Church of WiFi

Wireless
Extravaganza

Today's Brethren:

Thorn
theprez98
Renderman

Who Are The CoWF?

Q: Pirates? Ninjas? Pirates with stealthy Ninja skills? Ninjas who say "Arrgh"?

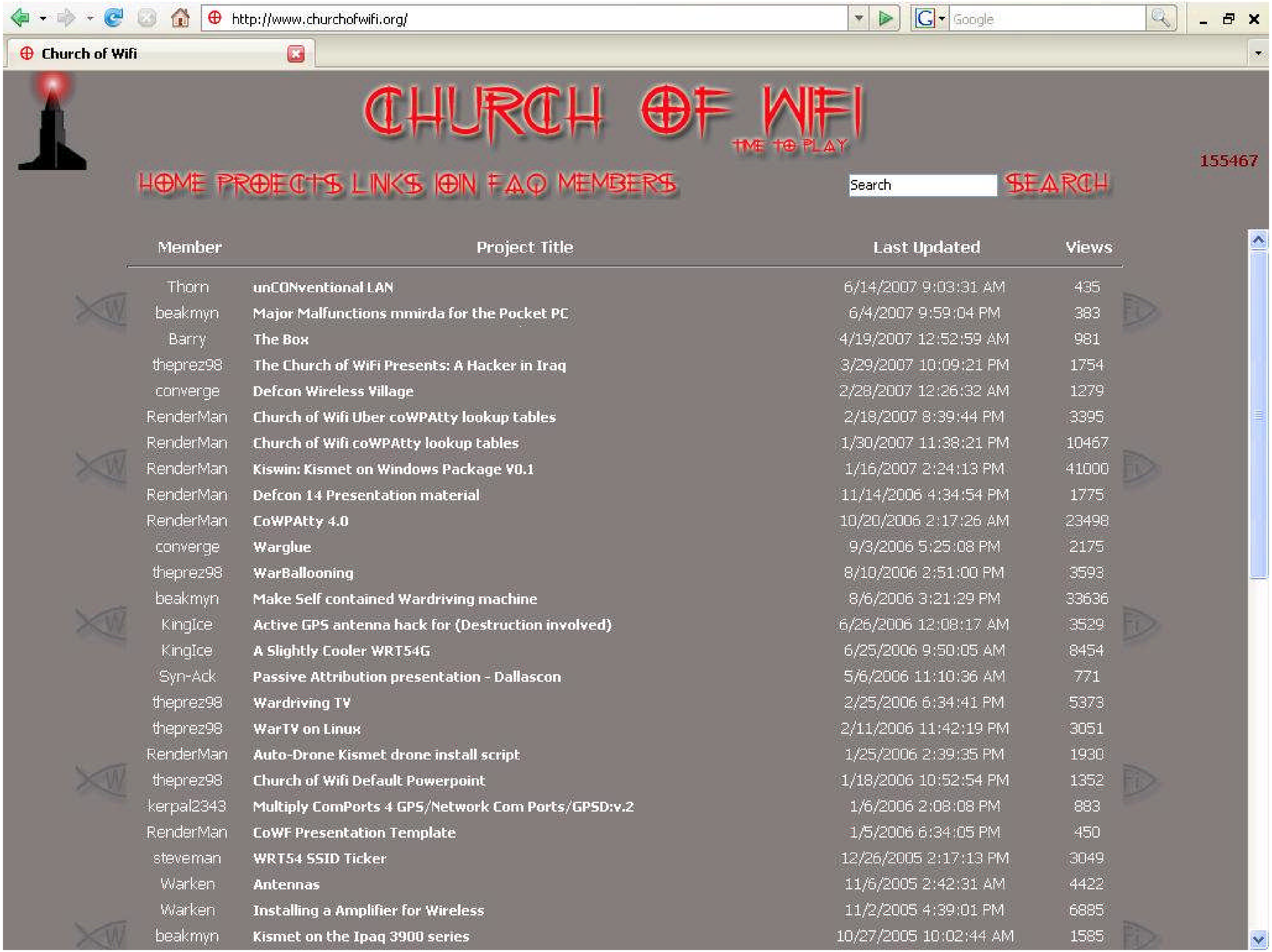
A #1: A “Church” where they do “WiFi Voodoo”

Who Are The CoWF?

A #2: A bunch of Monkeys who wear Pope hats

CHURCH OF WIFI

TIME TO PLAY


http://www.churchofwifi.org/
Google
Church of Wifi
CHURCH OF WIFI
TIME TO PLAY
155467
HOME PROJECTS LINKS JOIN FAQ MEMBERS
Search
SEARCH

Member	Project Title	Last Updated	Views
Thorn	unCONventional LAN	6/14/2007 9:03:31 AM	435
beakmyn	Major Malfunctions mmirda for the Pocket PC	6/4/2007 9:59:04 PM	383
Barry	The Box	4/19/2007 12:52:59 AM	981
theprez98	The Church of WiFi Presents: A Hacker in Iraq	3/29/2007 10:09:21 PM	1754
converge	Defcon Wireless Village	2/28/2007 12:26:32 AM	1279
RenderMan	Church of Wifi Uber coWPAtty lookup tables	2/18/2007 8:39:44 PM	3395
RenderMan	Church of Wifi coWPAtty lookup tables	1/30/2007 11:38:21 PM	10467
RenderMan	Kiswin: Kismet on Windows Package V0.1	1/16/2007 2:24:13 PM	41000
RenderMan	Defcon 14 Presentation material	11/14/2006 4:34:54 PM	1775
RenderMan	CoWPAtty 4.0	10/20/2006 2:17:26 AM	23498
converge	Warglue	9/3/2006 5:25:08 PM	2175
theprez98	WarBallooning	8/10/2006 2:51:00 PM	3593
beakmyn	Make Self contained Wardriving machine	8/6/2006 3:21:29 PM	33636
KingIce	Active GPS antenna hack for (Destruction involved)	6/26/2006 12:08:17 AM	3529
KingIce	A Slightly Cooler WRT54G	6/25/2006 9:50:05 AM	8454
Syn-Ack	Passive Attribution presentation - Dallascon	5/6/2006 11:10:36 AM	771
theprez98	Wardriving TV	2/25/2006 6:34:41 PM	5373
theprez98	WarTV on Linux	2/11/2006 11:42:19 PM	3051
RenderMan	Auto-Drone Kismet drone install script	1/25/2006 2:39:35 PM	1930
theprez98	Church of Wifi Default Powerpoint	1/18/2006 10:52:54 PM	1352
kerpal2343	Multiply ComPorts 4 GPS/Network Com Ports/GPSD:v.2	1/6/2006 2:08:08 PM	883
RenderMan	CoWF Presentation Template	1/5/2006 6:34:05 PM	450
steveman	WRT54 SSID Ticker	12/26/2005 2:17:13 PM	3049
Warken	Antennas	11/6/2005 2:42:31 AM	4422
Warken	Installing a Amplifier for Wireless	11/2/2005 4:39:01 PM	6885
beakmyn	Kismet on the Ipaq 3900 series	10/27/2005 10:02:44 AM	1585

The Problem…

The Defcon15 Wireless Village entices you with THE TOWER of POWER !

The Problem…

- No skillz!
- ***"You know, like nunchuck skills, bowhunting skills, computer hacking skills… Girls only want boyfriends who have great skills."***

The Idea…

Learn + Touch = DO!

"I care about demonstrating and inciting 'hacker attitude' toward my fellow attendees…"

-c0nverge

The Concept…

- Things we liked: Hands-on at Lockpick Village & LosT's informal breakout
- Provide an area for wireless tutorials, mini-presentations and breakout sessions
- Act as an introduction to the various wireless contests

Learn + Touch = DO!

