

22

Embedded Internet & Security Overview

18-649 Distributed Embedded Systems

Philip Koopman

November 21, 2011

**Carnegie
Mellon**

Four Engineers In A Car Run Off The Road

◆ Mechanical Engineer

- “I’d better check the fluid levels. Nope, they're OK -- must be those computer jerks made another mistake. It hasn't been the same since they started putting all that electronic junk into cars!”

◆ Hardware Engineer

- “CPU self-tests just fine; this must be a software bug”

◆ Software Engineer

- “Let’s reboot, roll it back up the hill and see if it does it again”

◆ Secure Embedded Engineer

- “Let’s check the car’s firewall, download the latest security patches, reboot, roll it back up the hill, and see if it does it again.”

Would You Pay More for an Internet Toaster?

◆ Toaster: \$20



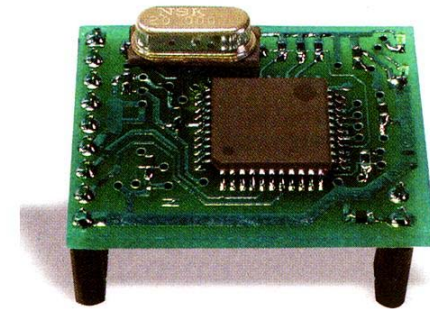
http://ecx.images-amazon.com/images/I/51Zhp9PCxdL._SS500_.jpg

◆ Internet Toaster:

- Toaster: \$20



- Embedded Web Server: \$20



The SitePlayer Web server, a 1-sq-in. module, costs less than \$20 in OEM quantities.

- Bluetooth radio chip: \$5
- *Toast etching laser* ~\$200
- WinCE license: ~\$50

What Would You Do With An Internet Toaster?

◆ Spam on toast for breakfast: *priceless*

To: Spamlist@spam.org
Subject: MAKE MONEY FAST!
From: David Rhodes
Date: 26 Aug 1994 14:53:58 -0600

INSTRUCTIONS

**Follow these instructions
EXACTLY, and in 20 to 60
days you will have received
well over \$50,000.00 cash,
all yours.**

- 1) IMMEDIATELY mail \$1.00 to the first 5 (five) names listed below starting at number 1 through number 5. Send CASH only please (total investment \$5.00). Enclose a note with each letter stating: "Please add my name to your mailing list." For other countries the equivalent amount may be sent, e.g. in Hong Kong Send HK\$10 as this is the lowest denomination note. (This is a legitimate service that you are requesting and you are paying \$1.00 for this service).
- 2) REMOVE the name that appears number 1 on the list. Move the other 9 names up one position. (Number 2 will become number 1 and number 3 will become number 2, etc.) Place your name, address and zip code in the number 10 position.
- 3) Post the new letter with your name in the number 10 position into 10 (Ten) separate bulletin boards in the message base or to the file section. Call the file, MAKE.MONEY.FAST.
- 4) Within 60 days you will receive over \$50,000.00 in CASH. Keep a copy of this file for yourself so that you can use it again and again

More Realistic 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 machine (Korean & Italian versions)

- Determines cycle based on care needs of clothing
- Adjusts for detergent, water conditions & soil conditions



◆ Idea: an Internet breadmaking machine

- Yeast bread is critically dependent upon humidity & temperature conditions
- Use short-range weather forecast to adjust yeast & rising profile

