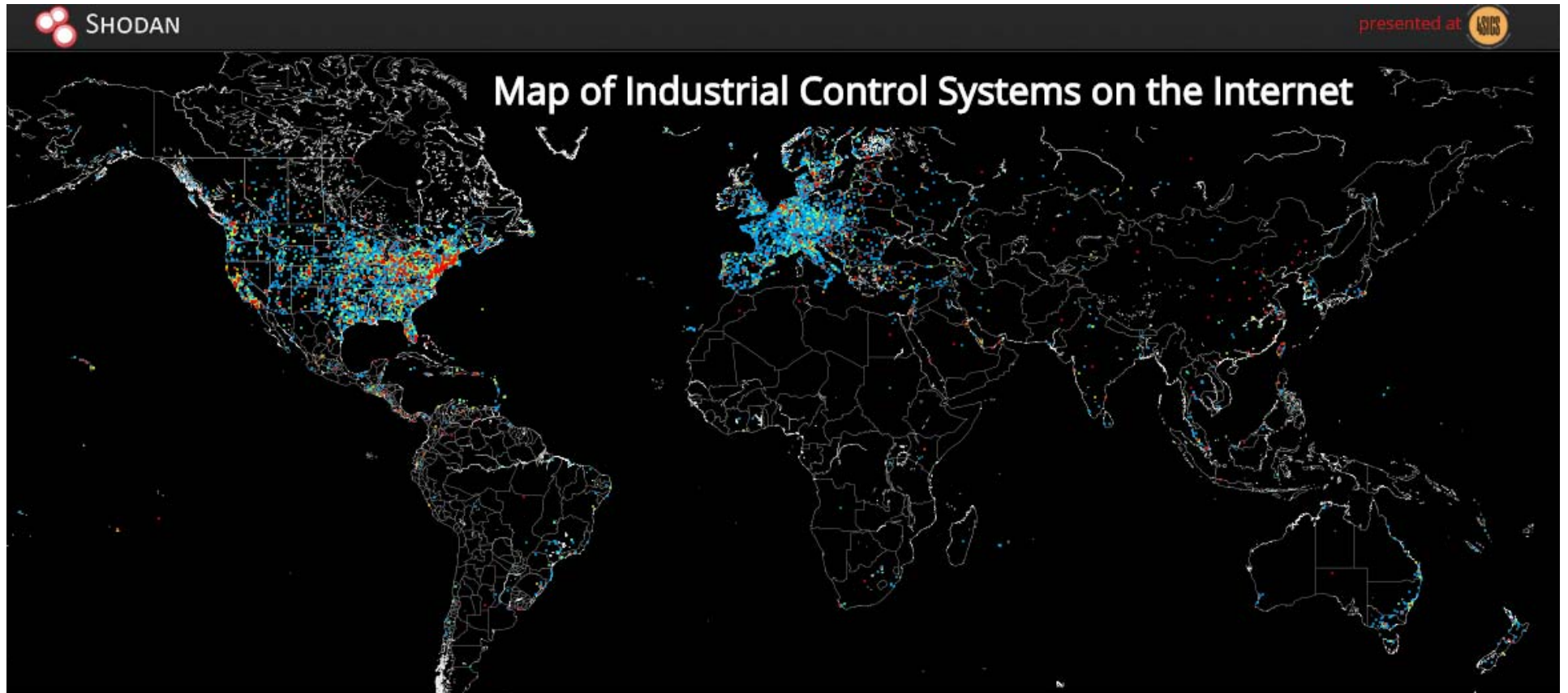


Infrastructure

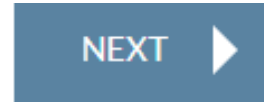
Cyber search engine Shodan exposes industrial control systems to new risks
- June 3

"Industrial control computers, the systems that automate such things as water plants and power grids, were found to be linked in to the Shodan search."

<https://icsmap.shodan.io/>



Traffic light controls



When something that literally anyone in the world can access says "DEATH MAY OCCUR !!!" it's generally a good idea to build some kind of security around it.

Oops - no. For some reason, someone thought it would be a good idea to put traffic light controls on the Internet. Making matters way, way worse is that these controls require no login credentials whatsoever. Just type in the address, and you've got access.

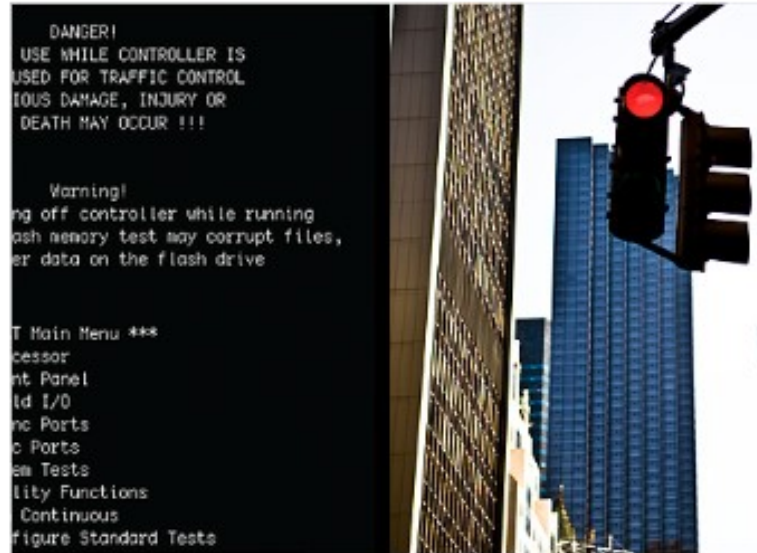


PHOTO: DAN TENTLER; THINKSTOCK

This is why Caps Lock was invented.

You'd have to know where to go looking, but it's not rocket science. Security penetration tester Dan Tentler found the traffic light controls using **Shodan**, a search engine that navigates the Internet's back channels looking for the servers, webcams, printers, routers and all the other stuff that is connected to the Internet.

Once the controls were brought up on a Web browser, anyone could put lights into "test"

<http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html>

A hydroelectric plant



French electric companies apparently like to put their hydroelectric plants online. Tentler found three of them using Shodan.

This one has a big fat button that lets you shut off a turbine. But what's 58,700 Watts between friends, right?

It's not just France that has a problem. The U.S. Department of Homeland Security commissioned researchers last year to see if they could find **industrial control systems for nuclear power plants** using Shodan. They found several.

Tentler told DHS about all the power plants he found -- actually, DHS called him after he accessed one of their control systems.

The screenshot shows a control interface for a turbine. At the top, it says "TURBINE DE BRUAUX" and "27/03/2013 03:58:12". Below this, there are two columns of data: "Puis totale" with values "58,7 kW" and "58,7 kW", and "Niveau amont" with a value of "260,3 mm". A vertical scale on the left ranges from 0 to 1000. The main control area contains several buttons: a large orange "T1MARCHÉ" button, a "MARCHÉ ARRÊT T1" button, a "MARCHÉ ARRÊT" button, a green "OUVERTURE" button, a red "FERMETURE" button, a yellow "CHOIX IMAGES" button, and a yellow "IMAGE PRECEDENTE" button. To the right of the interface is a photograph of the turbine's interior, showing yellow metal railings and machinery. At the bottom of the screenshot, there is a photo credit: "PHOTO: DAN TENTLER; THOMAS BREGARDIS/AFP/GETTY". Below the screenshot, a text box contains the question: "Wait, does that say kilowatts?"