The Solution:

DEFCON 15
WIRELESS
VILLAGE
Las Vegas Nevada : 2007 August 3rd - 5th , defcon.org and churchofwifi.org
CHURCH OF WIFI PRESENTS

Skybox 209

Wireless Village: Breakouts

- Breakout sessions are for any RF/Network subject
  - PSP Wireless Hacking (Squidly1)
  - RF Direction Finding (Renderman)
  - RFID (Thorn)
  - Even more! (WEP Cracking, WPA Cracking…)

Learn + Touch = DO!

Learn + Touch = DO!

Provide an open environment for learning of wireless network technologies

- Contests and tutorials: all skill levels from beginner to expert
- Breakout sessions: to introduce people to the wireless contests
- Mini-presentations and demonstrations: provide an venue for wireless speakers to follow-up their presentations with hands-on demos, classes, etc.

DEFCON 15
WIRELESS
VILLAGE
Las Vegas Nevada : 2007 August 3rd - 5th . defcon.org and churchofwifi.org
CHURCH OF WI FI PRESENTS

Skybox 209

DC Wireless Contests

- Integrated to the Village
- Allows people to learn a skill at the Village and then compete.

Learn + Touch = DO!

WPA-PSK ”Rainbow Tables”

- Same idea as LM or other “Rainbow” tables: Time vs. Computing power tradeoff
- 2006: 172,000 word dictionary x 1,000 most common SSIDs = 7 gig tables

WPA-PSK ”Rainbow Tables”

This year: 1,000,000 password dictionary x 1,000 most common SSIDs =

35GB

YIKES!

CoWF “Distro”

- USB-bootable full-Linux distro on a 100GB+ 3.5” HD (BackTrack 2 based)
- Boot off any laptop/PC, and run wireless security checks at will
- CoWPAtty integrated with the recently released CoWF WPA/WPA2 Rainbow tables
- 100GB+ leaves plenty of room for other Rainbow tables and other tools

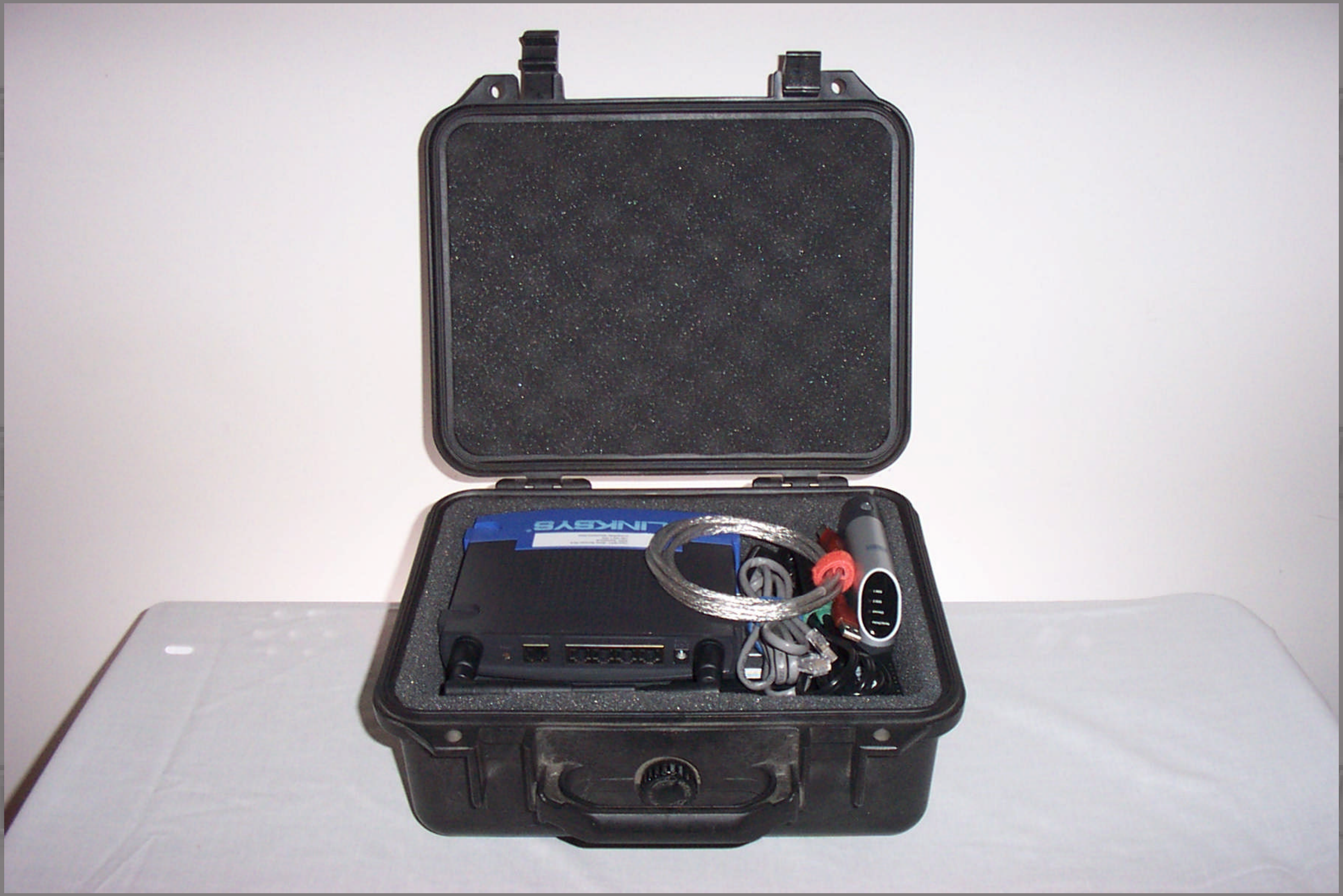
CoWF "Distro"

unCONventional LAN

- Linksys WRT54G Router version 2.2, running OpenWRT
- Linksys NSLU2 - Network Storage Link for USB 2.0 Disk Drives, running Unslung
- Maxtor OneTouch II USB hard drive
- Pelican Peli-Case
- Miscellaneous cables

unCONventional LAN

unCONventional LAN



Project Mutton

- Based on Linksys WPG12
- Unlike other Linksys products it's a PC-based SBC that boots from a CF card
- Built-in VGA
- Comes with a IR mouse/laser pointer.
- Keyboard PS2 interface on the PCB, but no connector
- New Linux distro and some scripts*, instant "Wall of Sheep/Wall of Shame in a box"