◆ Internet fridge

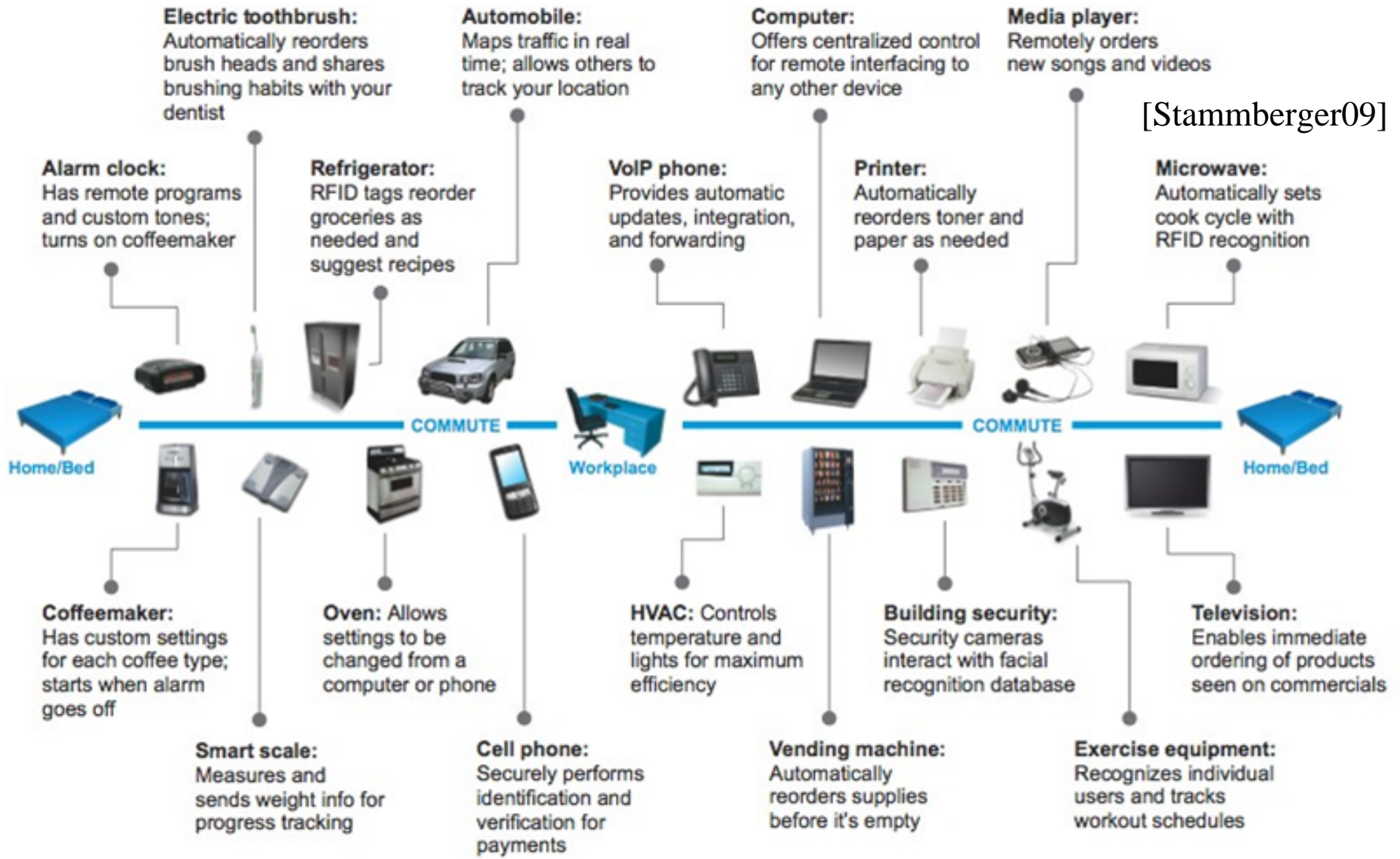
- Contacts grocery store to re-order

◆ Internet sewing machine

- Download stitching patterns from the web



Smart Homes/Offices – A good idea?



[Stamberger09]

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

Is Security An Issue For Embedded Systems?

◆ YES ... but only recently becoming real news

- Jul 2009: “Meticulously prepared” attack from N. Korea against S. Korea & US
- Nov 2009: *60 Minutes* reports two Brazilian power outages due to attacks

◆ 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 (Shipley & 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

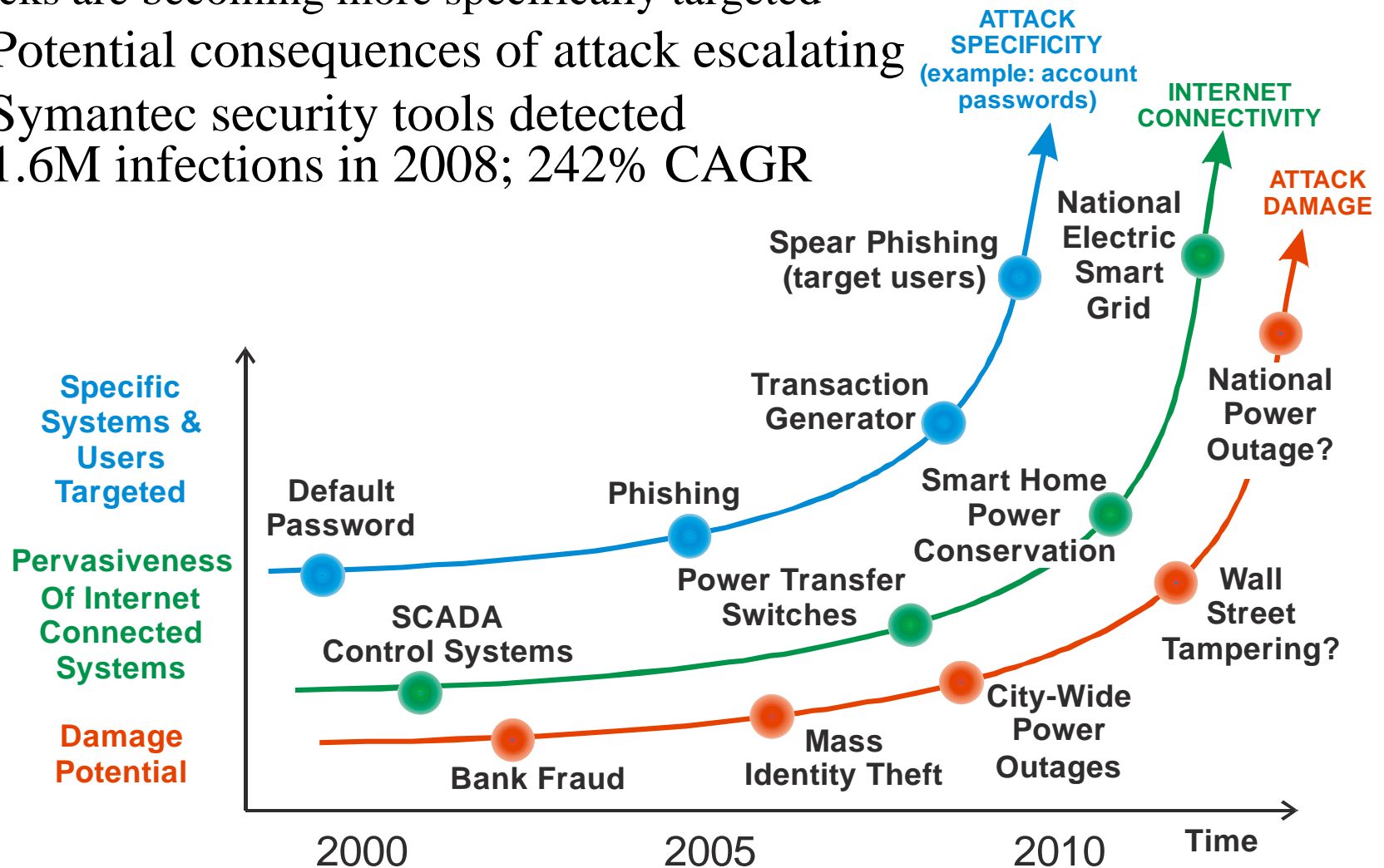
◆ But, why will this be different than, say, bank security?