<http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html>

A gondola ride

A gondola ride over a ski resort is a fun way to enjoy the mountain view. But not if you stop in the middle of the ride and the doors open.

Anyone could do that with a click of a button, even if they were sitting thousands of miles away. That's because this French ski resort put the control systems for the gondola ride on the Internet.

Attempts to contact the company were unsuccessful.



AIL SEMER

05 135
OS DE LA MADRAGUE

0,75 m/s CONSIGNE +/- VITE : 0,75 m/s

NTENANCE: CONDUITE DEPUIS PUPITRE MOTRICE

ARRET EXPLOITATION
PORTES FERMEES

ARRET EXPLOITATION
PORTES OUVERTES

Garmisch-Classic

PHOTO: DAN TENTLER; FABRICE COFFRINI/AFP/GETTY

Hey, why are the doors opening?

<http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html>

Basic Security Concepts

◆ Confidentiality

- Information is kept secret from those who aren't supposed to know it
- Privacy is a little different – it is more about association of information with an individual

◆ Integrity

- Unauthorized data alteration is detected (or prevented)
- Includes notion of authentication – making sure a node has proper permissions

◆ Availability

- Services are available when requested

◆ Embedded emphasis:

- Confidentiality often matters less for control systems
- Integrity matters a lot for safety critical systems
- Reliability might be more important than availability, but both matter
- (Every system is different; depends on user & context)

Embedded-Specific Security Issues

◆ General Internet concerns apply

- But, there are some special embedded concerns too
- And, of course, embedded systems are much more cost sensitive!

◆ Real time sensitivity

- Even a transient denial of service attack can disrupt real-time operations
- Intrusion detection and reaction might be too slow

◆ Control vs. transactions

- Much of Internet security is based on transactions (e.g., web purchases)
- Many embedded systems emphasize real time continuous process control

◆ Physical security

- Generally, the person owning the hardware is the good guy for Internet security
- Often, embedded systems are exposed to physical attack directly (e.g., smart card)

Maintenance Issues

◆ Interfacing to Internet may force need for embedded software update

- Security fixes
- Compatibility with evolving middleware & network standards
- Alternately, enterprise systems may have to drag 5 to 50 years of legacy interfaces around with them(!)



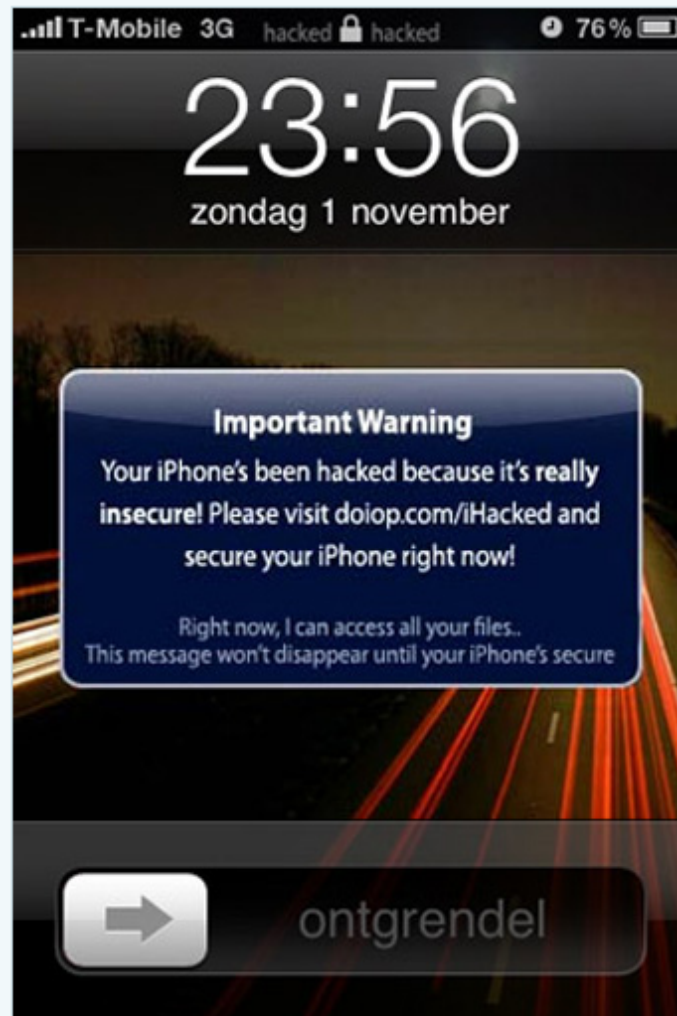
◆ Who's the sysadmin for your house? For your car?

- Classical embedded systems were shipped with immutable software
- Need to perform configuration management requires sophisticated maintainers
 - Can we trust automatic configuration management?
 - Do you want vendors able to arbitrarily change software in “your” belongings?
- What happens when there is a software incompatibility?
 - If the system stops working, whose responsibility is it to make it work?

Myth: Techies Are Perfect Sysadmins

◆ Nov 2, 2009

Dutch Hacker Holds Jailbroken iPhones Hostage For €5 Ransom While Exposing Security Vulnerability



Many of us have jailbroken our iPhones, but did everyone remember to change the default root password? Those guilty of that oversight are vulnerable to the simple intrusion method this guy used to hold iPhones hostage in the Netherlands. **Updated.**

Apparently all that it took to terrify many Dutch iPhone users was a "trivial" port scanning technique and "a modicum of networking know-how." After the hacker gained access to the jailbroken phones with unchanged root passwords and SSH enabled, he sent the pictured message which led to a demand for a €5 PayPal payment and

words of caution:

<http://gizmodo.com/5395645/dutch-hacker-holds-jailbroken-iphones-hostage-for-5-ransom-while-exposing-security-vulnerability>

Hackers Crack Into Texas Road Sign, Warn of Zombies Ahead

Thursday, January 29, 2009

FOX NEWS

By Joshua Rhett Miller

[E-Mail](#) | [Print](#) | [Share](#)



i-hacked.com

Texas Dept. of Transportation officials confirm a portable traffic sign at Lamar Boulevard and West 15th Street in Austin was hacked into last week.

Transportation officials in Texas are scrambling to prevent hackers from changing messages on digital road signs after one sign in Austin was altered to read, "Zombies Ahead."

Chris Lippincott, director of media relations for the Texas Department of Transportation, confirmed that a portable traffic sign at Lamar Boulevard and West 15th Street, near the [University](#) of Texas at Austin, was hacked into during the early hours of Jan. 19.

"It was clever, kind of cute, but not what it was intended for," said Lippincott, who saw the sign during his morning commute. "Those signs are deployed for a reason — to improve traffic conditions, let folks

know there's a road closure."

"It's sort of amusing, but not at all helpful," he told FOXNews.com.