***Thanks, Irongeek!**

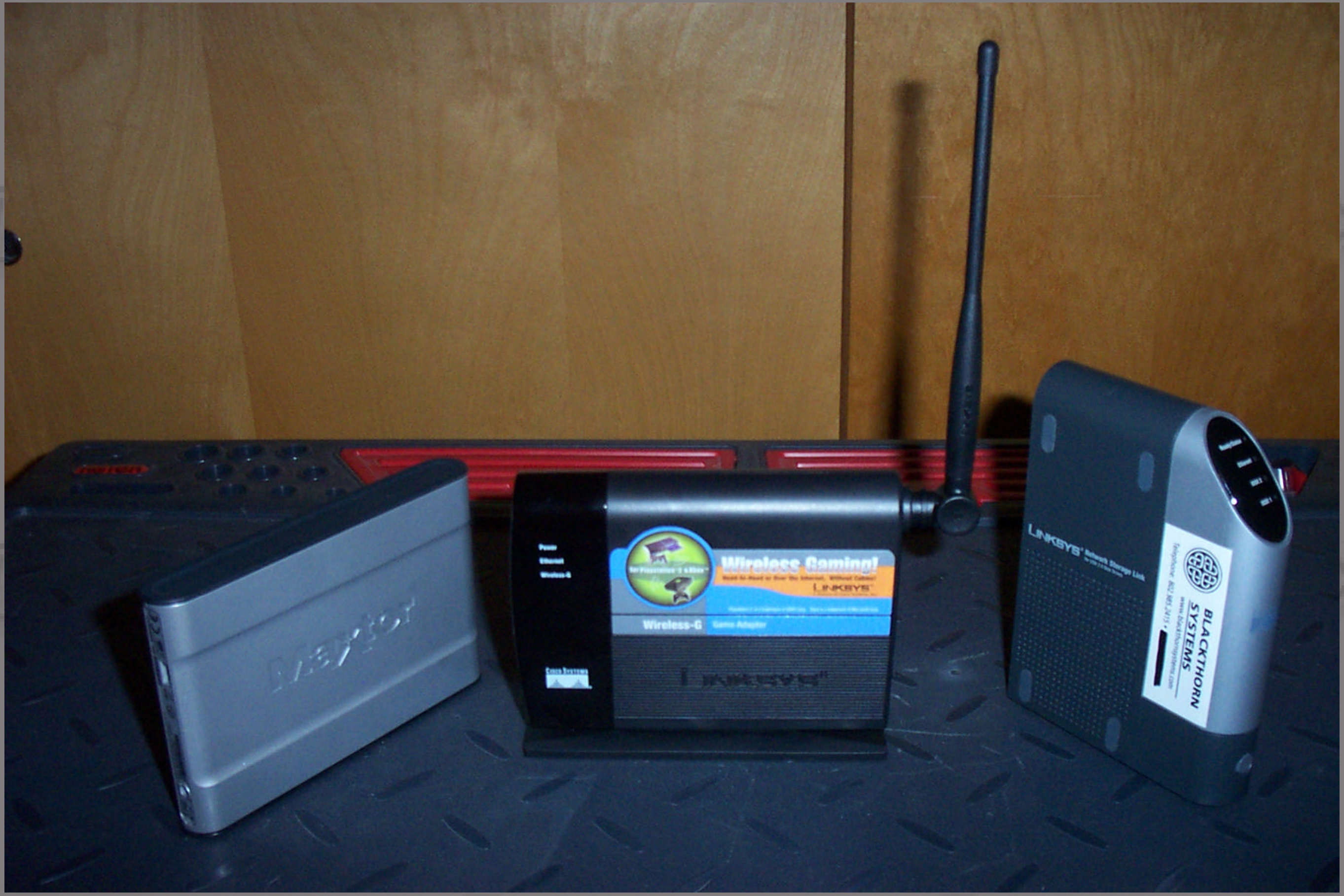
Project Mutton

Project Mutton

Stealth File Server

- Linksys WGA54G Game Adapter
- Linksys NSLU2 - Network Storage Link for USB 2.0 Disk Drives, running Unslung
- Maxtor OneTouch III USB hard drive
- Battery pack
- Fits in a camera bag
- David vs. the RIAA and MPAA’s Goliath?