- Beyond them being mostly 8- & 16-bit CPUs with no OS?

Risk Due To Attacks Is Increasing Over Time

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

[Emerson Electric]



ATTACK SPECIFICITY AND DAMAGE INCREASING AS CONNECTIVITY RISES

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

Basic Security Concepts

◆ Confidentiality

- Information is kept secret from those who aren't supposed to know it

◆ 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 might not matter much for control systems (except for privacy issues)
- Integrity matters a lot for safety critical systems
- Reliability might be more important than availability, but both matter

High-Level Embedded/Internet Contrast

◆ Classical Embedded:

- 5-50 year life cycle
- Small, multidisciplinary teams
- Real-time control of the physical world
- Safety/mission critical; reliability-based concerns
- Synchronized, short network messages; correlated traffic bursts
- Security prevents unauthorized use
- Software is incidental to tangible product; HW owned by consumer
- Computer is “invisible”

◆ Classical Internet:

- 3 month – 3 year life cycle
- Small to large software team
- Data processing
- Usually not perceived as critical; availability-based concerns
- Sporadic, longer messages; generally uncorrelated traffic
- Security is confidentiality/privacy
- Service or data *is* the product; capital equipment required
- Person is using a “real computer”

Embedded 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(!)



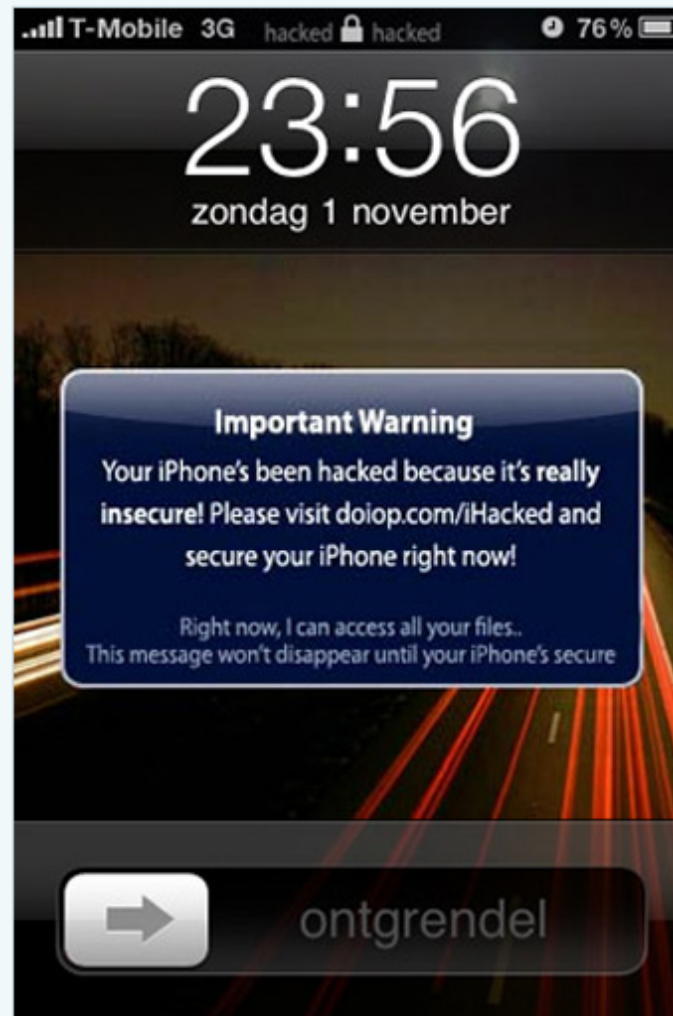
◆ Who's the sysadmin for your house? For your car?

- 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



words of caution:

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

War Dialing

[Material on this slide from Chenxi Wang]

◆ An automated method to connect to modems

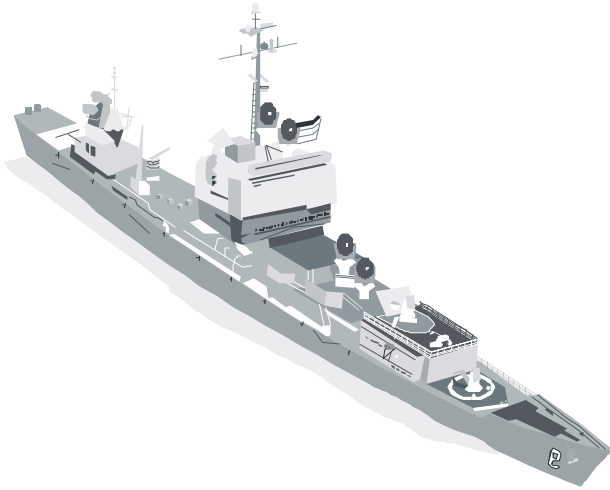
- One of the most common security breaches
- Embedded systems *still* assume unlisted phone number provides security