Zombie Copy-Cats

- ◆ Don't try this yourself... it is old and stale by now



Safety Criticality => Potential Release Of Energy

Polish Teen Hacks His City's Trams, Chaos Ensues

By Chuck Squatriglia  January 11, 2008 | 4:29:44 PM Categories: [Public Transit](#)

A teenager in Lodz, Poland hacked the city's tram system with a homemade transmitter that tripped rail switches and redirected trains, a prank that derailed four trams and injured a dozen people.

According to reports in the Register and the [Telegraph](#), the 14-year-old boy - described by his teachers as an electronics genius (Gee- you think?) - spent months studying the city's rail lines to determine the best places to redirect trains and cause the most havoc, then converted an old TV remote into an infrared transmitter capable for tripping the switches.

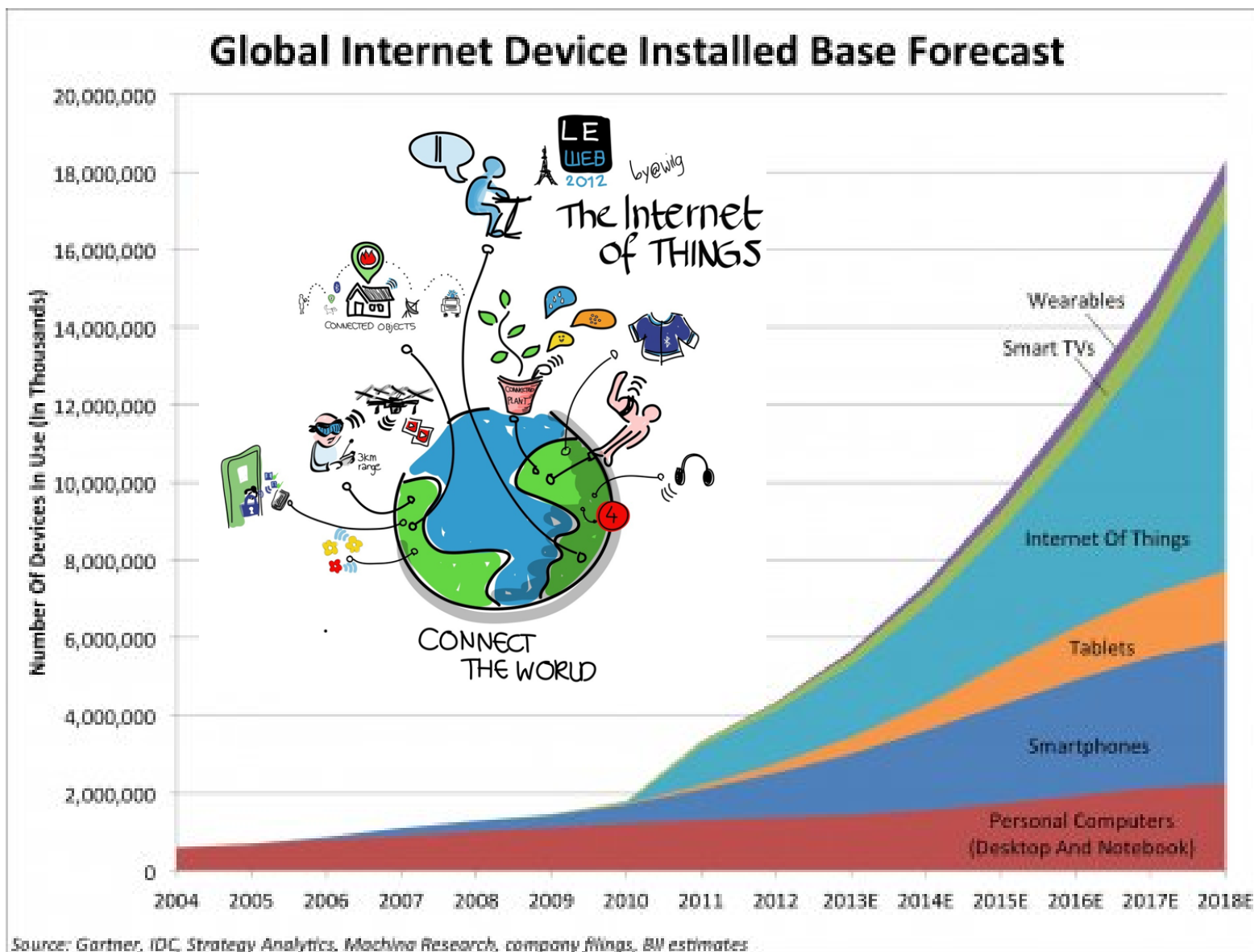


"He treated it like any other schoolboy might a giant train set, but it was lucky nobody was killed," Mirosław Micor, a spokesman for Lodz police, told the Telegraph. "Four trams were derailed, and others had to make emergency stops that left passengers hurt. He clearly did not think about the consequences of his actions."

[Wired Blog Jan 11, 2008]

Photo courtesy Telegraph.

Security: Embedded Products “Want” an Internet Connection



<http://static2.businessinsider.com/image/5266dc686bb3f78839059251-480/deviceforecast.jpg>

<http://metiscomm.com/the-internet-of-things-security-swiss-cheese/>

Just How Bad Could It Be?

◆ Consider the lowly thermostat

- Koopman, P., "Embedded System Security," *IEEE Computer*, July 2004.

◆ Trends:

- Internet-enabled
- Connection to utility companies for grid load management

◆ Proliphix makes an Internet Thermostat

- But it we're not saying that system has these vulnerabilities!

...

however, we're pretty sure *some* existing systems would be vulnerable to these types of problems.



Waste Energy Attack

◆ “I’m coming home” function

- Ability to tell thermostat to warm up/cool down house if you come home early from work, or return from a trip
- Save energy when you’re gone; have a comfy house when you return
- Implement via web interface or SMS gateway

◆ **Attack: send a false “coming home” message**

- Causes increase in utility bill for house owner
- If a widespread attack, causes increased US energy usage/cause grid failure
- Easily countered(?) – if designers think to do it!
 - Note that playback attack is possible – more than just encryption of an unchanging message is required!

Discomfort Attack

◆ Remotely activated energy saver function

- Remotely activated energy reduction to avoid grid overload
- Tell house “I’ll be home late”
- Saves energy / prevents grid overload when house empty

◆ Attack: send a false “energy saver” command

- Will designers think of this one?
- Some utilities broadcast energy saver commands via radio
 - In some cases, air conditioning is completely disabled
 - Is it secure??
- Consequences higher for individual than for waste energy attack
 - Possibly broken pipes from freezing in winter
 - Possibly injured/dead pets from overheating in summer

Energy Auction Scenario

◆ What if power company optimizes energy use?

- Slightly adjust duty cycles to smooth load (pre-cool/pre-heat in anticipation of hottest/coldest daily temperatures)
- Offer everyone the chance to save money if they volunteer for slight cutbacks during peak times of day
- Avoid brownouts by implementing heat/cool duty cycle limits for everyone

◆ You could even do real time energy auctions

- Set thermostat by “dollars per day” instead of by temperature
 - More dollars gives more comfort
- Power company adjusts energy cost continuously throughout day
- Thermostats manage house as a thermal reservoir

Energy Auction Attacks

◆ What if someone broke into all the thermostats?