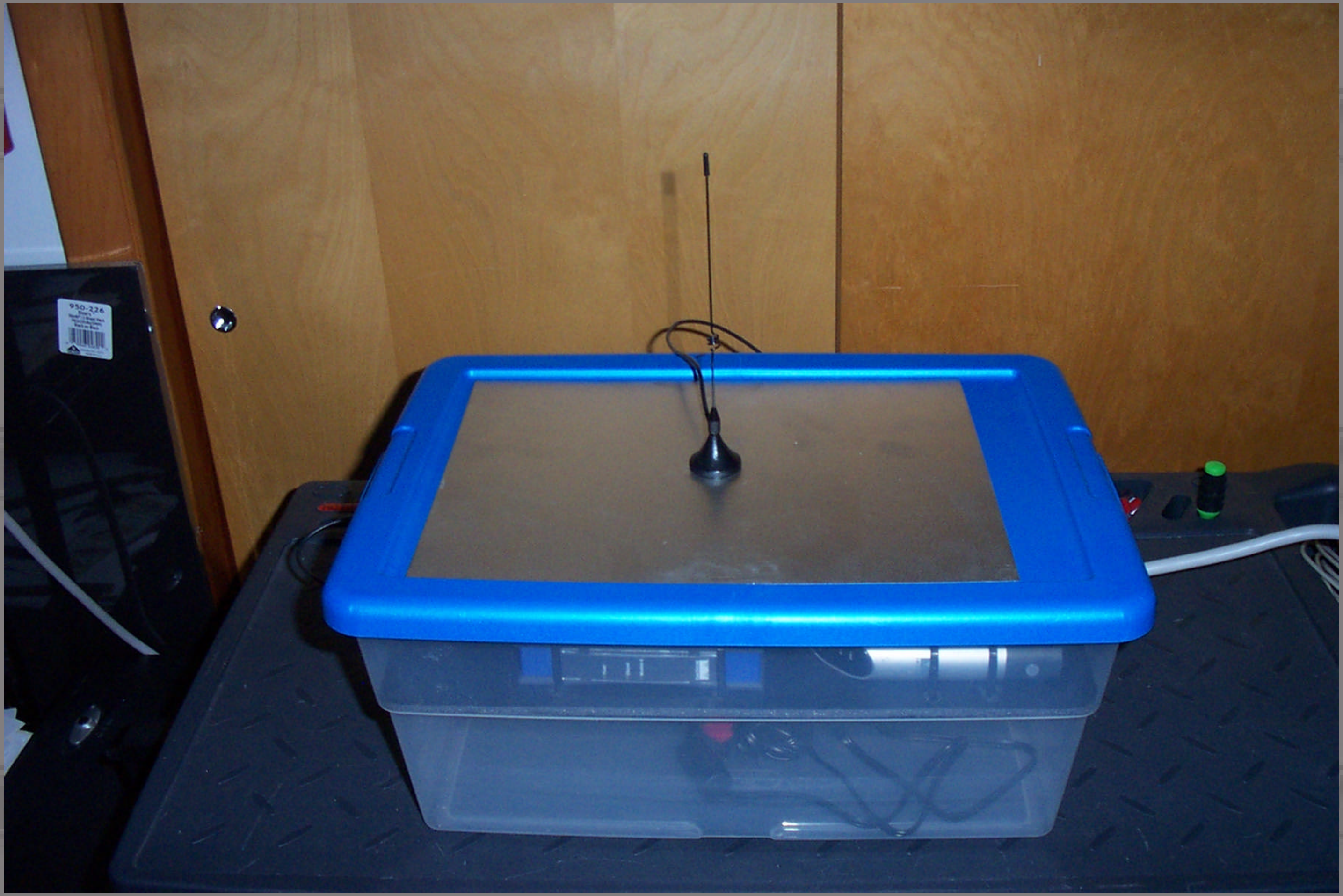
Stealth File Server



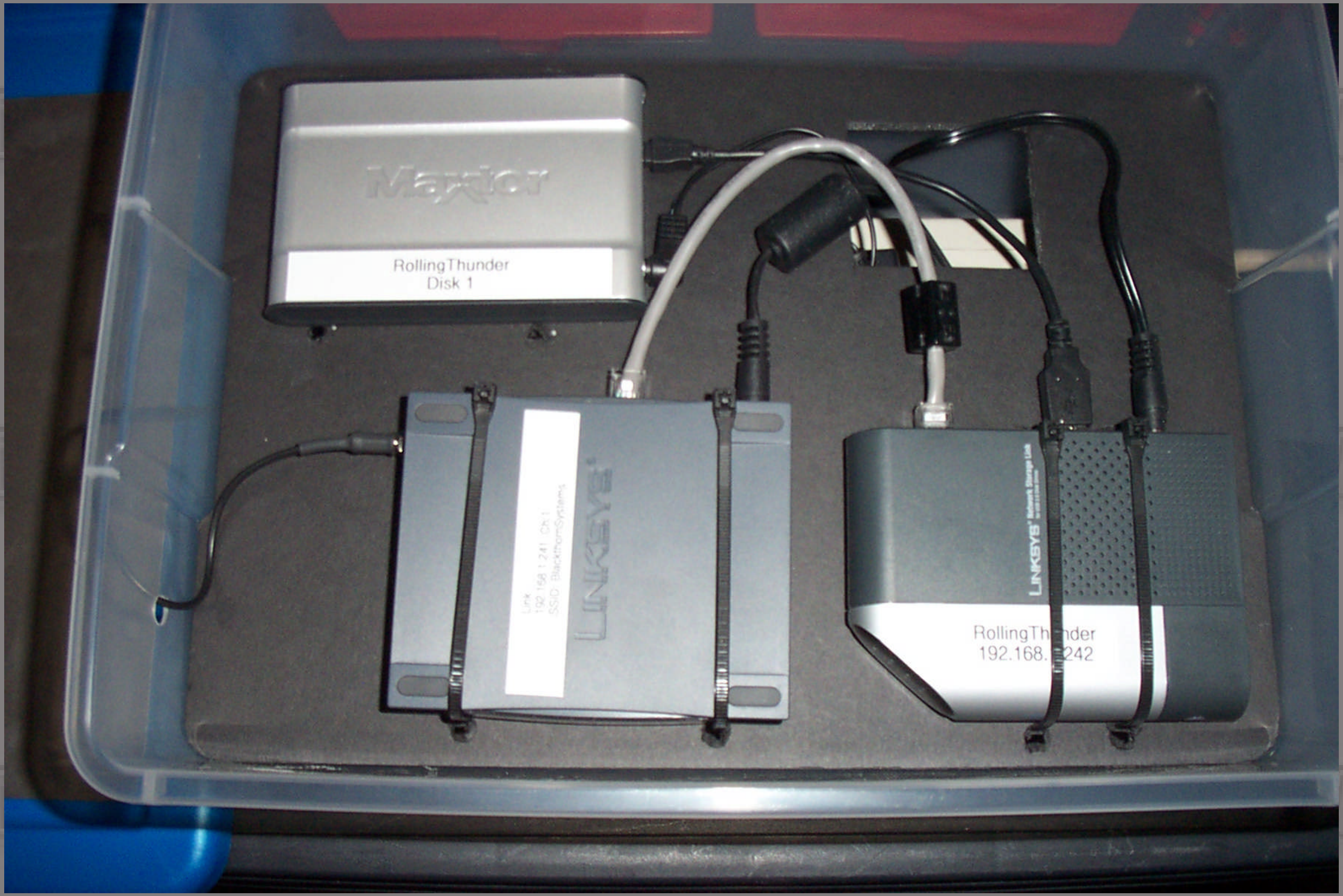
Rolling Thunder

- Linksys WET54G Wireless Bridge
- Linksys NSLU2 - Network Storage Link for USB 2.0 Disk Drives, running Unslung. Packages include Samba and rsync
- Maxtor OneTouch III USB hard drive
- Storage case
- 7dBd Antenna plus miscellaneous cables

Rolling Thunder



Rolling Thunder



CHURCH OF WIFI

TIME TO PLAY

theprez98!

What were you expecting? "The Larch?"

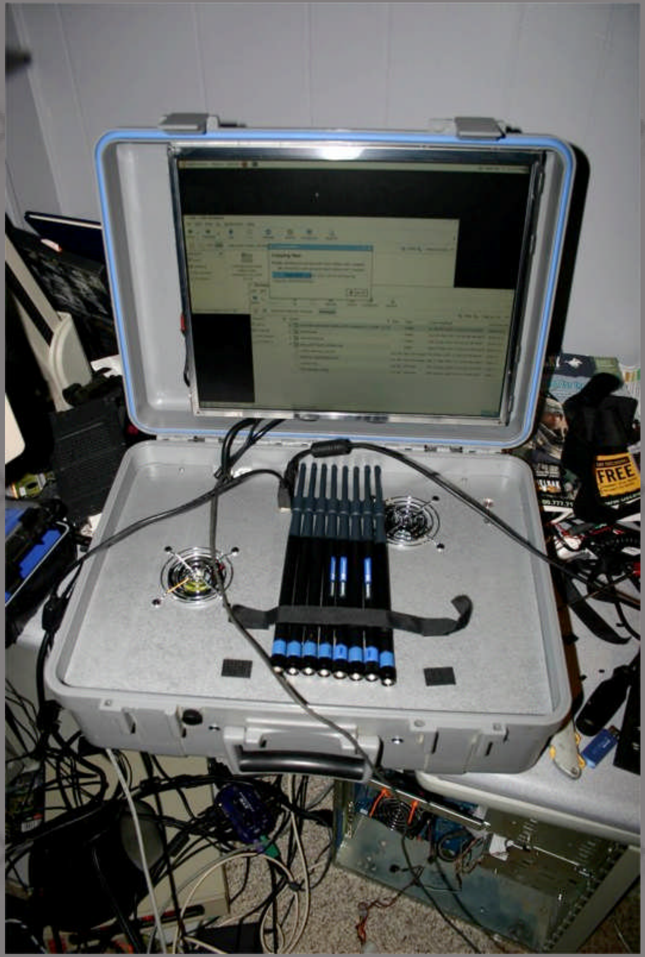
Wireless Contests

- Tower Challenge (tiered wireless challenge)
- WPA Cracking
- WEP Cracking
- Direction Finding
- RFID Locating – Find the RFID tags

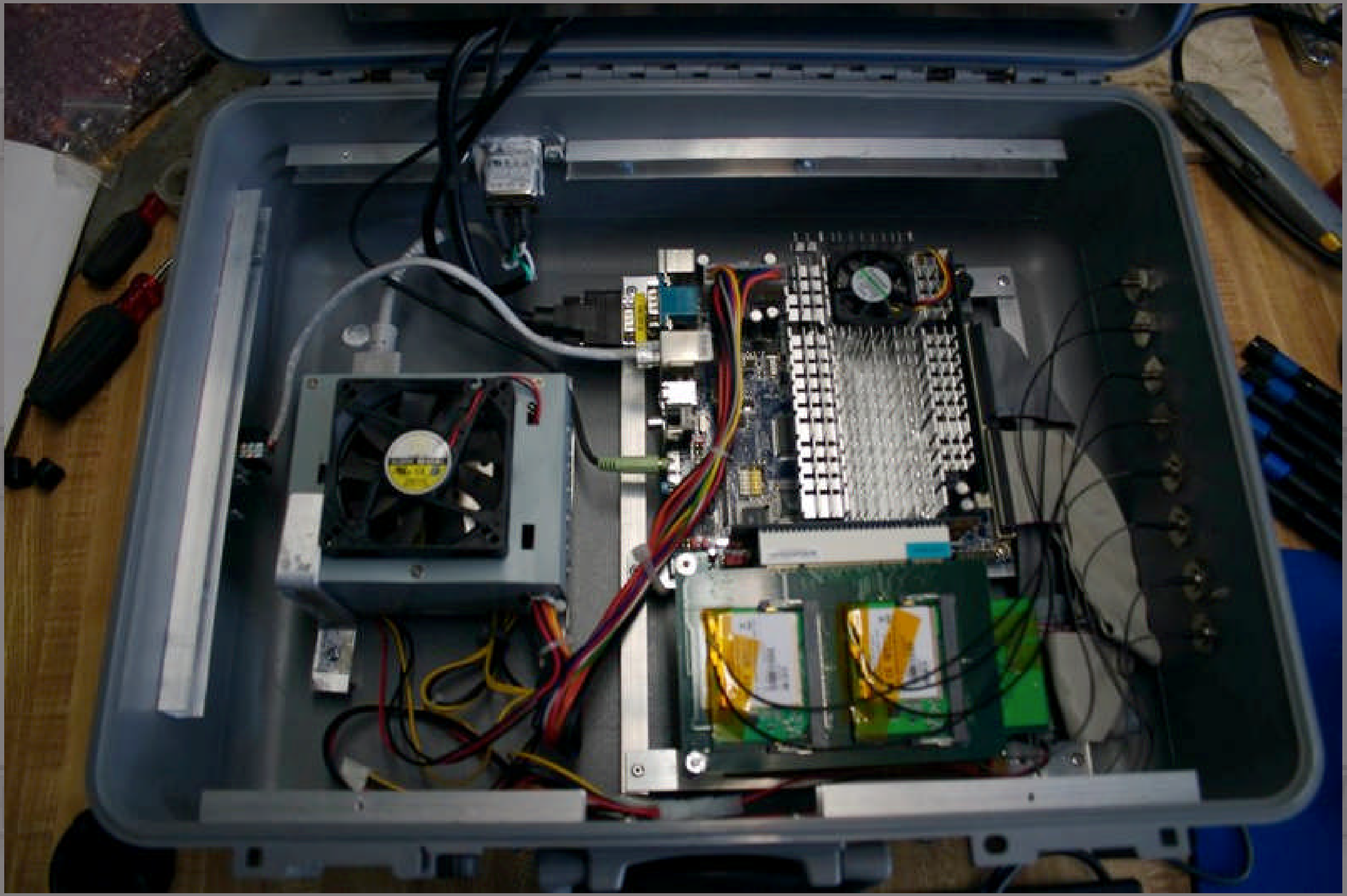
Barry's “The Box"

