

# HIPPA Violated by Wireless Access Points

---

Paper: ISP113

Authors:  
Jonathan Scott Leigh  
and  
Dr. Ray Vaughn

# Summary

---

- What is HIPPA?
- The experiment plan
- Equipment used
- Execution of the experiment
- Analysis of the results
- How HIPPA is violated
- Danger of these results



# HIPPA – The Health Insurance Portability and Accountability Act

---

- Five Security Standards
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
  - Organizational requirements
  - Policies, procedures, and documentation requirements

# The Experiment Plan

---

- Find medical facilities around Mississippi that are in drivable distance
- Go war driving around the places where these facilities are located and sniff for any packets being broadcast
- Use a GPS to correlate the access points found in these locations to the buildings the wireless signals are coming from, and plot the access points in google earth

# Equipment used

---

- A number of both hardware and software devices were used for this experiment...



# IBM Thinkpad T40

- \$300.00



# Ubiquiti SRC Wireless PCMCIA Card with Antenna

---

- \$100.00



# Garmin Etrex Hand Held GPS with Cable

- \$80.00

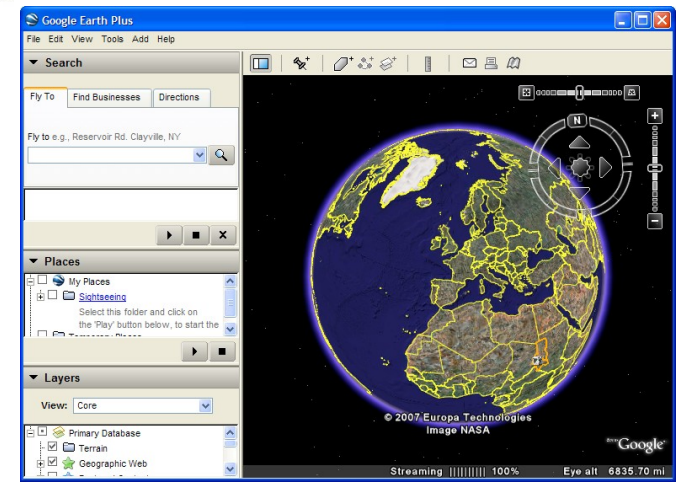
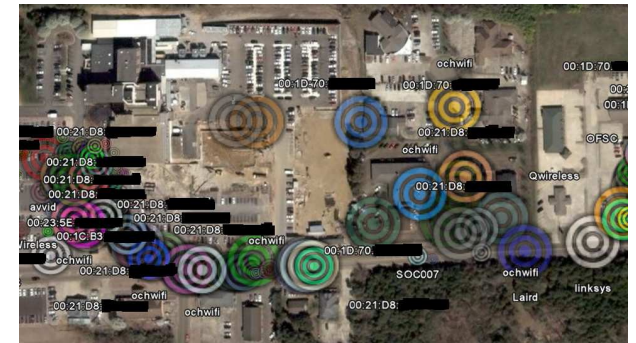


# Software

- \$0.00
- Kismet
- gpsd
- Kisgerath
- Google Earth
- Wireshark
- Ubuntu

```
Network List (Autofit)
Name      T W Ch  Packets  Flags  IP Range  Size
-----
I exceed  A N 001 1145  A4  10.3.1.13  72K
I TeletexNET  A N 001 1074  A4  10.10.100.47  65K
+ Probe networks
  gnet     A Y 011 61  0.0.0.0  00
+ Ad-hoc networks
  WDC      A Y 006 91  0.0.0.0  00
  WDC      A Y 006 91  0.0.0.0  00
+ <Data networks>
  TRB      A Y 006 12  0.0.0.0  00
  WEST6697 A Y 006 2  0.0.0.0  00
  2WIRE424 A Y 006 19  0.0.0.0  00
  2WIRE250 A Y 006 30  0.0.0.0  00
  Linksys  A N 000 4 F 102.100.1.1  00
  Con      A N 006 25  0.0.0.0  00
  Moto     A Y 006 1  0.0.0.0  00
  Motorola62 A Y 006 1  0.0.0.0  00
  HUNTER   A Y 006 1  0.0.0.0  00
  ALans's  A Y 006 1  0.0.0.0  00
  0033     A Y 006 1  0.0.0.0  00
  George   A O 006 1  0.0.0.0  00
  dmiller5206 A Y 006 1  0.0.0.0  00
  Motorola A N 001 2  0.0.0.0  00
  Linksys-g A N 006 107  0.0.0.0  1248
  Alice1   A Y 006 2  0.0.0.0  00
  HealthColumbus A N 006 1  0.0.0.0  00
  kno ssid- A O --- 1  0.0.0.0  650
  Linksys  A N 006 1  0.0.0.0  00
  GIGI     A Y 006 7  0.0.0.0  00
  kno ssid- A Y 002 5  0.0.0.0  00
  witty    A O 006 5  0.0.0.0  00

Status
Found new network "GIGI" bssid 00:14:A5  Crypt Y Ch 6 @ 11.00 mbit
Found new network "witty" bssid 00:1C:102  Crypt Y Ch 6 @ 54.00 mbit
Found new network "kno ssid" bssid 00:40:985  Crypt Y Ch 2 @ 11.00 mbit
Associated probe network "00:13:C4C" with "00:0A:0B:" via data.
Battery: 33% 0h30m50s
```