- Set dollar per day value to maximum, ignoring user settings
 - Surprise! Next utility bill will be unpleasant
- Turn on all thermostats to maximum
 - Could overload power grid
- Pulse all thermostats in a synchronized way
 - Could synchronized transients destabilize the power grid?

◆ What if someone just broke into the auction server?

- If you set energy cost to nearly-free, everyone turns on at once to grab the cheap power
- Guess what – enterprise computer could have indirect control of thousands of embedded systems!
- Someday soon, almost “everything” will be “embedded,” at least indirectly
- Look at it as classical industrial safety – ask:
How can software directly or indirectly control the release of energy?

Example IoT Security Needs [IoT-A]

◆ Authentication

- Is this user OK? Is that device I'm talking to OK?

◆ Authorization

- Which user can perform which functions on a device?

◆ Identity Management

- Which user is which? Which device is which?

◆ Key Management

- Exchange of cryptographic keys; certificate management

◆ Trust & Reputation

- In a peer-to-peer system, trust based on past behavior
(might not be viable for Emerson systems)

In general this list is incomplete – as are many IoT Security lists!

Possible IoT-Specific Threats [Garcia 2013]

- ◆ **Cloning of things / substitution after commissioning**
 - Unauthorized copy of a device (black market; gray market)
 - Inferior or subverted copy can lead to reputation loss
 - What if you let it connect to your cloud service?
- ◆ **Eavesdropping**
 - Especially during commissioning (e.g., sending keys in the clear)
- ◆ **Man in the middle**
 - Especially during commissioning to act as a malicious relay
- ◆ **Firmware replacement**
 - Malicious content in an automatically pushed firmware update
 - Malicious content in update installed by user (intentional or not)
- ◆ **Privacy threat**
 - Can your competitor tell your factory production by counting number of encrypted messages sent from an area of your plant?
- ◆ **Denial of service**
 - Battery drain; network overload

Example IoT Challenges



<http://arc0f72.com/protecting-our-privacy/>

◆ Commissioning

- Already difficult – how do you know which node is which?
- Need to distribute cryptographic key information
- Need to manufacture and manage secret key information

◆ Establishing trust

- Two devices meet for the first time – how can they trust each other?
- A device meets a router for the first time – how can it trust the router if the device doesn't have its own internet connection?
- Can you trust third parties with your key material?

◆ Revoking trust

- How do you revoke key material if there has been a compromise?
- How do you exclude a retired device to avoid key scavenging?

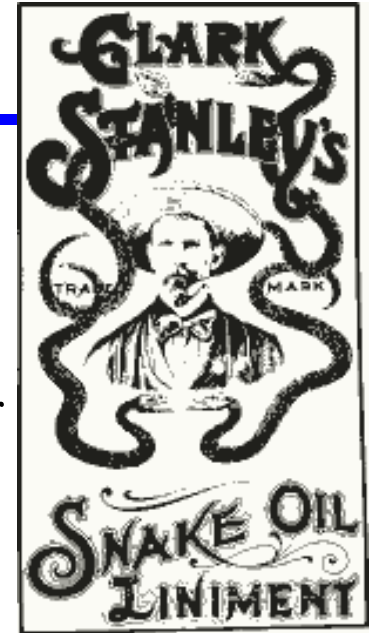
◆ Security updates

- How do you know that new patch/key update is authentic?

◆ Per-device feature activation

- Preventing privilege cloning

Security Snake Oil (avoid these!)



◆ Secret system

- Security claims rest even in part on “we won’t tell you how we do it” or “we have a proprietary algorithm”
- Good systems are secure even against the actual system designer
- Security should be based on the secret key (which means the actual system designer can’t know the secret key in all devices)

◆ Technobabble

- Buzzwords don’t make you secure

◆ We’re “unbreakable”

- No, they’re not. Best you can do is a sufficiently high cost to break

◆ Strong claims about weak systems

- What does the cryptography actually protect?
 - 2008 hard drive used AES for encrypting the key – but only XOR data
- Are big keys sent in the clear?
- Does the manufacturer have a back door device key?

<http://www.h-online.com/security/features/Enclosed-but-not-encrypted-746199.html>

[http://en.wikipedia.org/wiki/Snake_oil_\(cryptography\)](http://en.wikipedia.org/wiki/Snake_oil_(cryptography))

Myth: Discipline Will Solve Security Worries

- ◆ **Hacker's can't hurt your flight controls if the passenger laptops don't "talk" to the flight controls**
 - Solution: don't put a connection passengers and flight controls
 - Do seat-back displays "talk" to flight controls?



Delta B757
(Airbus is
similar)

Malware implicated in fatal Spanair plane crash

Computer monitoring system was infected with Trojan horse, authorities say

By Leslie Meredith



updated 8/20/2010 4:48:01 PM ET

Share | Print | Font: + -

Authorities investigating the 2008 crash of Spanair flight 5022 have discovered a central [computer](#) system used to monitor technical problems in the aircraft was infected with malware.

An internal report issued by the airline revealed the infected computer failed to detect three technical problems with the aircraft, which if detected, may have prevented the plane from taking off, according to reports in the Spanish newspaper, El Pais.

Flight 5022 crashed just after takeoff from Madrid-Barajas International Airport two years ago today, killing 154 and leaving only 18 survivors.

The U.S. National Transportation Safety Board reported in a preliminary investigation that the plane had taken off with its flaps and slats retracted — and that no audible alarm had been heard to warn of this because the systems delivering power to the take-off warning system failed. Two earlier events had not been reported by the automated system.

The [malware](#) on the Spanair computer has been identified as a type of Trojan horse. It could have entered the airline's system in a number of ways, according to Jamz Yaneeza, head threat researcher at Trend Micro.

Some of the most likely ways are through third party devices such as USB sticks, Yaneeza said, which were responsible for the [International Space Station virus infection](#) in 2008, or through a remote VPN connection that may not have the same protection as a computer within the enterprise network. Opening just one malicious file on a single computer is all it takes to [infect an entire system](#).

http://www.msnbc.msn.com/id/38790670/ns/technology_and_science-security/

Would You Run Windows As In-Flight Software?