- "Janus" style portable computer for wireless surveys
- Epia EN1500G mini-itx logic board with a 1.5 GHz VIA C7 processor
- 1 GB DDR2 RAM
- 4X WLM54G 200mW 802.11bg mini PCI cards
- 30 Gb hard drive
- 60 Gb hard drive
- Ubuntu 6.10

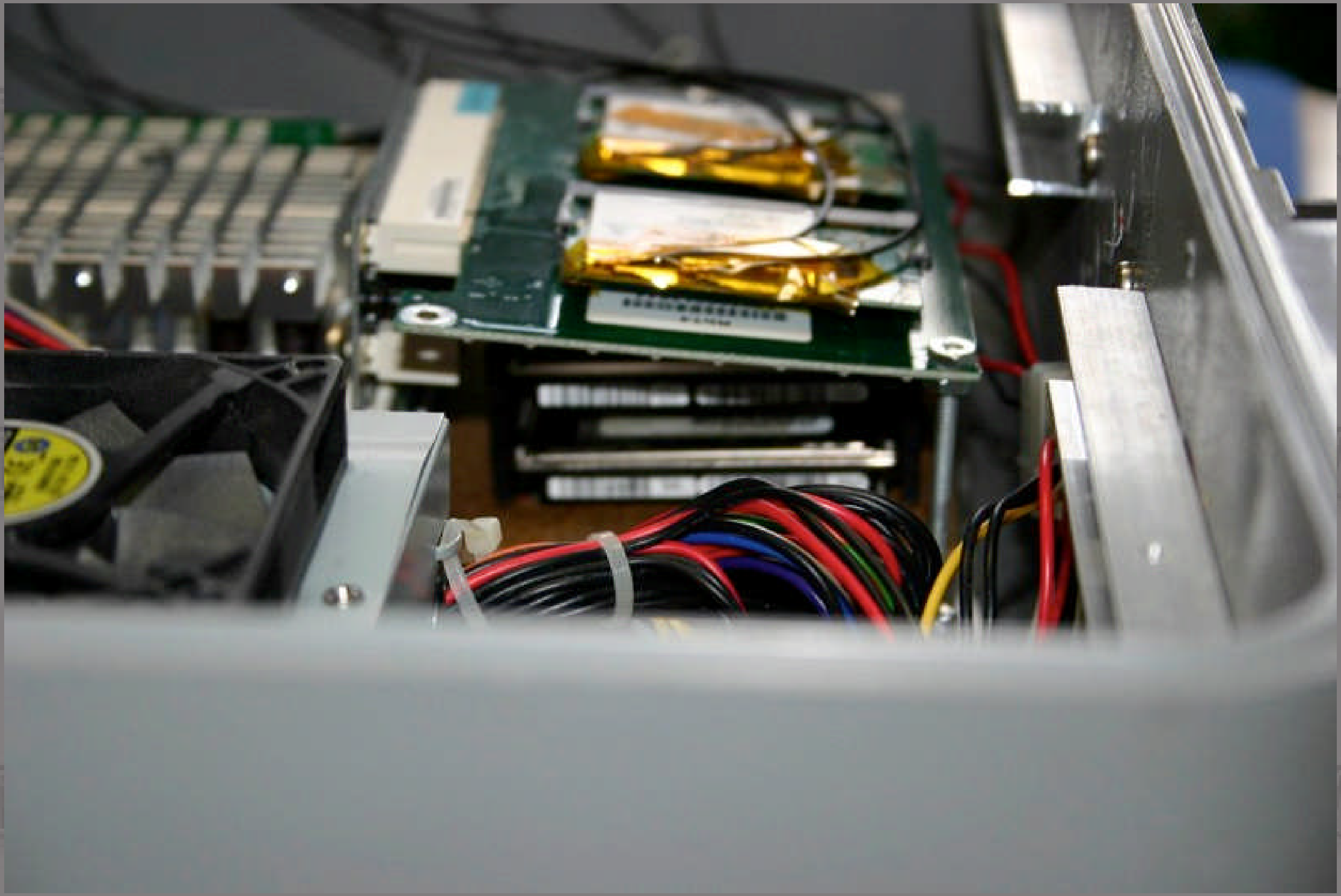
Barry's “The Box"