◆ A war-dialing study (Shipkey, 2000)

- A Fortune 100 company's air conditioner and environmental control units accessible by modems were unprotected, a hacker can overheat buildings or kill lights at will
- Medical records for several Bay Area facilities
- Oakland Fire Department's dispatch computers

Area Code	Prefix	Begin	End
210	324	1000	2000

Trend: Desktop Software In Embedded Systems



7/28/98:

“Windows NT Cripples US Navy Cruiser”

◆ Diebold voting machine problems

- Electronic voting machines booting to windows instead of votes
- <http://catless.ncl.ac.uk/Risks/23.27.html#subj8.1>

◆ Automated teller machine crashes

- Windows error messages
- At Carnegie Mellon, someone got an ATM to run media player



http://www.coed.org/photodb/folder.tcl?folder_id=3334
"When ATMs go bad by Carla Geisser", March 18, 2004
(See also: <http://midnightspaghetti.com/newsDiebold.php>)

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.

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.

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?

Myth: Discipline Will Solve Security Worries

- ◆ **Hacker's can't hurt your car if the infotainment system doesn't "talk" to the braking system**
 - Solution: don't put a connection between radio and brakes
- ◆ **Product idea: radio volume to achieve constant SNR**
 - Road noise based on wheel speed, tire pressure, road surface
 - Which sensor has the best information about this?
 - Anti-lock brake system
 - “Well, we'll just put in a fire-wall... surely that will be OK”
 - ***Reality:*** the connectivity will happen; denial is counterproductive
 - Prototype vehicle of a Big-3 manufacturer suffered failure when the radio speaker caused an engine controller malfunction

Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen  March 17, 2010 | 1:52 pm | Categories: [Breaches](#), [Crime](#), [Cybersecurity](#), [Hacks and Cracks](#)

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.



Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership's four Austin-area lots.

"We initially dismissed it as mechanical failure," says [Texas Auto Center](#) manager Martin Garcia. "We started having a rash of up to a hundred customers at one time complaining. Some customers complained of the horns going off in the middle of the night. The only option they had was to remove the battery."

The dealership used a system called Webtech Plus as an alternative to repossessing vehicles that haven't been paid for. Operated by Cleveland-based [Pay Technologies](#), the system lets car dealers install a small black box under vehicle dashboards that responds to commands issued through a central website, and relayed over a wireless pager network. The dealer can disable a car's ignition system, or trigger the horn to begin honking, as a reminder that a payment is due. The system will not stop a running vehicle.

[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.

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.

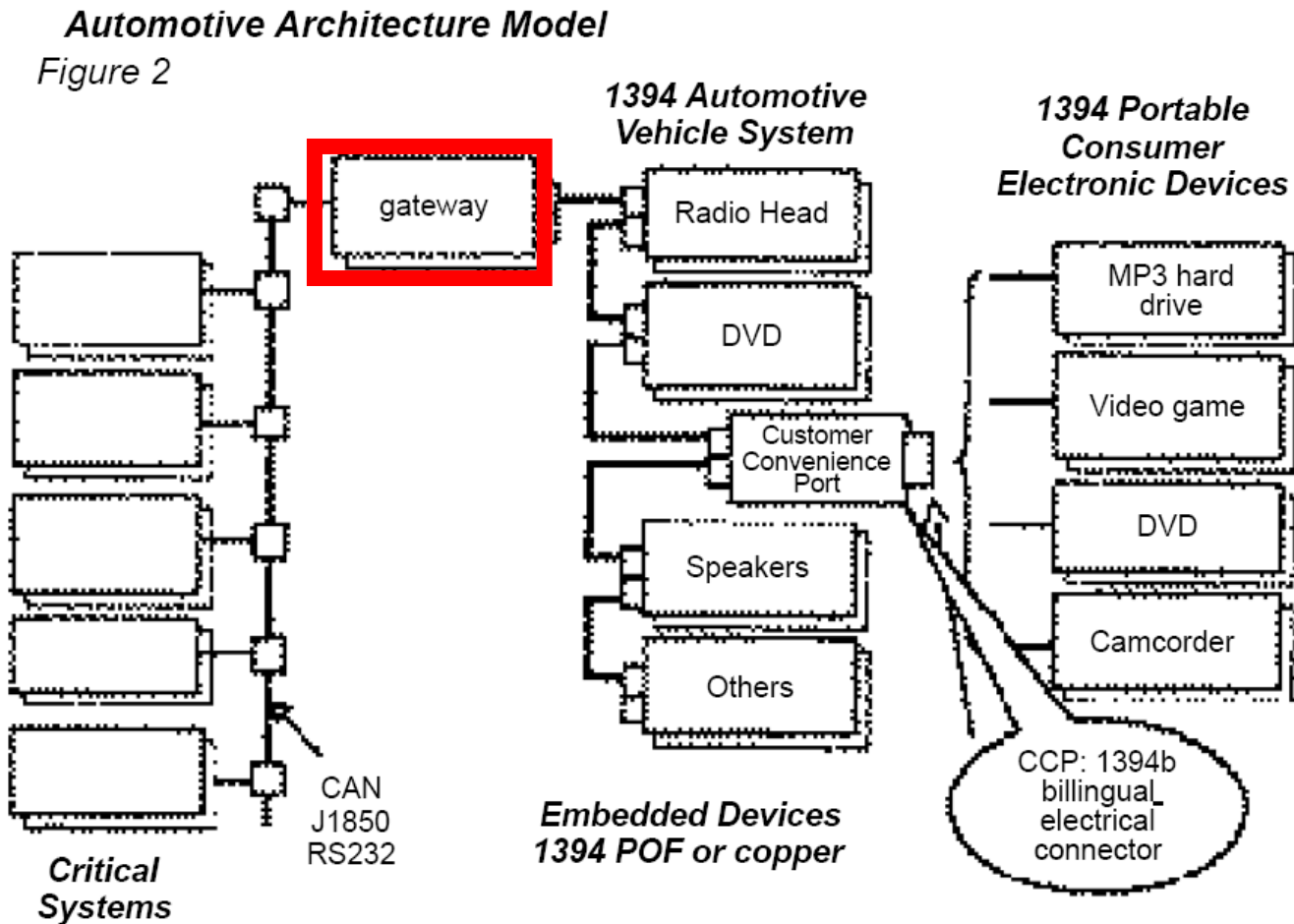
The U.S. National Transportation Safety Board reported in a preliminary investigation that the plane had taken off with its flaps and slats retracted — and that no audible alarm had been heard to warn of this because the systems delivering power to the take-off warning system failed. Two earlier events 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/