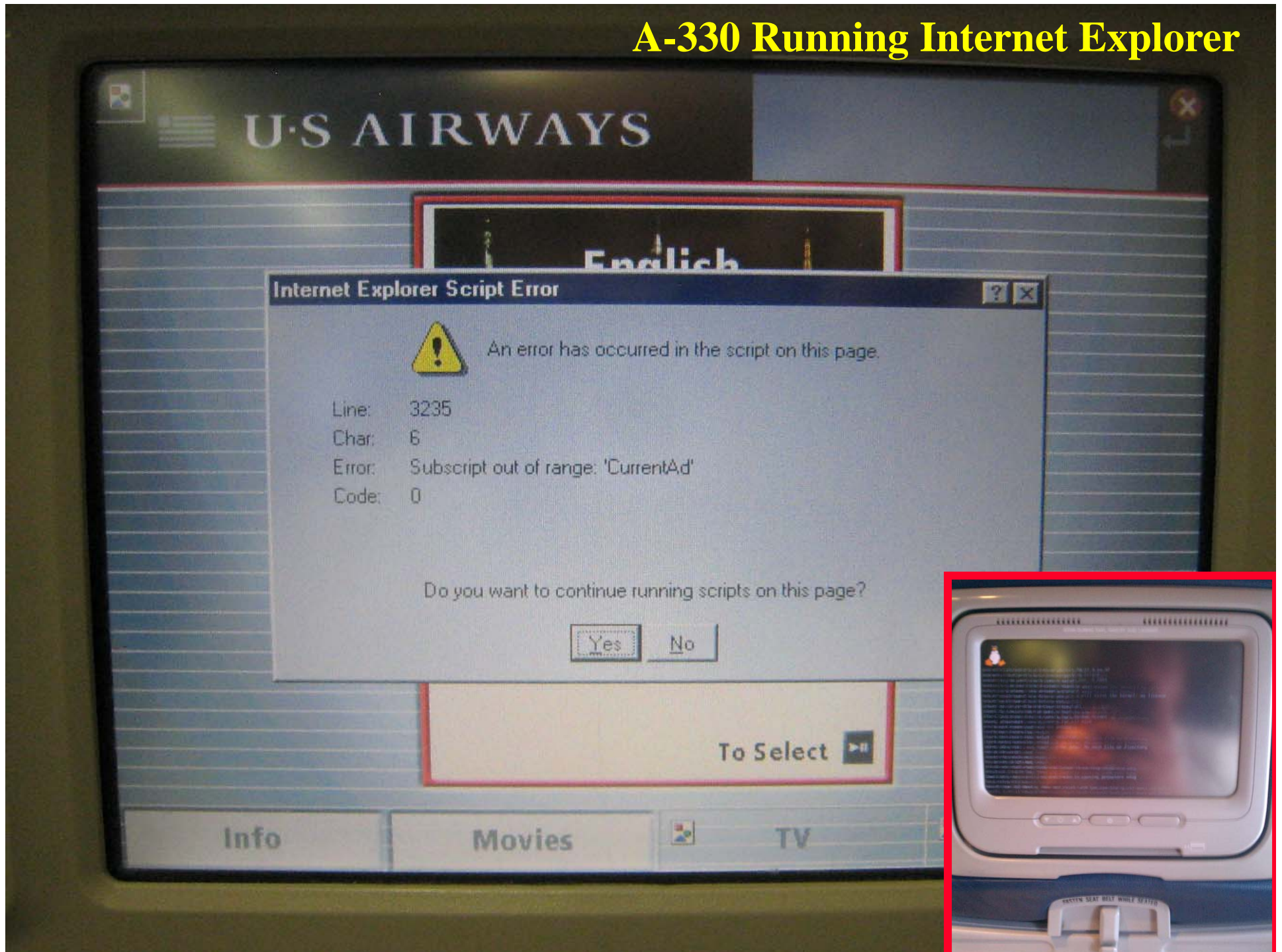
- ◆ **Safety critical subsystems will be connected to external networks (directly or indirectly)**
 - (Do airplanes run Windows? Or Linux?)

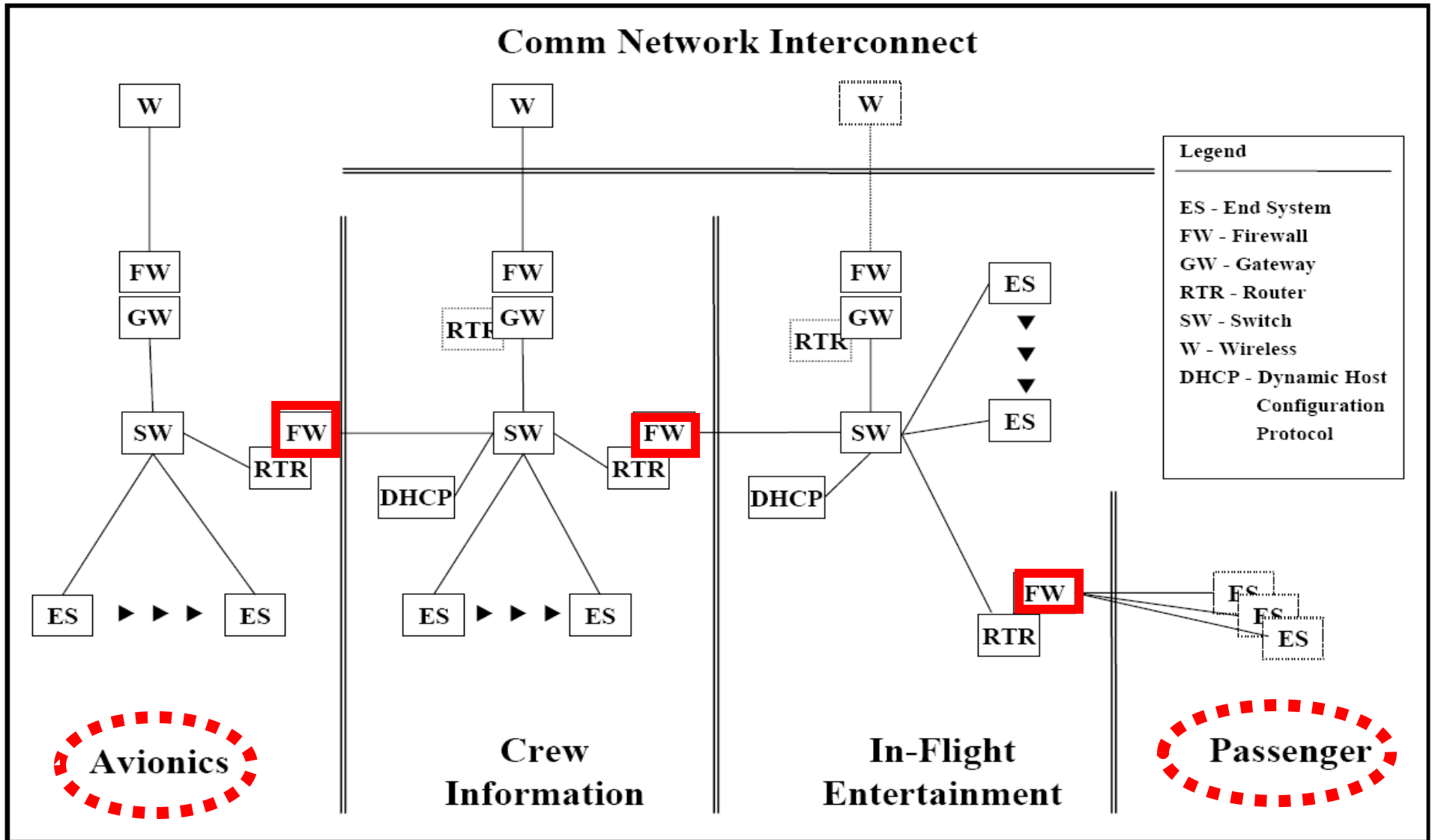


Computer graphics by IBM

[Airbus 2004] Airbus 380 uses IP-based flight controls

A-330 Running Internet Explorer





Wargo & Chas, 2003, proposed Airbus A-380 architecture

Passenger laptops are 3 Firewalls away from flight controls!