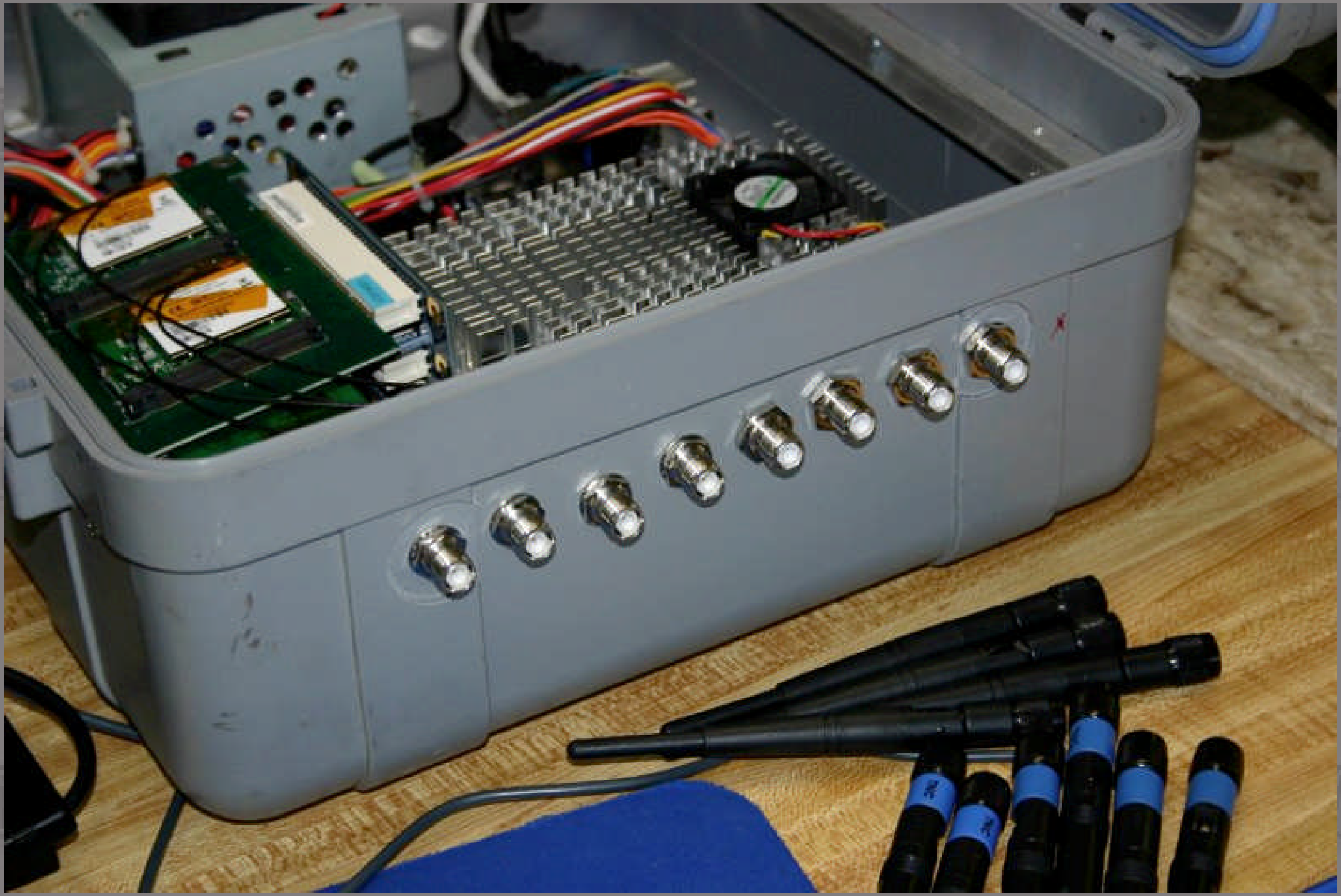
Barry's “The Box"



Barry's “The Box"



Barry's “The Box"



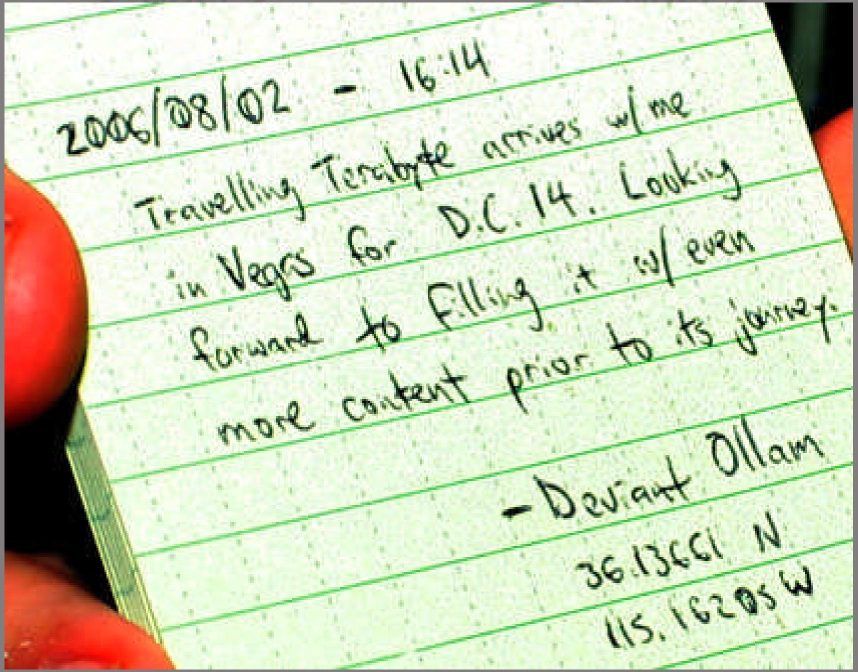
TTB Project Update

TTB Project Update

- Conceived by Deviant Ollam in June 2006
- "Army" Green Pelican Case (thx DaKahuna!)
- Two 500GB external hard drives
  - Past DEFCON content, movies, books, MP3s, etc.
  - Power adapters
  - Power converters
  - USB/Firewire

TTB Project Update

Debuted at DEFCON 14



2006/08/02 - 16:14

Travelling Terabyte arrives w/ me in Vegas for D.C. 14. Looking forward to filling it w/ even more content prior to its journey.

-Deviant Ollam

36.13661 N

115.16205 W

Already it's an "urban legend"!

TTB Project First “Owner”

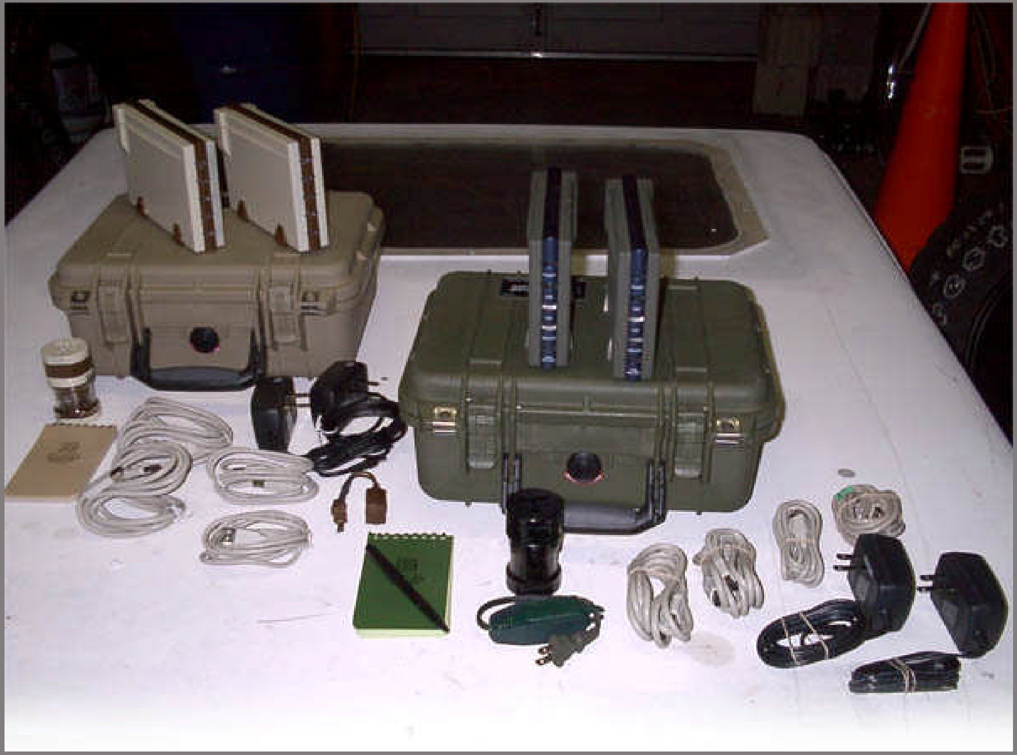
Las Vegas to Tampa

TTB Project Destination: Iraq

- Ashraf, Iraq (~50 miles north of Baghad; could be the middle of nowhere)
- New laptop + 25 DVDs provided plenty of storage space

TTB Project Update

- By October, a second TTB set of drives was unveiled



Travel Logs

- TTB #1 has been throughout the continental U.S. as well as Iraq and Kuwait
- Estimated to have travelled approximately ~25,000 miles (around the globe!)