What Goes In the Gateway?



Polishuk, 2001, proposed automotive vehicle architecture
Infotainment 1 FW away from critical systems!

Would You Run Windows As In-Flight Software?

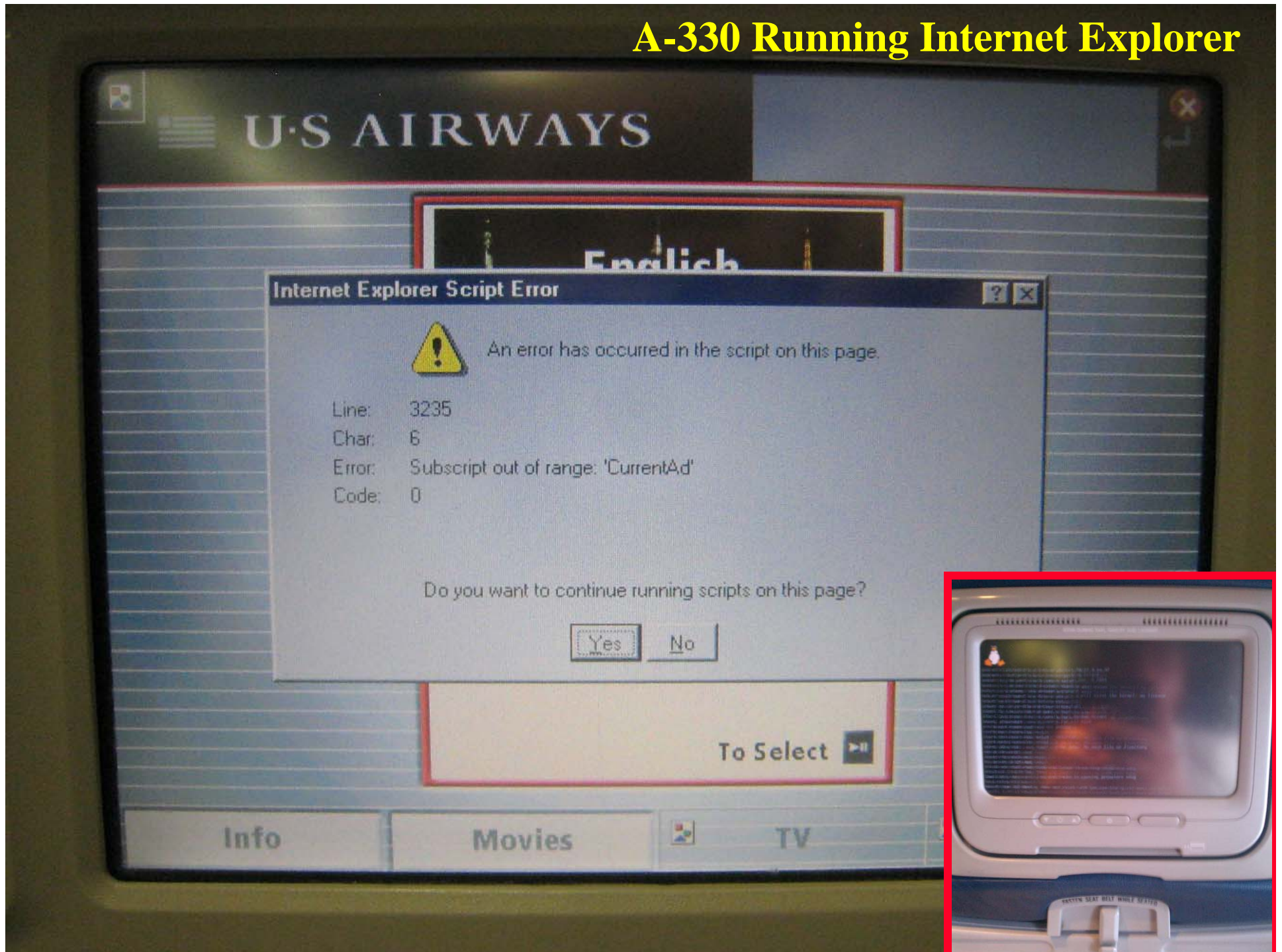
- ◆ **Safety critical subsystems will be connected to external networks (directly or indirectly)**
 - E-enabled aircraft architecture (next slide)