Internet connects somewhere as well

Automotive Network Attacks

◆ CAN has no authentication

- You can cause problems by spoofing CAN messages



Figure 6. Displaying an arbitrary message and a false speedometer reading on the Driver Information Center. Note that the car is in Park.

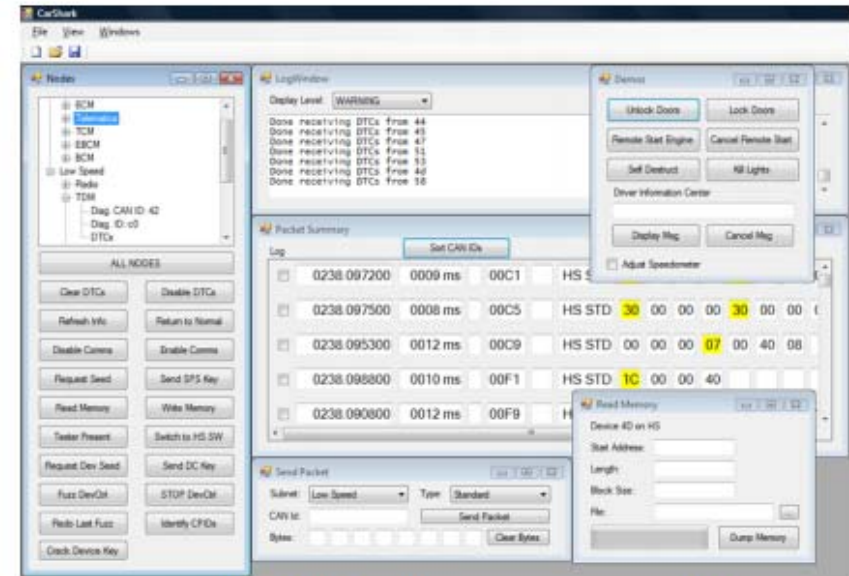


Figure 4. Screenshot of the CARSHARK interface. CARSHARK is being used to sniff the CAN bus. Values that have been recently updated are in yellow. The left panel lists all recognized nodes on high and low speed subnets of the CAN bus and has some action buttons. The demo panel on the right provides some proof-of-concept demos.

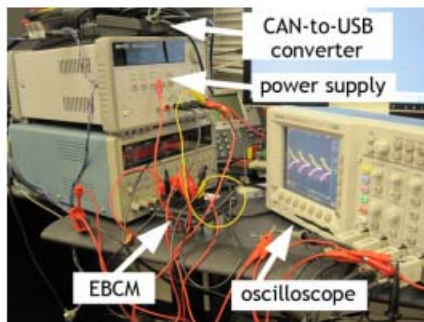


Figure 1. Example bench setup within our lab. The Electronic Brake Control Module (EBCM) is hooked up to a power supply, a CAN-to-USB converter, and an oscilloscope.

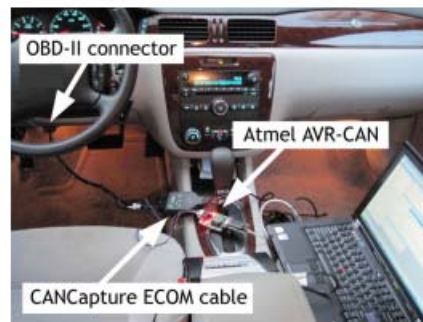


Figure 2. Example experimental setup. The laptop is running our custom CARSHARK CAN network analyzer and attack tool. The laptop is connected to the car's OBD-II port.



Figure 3. To test ECU behavior in a controlled environment, we immobilized the car on jack stands while mounting attacks.

[Koscher 2000]

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

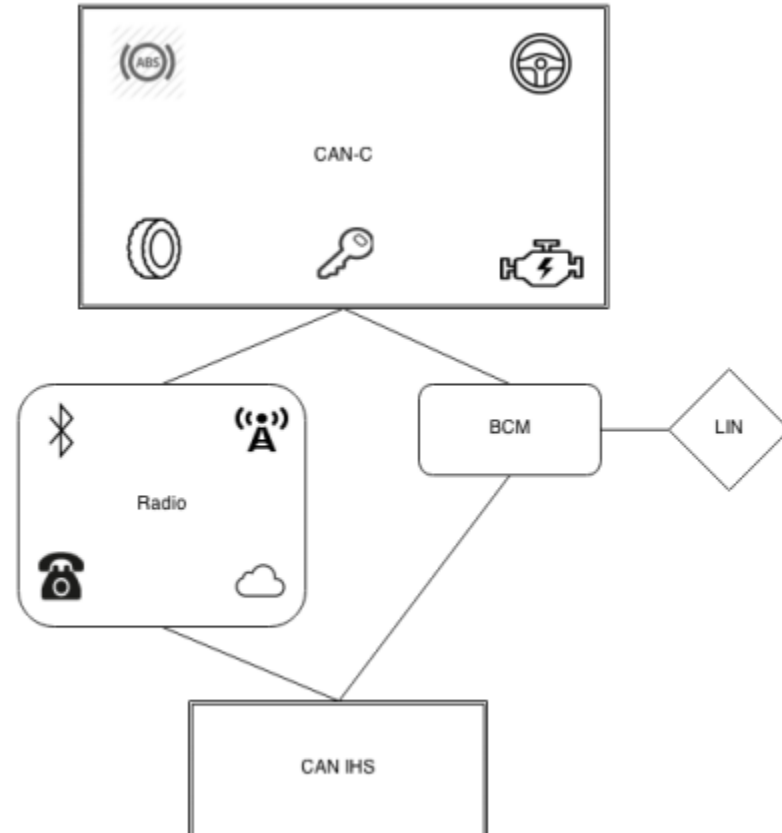
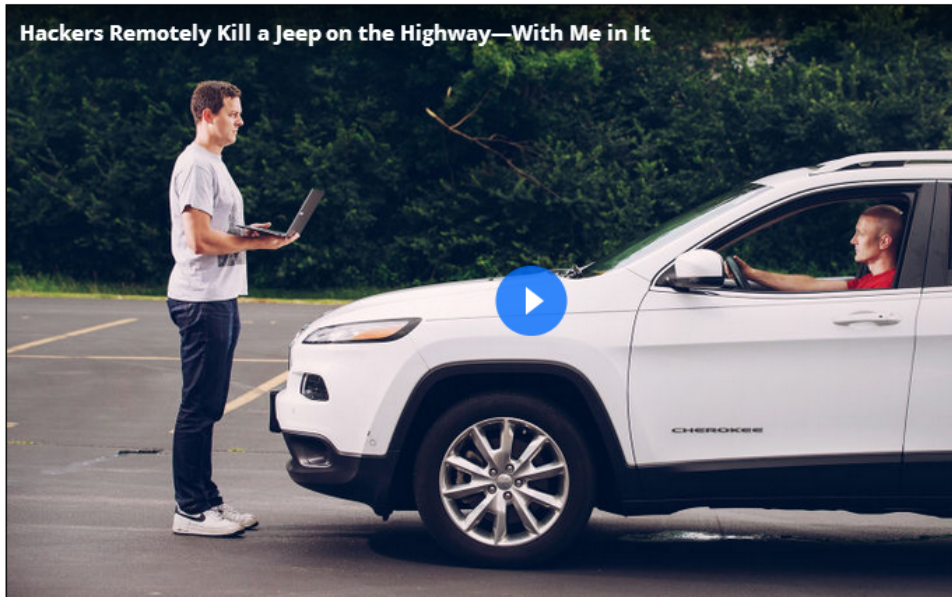


Figure: 2014 Jeep Cherokee architecture diagram

SHARE

- SHARE 202560
- TWEET 23228
- FIN 186
- COMMENT 717
- EMAIL

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.