# Laptop Car Charger

- \$20.00



Powered by DIYTrade.com



MISSISSIPPI STATE  
UNIVERSITY™

# Piece-o-junk Corolla

- \$400.00



# Execution of the experiment

---

- I started up Kismet, gpsd, and Wireshark
- Then I drove up and down streets where the medical facilities were located



Network List (Autofit)

Name	T	W	Ch	Pkts	Flags	IP Range	Size
! exceed	A	N	001	1145	A4	10.3.1.13	73k
! TeletecNET	A	N	001	1074	A4	10.10.100.47	65k
+ Probe networks	G	N	---	6097		0.0.0.0	0B
gastro	A	Y	011	61		0.0.0.0	0B
+ Adhoc networks	G	N	---	190		0.0.0.0	0B
WBDC	A	Y	006	91		0.0.0.0	0B
+ <Data networks>	G	N	---	57		0.0.0.0	1k
TR6	A	Y	006	12		0.0.0.0	0B
WEST6697	A	Y	006	2		0.0.0.0	0B
2WIRE424	A	Y	006	19		0.0.0.0	0B
2WIRE250	A	Y	006	30		0.0.0.0	0B
Linksys	A	N	006	4	F	192.168.1.1	0B
Con	A	N	006	25		0.0.0.0	0B
Moto	A	Y	006	1		0.0.0.0	0B
Motorola62	A	Y	006	1		0.0.0.0	0B
HUNTER	A	Y	006	1		0.0.0.0	0B
Alans's	A	Y	006	1		0.0.0.0	0B
0613	A	Y	006	1		0.0.0.0	0B
George	A	O	006	1		0.0.0.0	0B
dmiller5206	A	Y	006	1		0.0.0.0	0B
Motorola	A	N	001	2		0.0.0.0	0B
! linksys-g	A	N	006	107		0.0.0.0	124B
Alicel	A	Y	006	2		0.0.0.0	0B
HemOncColumbus	A	N	006	1		0.0.0.0	0B
<no ssid>	A	O	---	1		0.0.0.0	65B
linksys	A	N	006	1		0.0.0.0	0B
GiGi	A	Y	006	7		0.0.0.0	0B
<no ssid>	A	Y	002	5		0.0.0.0	0B
witty	A	O	006	5		0.0.0.0	0B

Info

Ntwrks 104  
 Pkts 9870  
 Cryptd 88  
 Weak 0  
 Noise 5  
 Discrd 5  
 Pkts/s 44  
 madwif  
 Ch: 11  
 Elapsd 00:02:51