Computer graphics by IBM

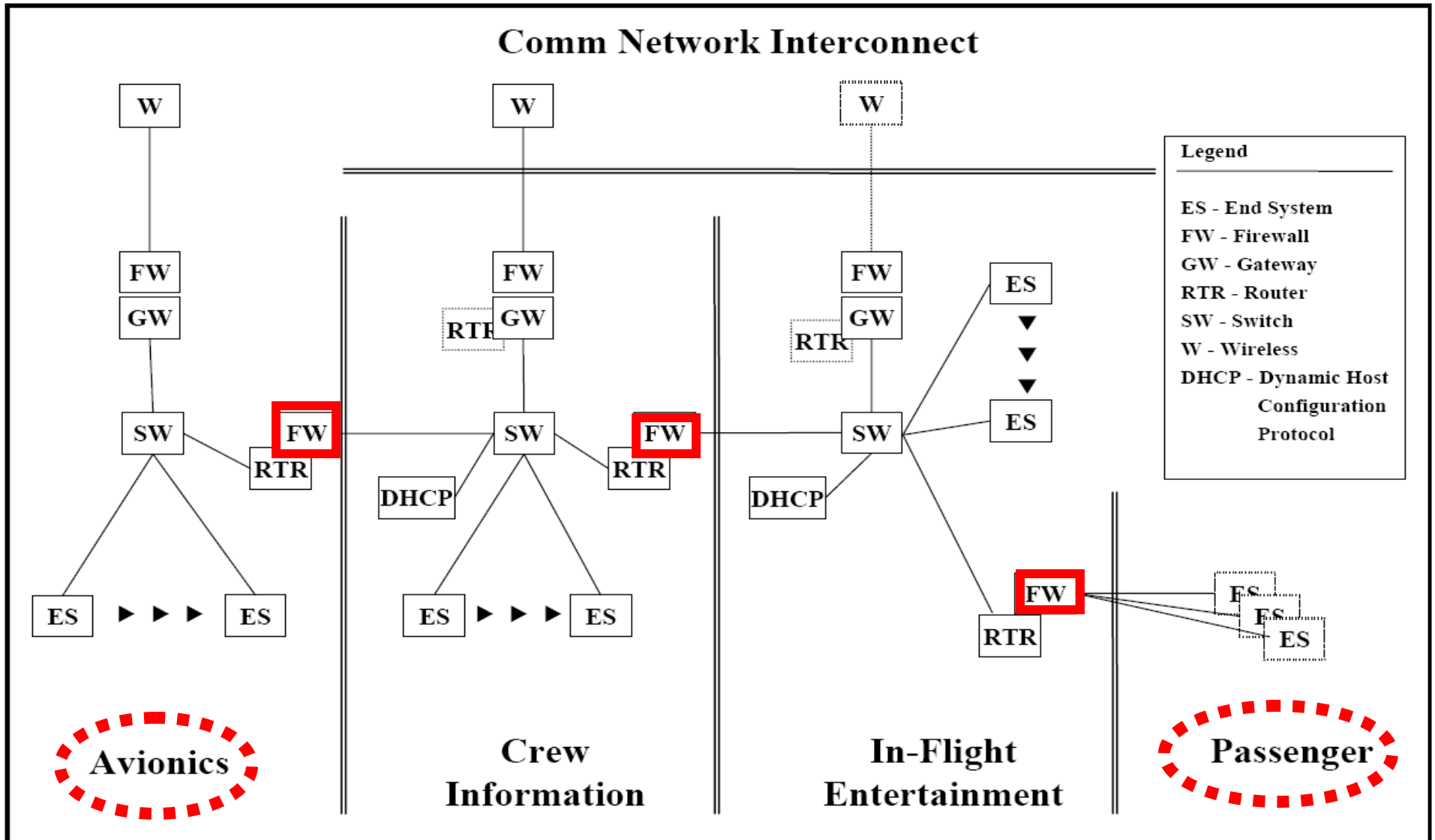
[Airbus 2004] Airbus 380 uses IP-based flight controls

A-330 Running Internet Explorer



Do Plane Seats Talk To Flight Systems? (Yes.)