As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car's digital display: Charlie Miller and Chris Valasek, wearing their trademark track suits. A nice touch, I thought.

LATEST NEWS

- OBSESSIONS**
 Wickedly Cool Space Book Comes Personalized to Your...
 48 MINS
- ANIMAL SCIENCE**
 Absurd Creatures: Bats Are Totally Legit. Trust Me, I'm a Vampire
 2 HOURS
- BRANDED CONTENT**
 How the Adventure Capitalist Gets More Out of Every Trip
 THE MARRIOTT REWARDS® PREMIER CREDIT CARD

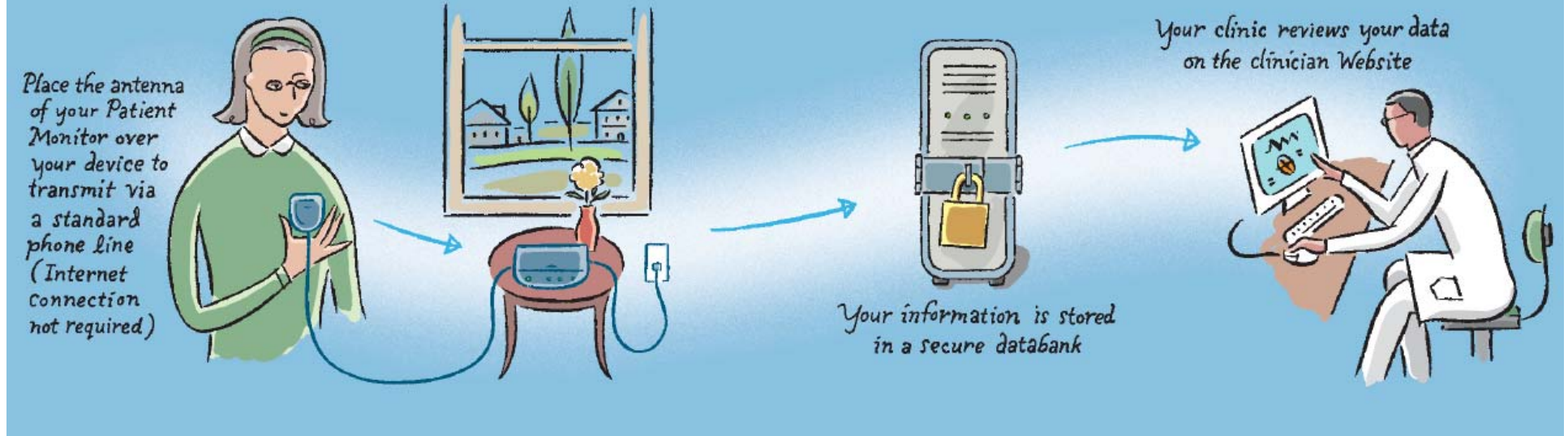
<http://illmatics.com/Remote%20Car%20Hacking.pdf>



<http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

Internet Pacemaker Anyone?


Medtronic CareLink Service



<http://www.medtronic.com/carelink/patient/downloads/patient-brochure2712aEN3.pdf>

HACKER CAN SEND FATAL DOSE TO HOSPITAL DRUG PUMPS



Hospira's drug infusion pumps include a serial cable (the wide grayish-white cable with the single red stripe on one edge) that connects the communications module to the main pump board.  BILLY RIDS

<http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/>

LG Smart TV Privacy Issue, Nov 2013

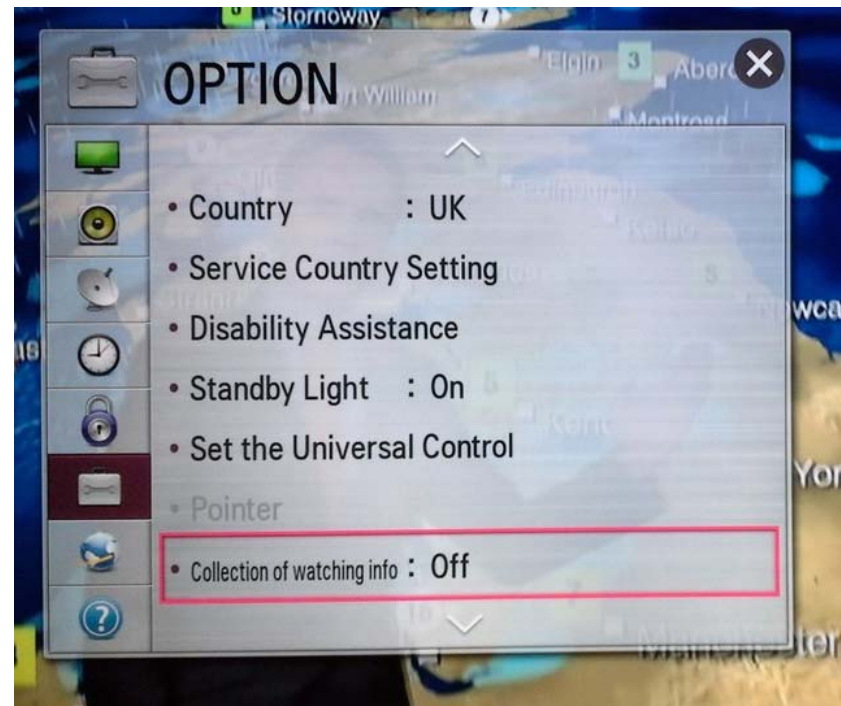
◆ Summary:

- LG TVs support “Smart Ads” by monitoring your viewing habits
- Turned off viewing data collection (on by default)
- But, TV still sent viewing information back to LG servers anyway
- AND, snooped file names on a USB flash drive and sent them in too

◆ LG Initial Response: “... as you accepted the Terms and Conditions on your TV, your concerns would be best directed to the retailer.”

◆ Further question: do you think Netflix Streaming monitors your viewing habits?

- They do!
- What happens with that info?