TTB Project Further Resources

- TTB home - http://deviating.net/ttb/
- DC forums thread - https://forum.defcon.org/showthread.php?t=7381
- News article - http://seclists.org/isn/2006/Aug/0053.html

Shameless Self Promotion Slide

- Check out the Wireless Village in Skybox 209
- Check out the Wireless Contests
- “The Church of WiFi presents…Hacking Iraq”
  - 8pm tomorrow night in Area 1
- I'm looking for a job, consider hiring me ;-)

Render’s Rant

You didn't think you'd get away that easily, did you?

Render’s Rant

- The Good ole' days are gone
- Hack because you should, not just because you are getting paid
- Someone hire me dammit!
- Community needs to talk to each other more
- Companies need to allow more interaction among developers

New Site!

- Moving away from 'Evil' look
- Extolling the virtues of a high SNR
- Easier to navigate
- Easier to maintain
- Easier to link too!
- Non-denominational, equally offensive to all

The CoWF Confessional

- Concept - people to reveal their wireless sins/errors so that other can learn from it
- "Security has to be right every time, but the bad guys only have to be right once“
- We're all human, we all screw up
- CORE USB pwnage
- Share your sins
- Let others learn from your screw ups

The CoWF Confessional

- Anonymous, scrubbed, safe
- Moderated for anonymity
- <EMAIL ADDRESS> at later date

Bluetooth

- Wi-Fi is not the only wireless
- So many BT peripherals
- So many hardware hacks
- So disappointed….

Bluetooth

- There is the Bluetooth Glove

Bluetooth

- The Bluetooth Bananna

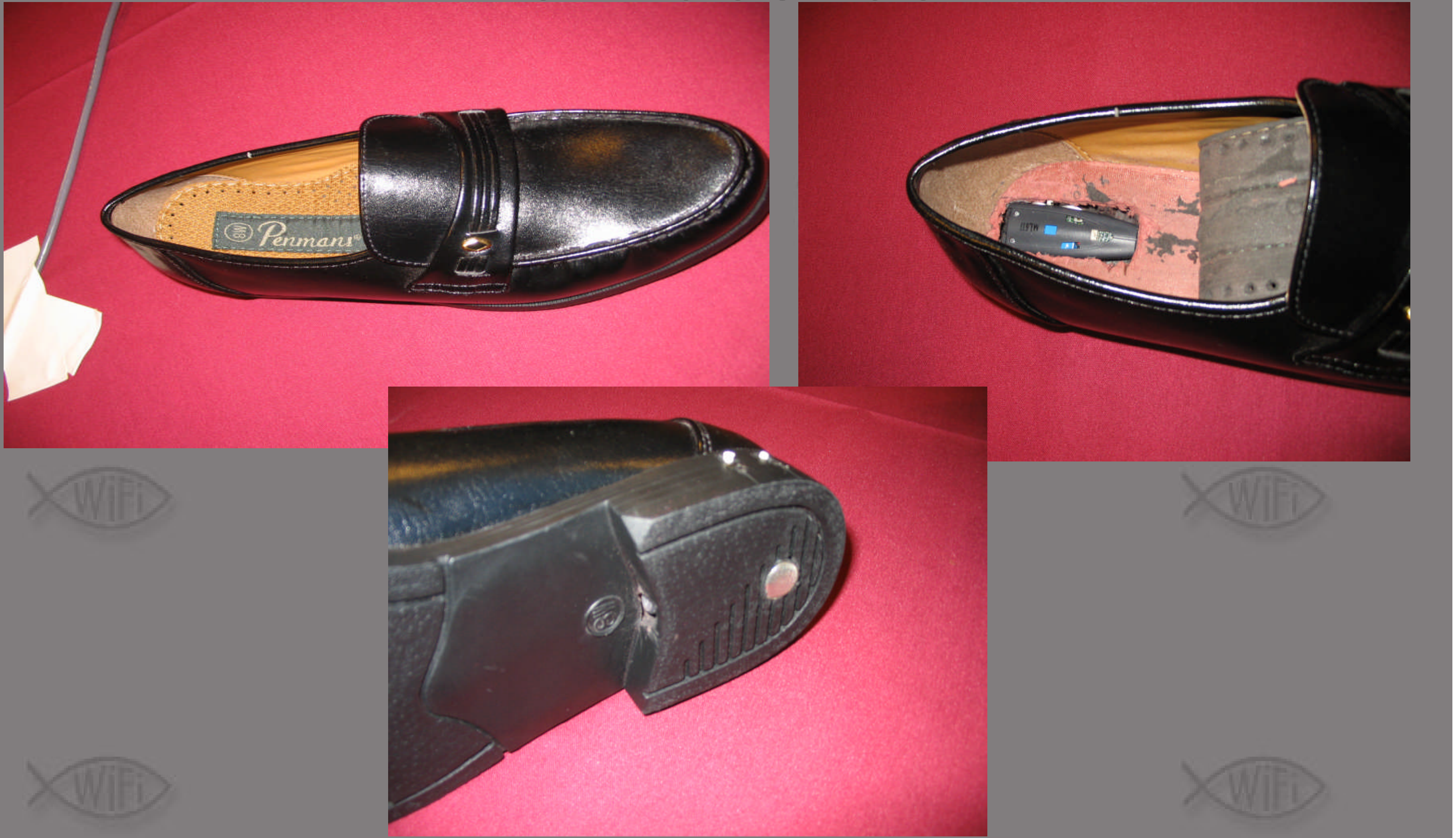
Bluetooth

- And the Bluetooth Brick Phone

Bluetooth

Excuse me, I have a call.....

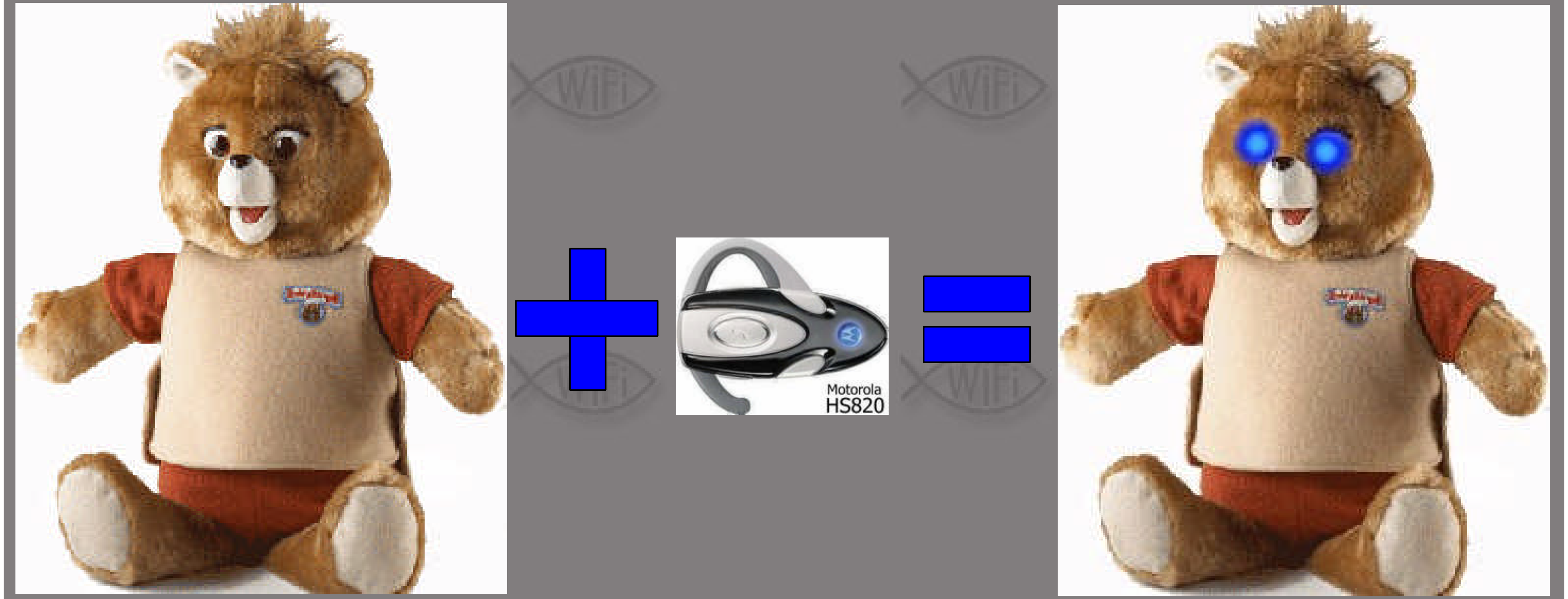
The Blueshoe



The Blueshoe

- BT Headset + Shoe = Agent 86 for real!