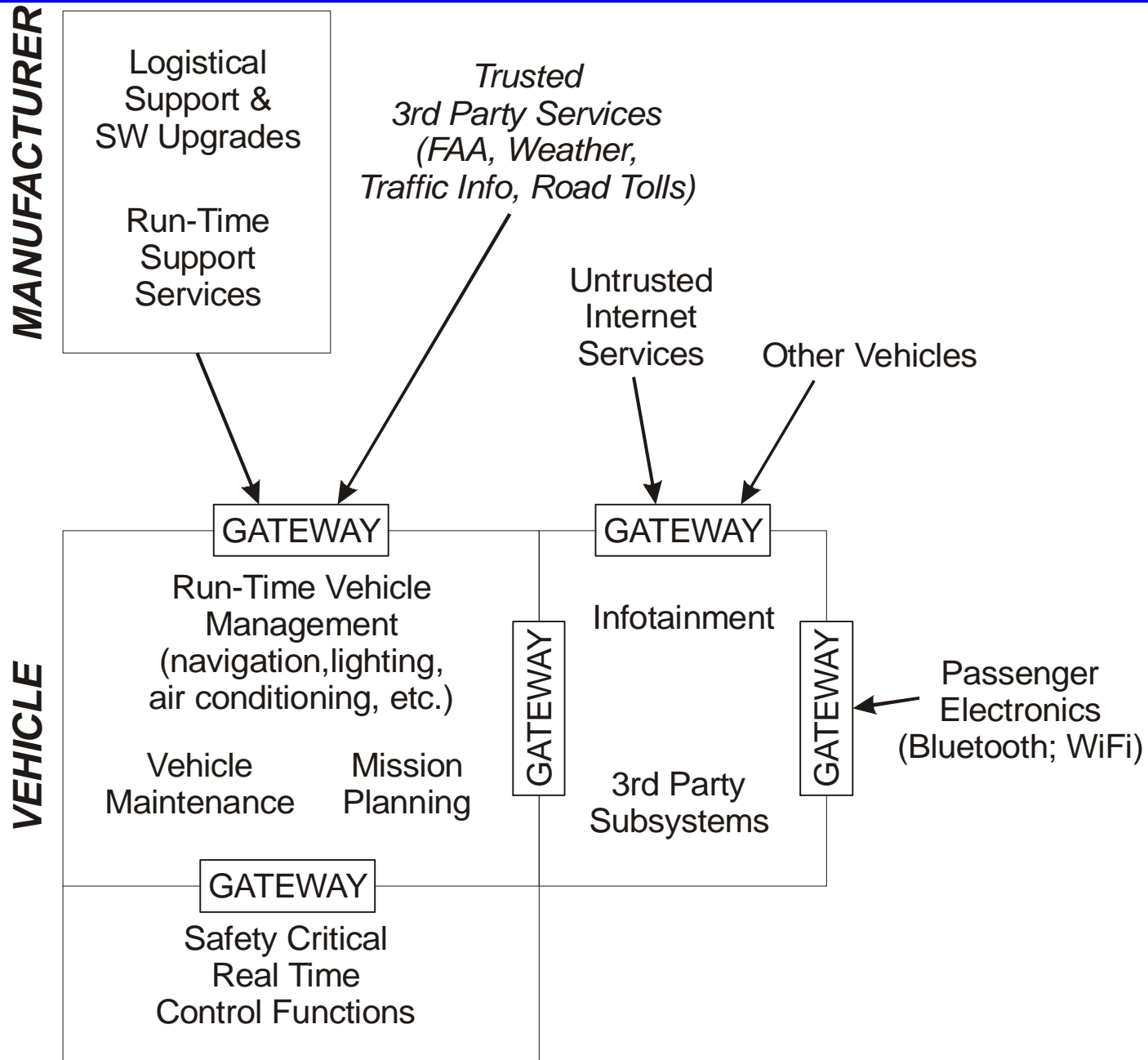


Wargo & Chas, 2003, proposed Airbus A-380 architecture

Passenger laptops are 3 Firewalls away from flight controls!

Internet connects somewhere as well

General Vehicle Architecture With Gateways



Research Area: Embedded/Internet Gateway

- ◆ What happens at the embedded/internet interface?
 - If there is a “firewall” or “gateway” there, what does it do?
 - Open research question...

**Embedded
Side**

Control-oriented
Time Triggered
Continuous
Real Time
Periodic Messages
Short Messages
Roll-forward
Lower cost

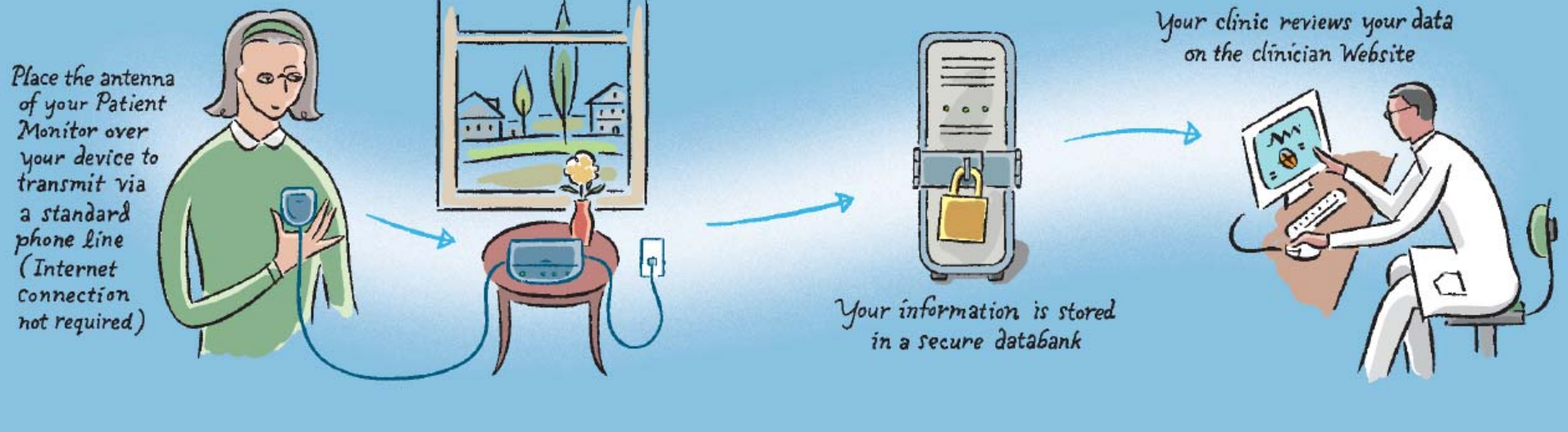
GATEWAY

**Enterprise
Side**

Transaction-oriented
Event Triggered
Discrete
Mostly not Real Time
Aperiodic Messages
Longer messages
Rollback
Higher cost

Internet Pacemaker Anyone?