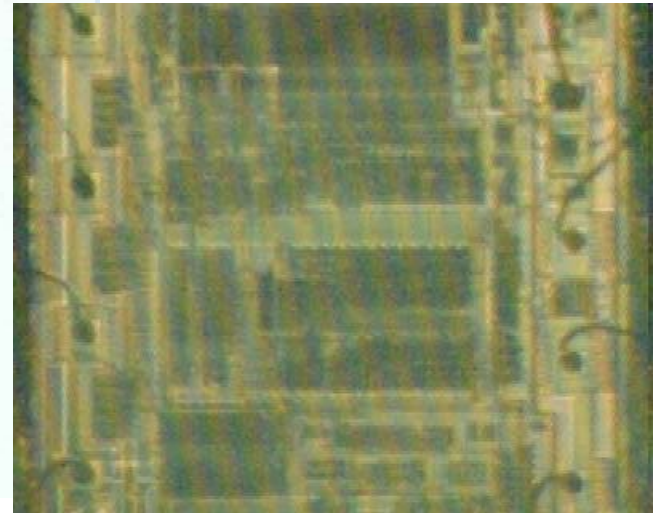
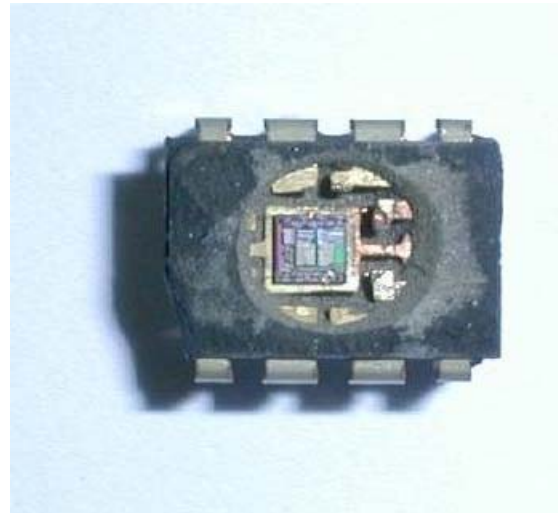
Intellectual Property Protection

◆ How easy is it for someone to steal your design?

- Hardware design
- Software design

◆ Chip peels are no big deal

- Can recover hardware schematics from silicon
- Can recover software from memory
- “Tamper resistant” slows down attacks; doesn’t really stop them



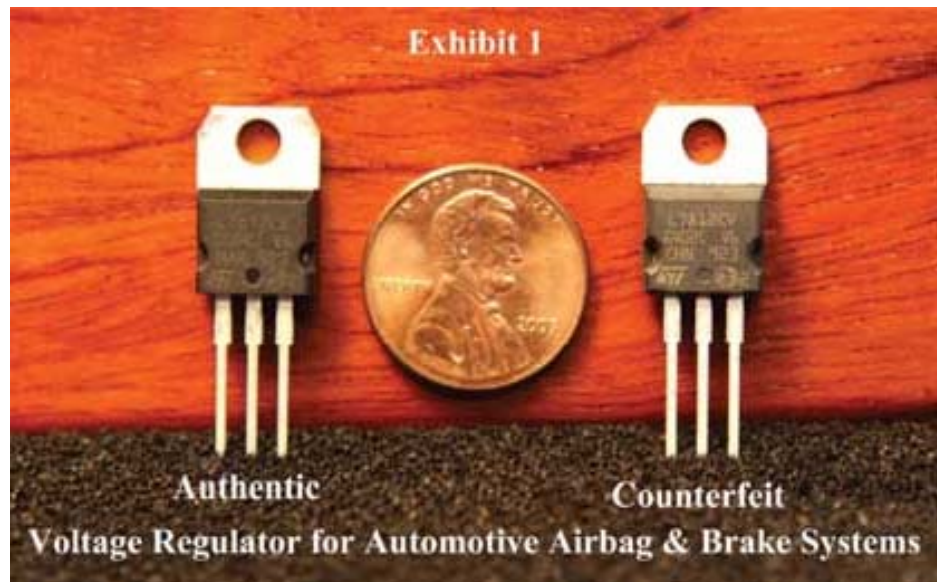
Counterfeit Systems

◆ How do you know components are legitimate?

- Often chips fail to meet specifications, but are superficially the same function
- What if such a chip finds its way into a critical application?
- US Customs seizes perhaps 1-2million fake ICs per year (others get by)

◆ What if someone wants to clone your whole product?

- “Tamper-proofing” may help, but not if lots of money is to be made
- Clones might be built in part via scavanging authentic components
- Will need to have some way to authenticate and track serial numbers



Example Security Pitfalls

◆ Security via obscurity

- Secret designs never stay secret

◆ Cheesy cryptography

- Use full-strength crypto & keys
- Kids: don't try this at home

◆ Assuming tamper-proofing really works

- It mostly works, but chip peels aren't that expensive

◆ Back doors, manufacturer passwords, master keys

- What will you do when someone finds out the master password?

◆ Using encryption when what you want is integrity

- Especially if you want to export a device (authentication is easier)

◆ Forgetting to plan for patches/updates

- Can you trust the owner to keep up with patches? Who gets sued if they don't?

◆ Forgetting that the owner of the device is an attacker

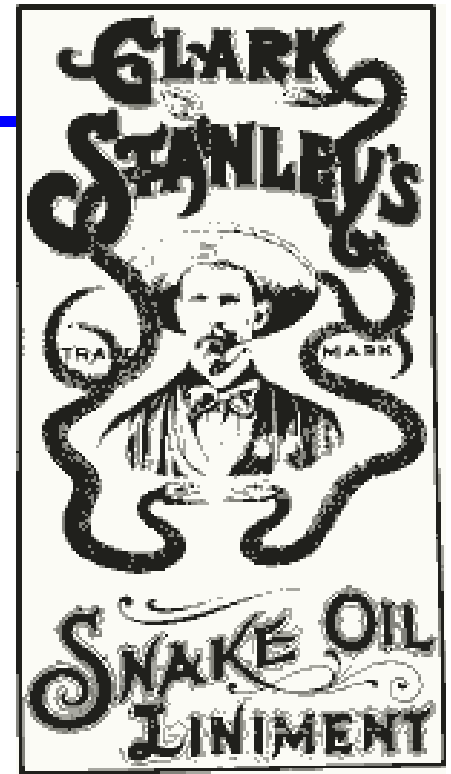


<http://www.deseretnews.com/article/865591266/Truck-driver-crashes-through-airport-fence-and-flees-on-foot-with-passenger.html?pg=all>

<http://betterembsw.blogspot.com/2011/10/embedded-security-pitfalls.html>

Security Big Picture

- ◆ **Getting embedded security right is hard work**
 - Getting embedded-to-cloud security is harder
- ◆ **Embedded security is immature**
 - Most security folks don't understand embedded
 - Most embedded systems folks don't understand security
 - Thus ... there will be a lot of **snake oil** out there for a while
 - **Get some help** sorting out the real stuff from the snake oil
- ◆ **Have a Security Plan as part of your system design**
 - Security goals (how much security do you need?)
 - Plausible attacks
 - Failure criticality if attacks succeed
 - Countermeasures to mitigate the most critical attacks
 - Update & monitoring strategy



Summary

- ◆ **Embedded Internet is more than just adding an Internet connection**
 - Embedded systems have different characteristics than desktop systems
- ◆ **As difficult as security for desktop systems is, embedded might be harder**
 - Harsher operating environment
 - Can have high consequences for failure
 - Lower availability of trained maintenance personnel
 - ...
- ◆ **This talk is largely motivation/horror stories**
 - Book chapter presents a more typical overview of security