Next?



Larger Bluetooth Issues

- Every BT headset is a listening device
- Board rooms, offices, homes, etc
- Easily blend in RF traffic
- Can't search for rogues!
- Can't monitor for bad traffic!

Larger Bluetooth Issues

- Lack of tools for full research, mayhem
- Btcrack Needs BT protocol analyzer -$$$$$
- No “monitor mode” for BT – This sucks
- Need to light a fire under the community
- Has been tried before but we’re better

Bluetooth Protocol Analyzer

- Cost >$10,000
- Render's a cheap and poor
- GNU Radio? - $$$$
- No cheap RAW devices
- No OSS software available
- What's a hacker to do?

Bluetooth Protocol Analyzer

- Busting the Bluetooth – Max Moser
- **http://www.remote-exploit.org/research/busting_bluetooth_myth.pdf**
- Cheap CSR based adapters, re-flashed to support RAW with un-named companies firmware
- Slightly illegal (OK, lots)
- Google “Bluetooth Sniffing For Less” for more
- Not good for 'legit research‘
- Thanks to the EFF for keeping me out of Jail here

Bluetooth Protocol Analyzer

- What do we need?
- Need an OSS application suite for RAW interface sniffing
- Need a cheap RAW device - New Firmware for CSR based adapters
- It can be done! We have code! (Can’t show here though)
- Several individuals have made progress

Example, EFF declined

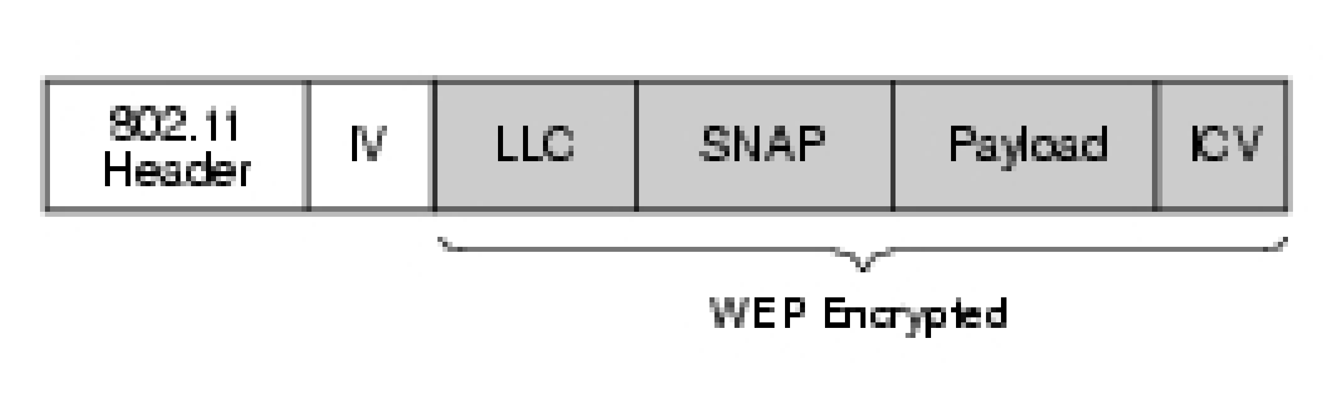
- I'm a foreign national who wants to go home after this
- http://darkircop.org/bt/ - Mail list
- Andrea Bittau, Dominic Spill and many others
- We can already sniff pair keys!
- See the wireless village for some more specifics

WIFI Mischief

- What you've probably been waiting for
- WEP is not dead for research
- Attack the attack tools?
- Michael and the IEEE saga continues…

Flinging mud at WEP cracking

- Aircrack-ptw - Final nail in the coffin?
- Throw some mud into the mix!
- Aircrack - No validation of IV traffic
- Replay during the replay…



802.11 Header	IV	LLC	SNAP	Payload	ICV

WEP Encrypted

Flinging mud at WEP cracking

- Send spoofed frames with random IV's at random intervals
- Aircrack can't tell the difference, Statistical analysis goes WTF?
- Stopgap for legacy apps
- Research duplicated 3 times!
- Airdefense **MAY** have a patent. Airtight presenting more on saturday?
- Free WPA Tables to the first person to present working version this weekend!

Michael can bite me!

- 802.11i spec has a DoS built in (MIC countermeasures)
- Ranted a lot in the last year
- Put my foot in my mouth at DC14
- Turned into a Shmoocon talk
- Drinking on stage with the Chair of the IETF
- Still not seen as a major problem….

Michael can bite me!

- Legacy hardware = Design concessions
- MIC = Per Packet CRC of payload
- 2^29 bits of security – Brute forceable
- 2 bad packets/min = Rekey
- Radio turns off for 60 seconds!
- Prevents replay attacks
- Sequence enforcement
- MIC is encrypted with payload
- MIC checked after several other checks

Michael can bite me!

- Google and NIST were great help
- Rumors, hushed discussion, 'feelings'
- One lonely NIST PDF
- “Decryption/integrity check fail if traffic class bits are altered”

Michael can bite me!

- QoS breaks sequence enforcement
- Wireless MultiMedia Specifications
- Solved with seperate counters for each QoS level
- MIC extends over WMM (QoS) header, but header not part of encrypted portion…
- QoS flags can be modified and packet will still be decrypted….
- So……

Michael can bite me!

- Capture high priority data packet
- Set to low priority, retransmit
- Send to other queues
- Packet adheres to sequence enforcement….
- Packet decrypts successfully….
- MIC fails (WMM bits changed)
- MIC countermeasures counter increments
- **2 packets = AP KICKS USERS, TURNS OFF RADIO FOR 60 sec FOR REKEY!**

Michael can bite me!

- 802.11i spec section 8.3.2.4.2, paragraph C
- *"If a non-AP STA receives a deauthenticate frame with the reason code "MIC failure," it cannot be certain that the frame has not been forged, as it does not contain a MIC. The STA may attempt association with this, or another, AP. If the frame was genuine, then it is probable that attempts to associate with the same AP requesting the use of TKIP will fail because the AP will be conducting countermeasures."*

Michael can bite me!

- Clients can't verify the Michael countermeasure deauth is legit..
- Clients keep trying to associate to AP
- Begin the client attacks!
- Karma, etc can fill in

Micheal can bite me!

- Not any real defense, it's built into the standard
- Does require WMM client
- IEEE/IETF do good work
- Need to step up development cycle
- Free WPA tables to first person to present working exploit this weekend!

Conclusion

- Visit the Wireless Village!
- Contribute projects!
- Ask questions about our current projects!
- Donate!
- Learn + Touch = DO!
- Share the knowledge!
- Keep on hacking the air!
- Give Render & theprez98 jobs!