Medtronic CareLink Service



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

Some Embedded-Specific Security Issues

- ◆ **Adding authentication to embedded systems**
 - Small CPUs, little memory, short network messages, no built-in security
- ◆ **Power drain attacks**
 - Attacks designed to deplete batteries
- ◆ **Real time operation attacks**
 - Only a slight overload might cause real time schedule problems
- ◆ **Tamper resistance & evidence for critical properties**
 - How can you prove someone didn't alter your safety critical system? (Even if they have permissions to install updates?)
- ◆ **Ensuring updates are authentic & are installed**
 - How can you ensure only certified configurations will run?
 - How do you ensure installation of required updates with intermittent external connectivity?

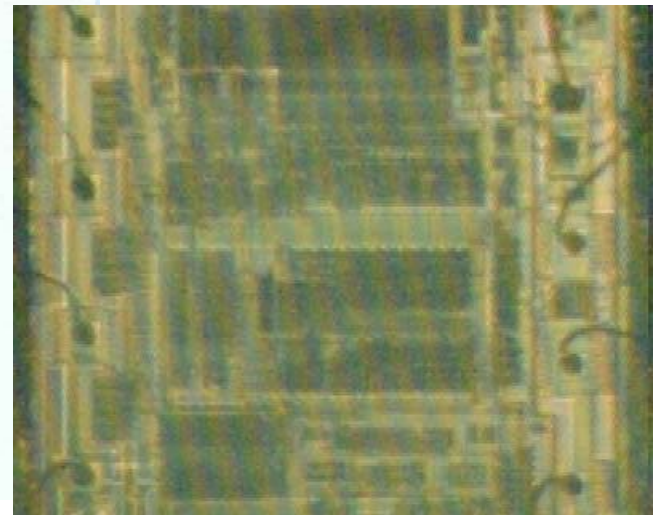
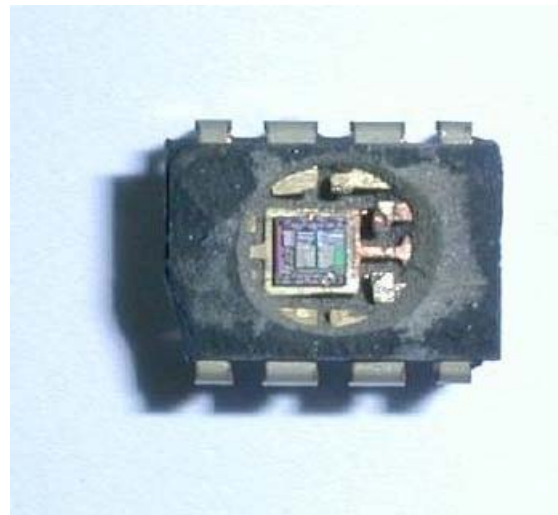
Intellectual Property Protection

◆ 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



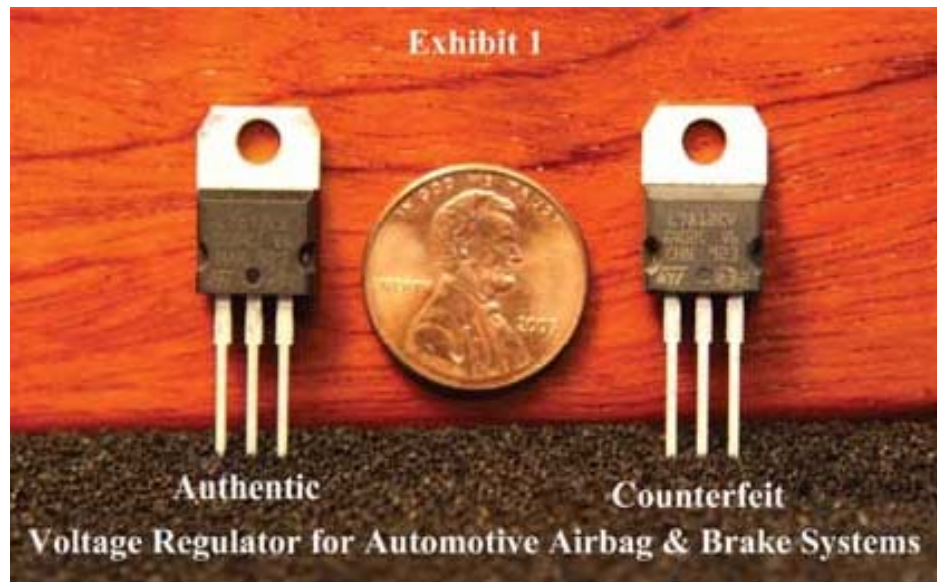
Counterfeit Systems

◆ 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



Would You Drive A Car In Which:

“THE SOFTWARE is provided ‘AS IS’ and with all faults. THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY, AND EFFORT (INCLUDING LACK OF NEGLIGENCE) IS WITH YOU.”

(You will.)



Summary

- ◆ **Embedded Internet is more than just adding an Internet connection**
 - Embedded systems have different characteristics than desktop systems
 - Cost is always an issue
 - Does it make sense to use a 32-bit CPU as a network interface peripheral to an 8-bit thermostat CPU?
- ◆ **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