Status

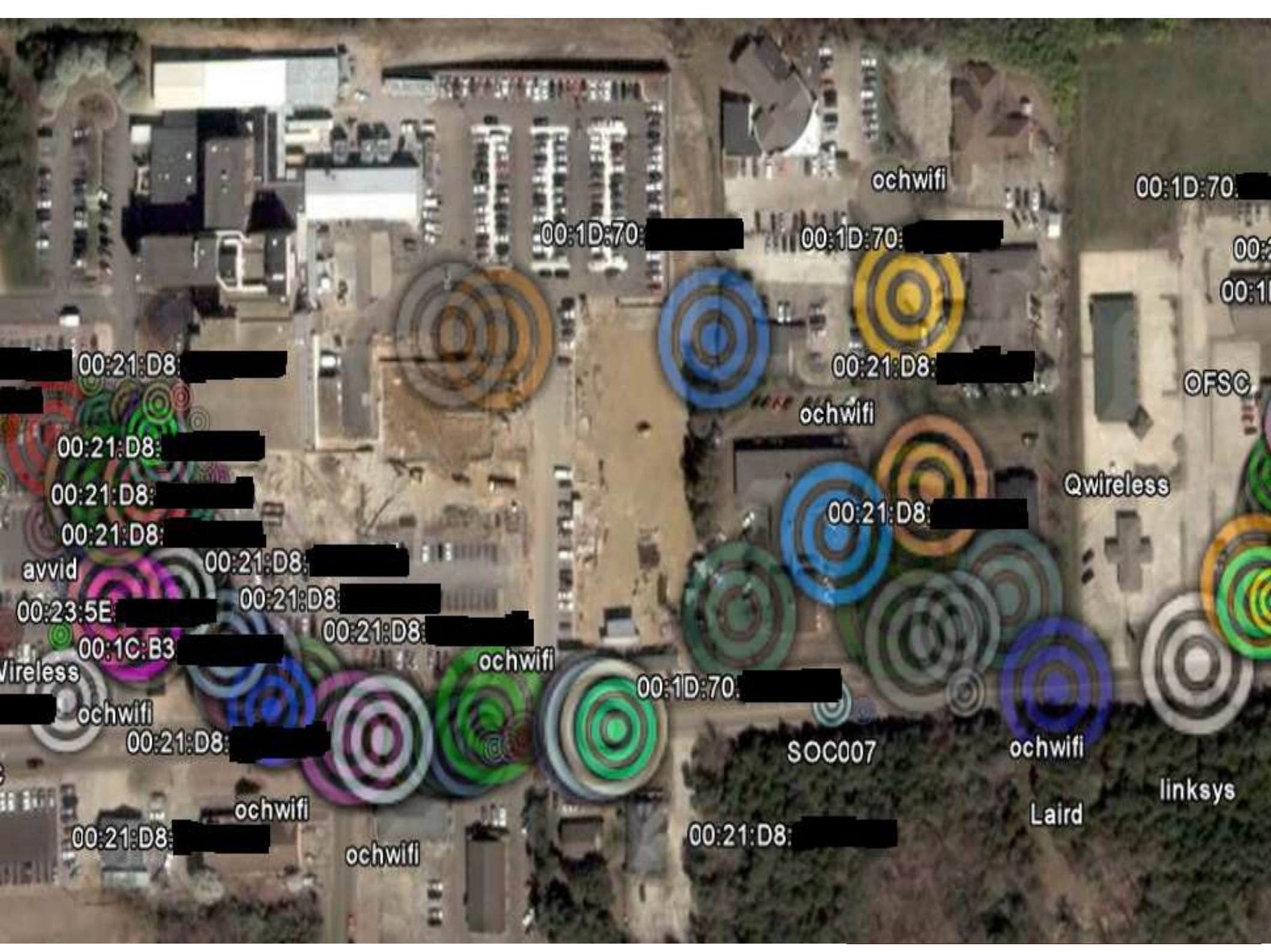
Found new network "GiGi" bssid 00:14:A5: [redacted] Crypt Y Ch 6 @ 11.00 mbit  
 Found new network "witty" bssid 00:1C:10: [redacted] Crypt Y Ch 6 @ 54.00 mbit  
 Found new network "<no ssid>" bssid 00:40:96: [redacted] Crypt Y Ch 2 @ 11.00 mbit  
 Associated probe network "00:13:CE: [redacted]" with "00:0A:DB: [redacted]" via data.

Battery: 33% 0h38m50s

# Analysis of the results

---

- Used kismet to convert GPS data points to a google earth KML file
- Looked at the GPS points in google earth to see if the wireless access points were in the correct area that gpsd recorded them in
- Loaded some of the wireless data up into wireshark to see if there were any interesting packets
- Used the linux command "grep" to parse the kismet logs and generate statistics of hackable wireless access points



ochwifi

00:1D:70: [REDACTED]

00:1D:70: [REDACTED]

00:1D:70: [REDACTED]

00: [REDACTED]  
00:1 [REDACTED]

00:21:D8: [REDACTED]

00:21:D8: [REDACTED]

OFSC

00:21:D8: [REDACTED]

ochwifi

Qwireless

00:21:D8: [REDACTED]

00:21:D8: [REDACTED]

00:21:D8: [REDACTED]

avvid 00:21:D8: [REDACTED]

00:23:5E [REDACTED] 00:21:D8: [REDACTED]

00:1C:B3 [REDACTED] 00:21:D8: [REDACTED]

Wireless

ochwifi

00:1D:70: [REDACTED]

ochwifi

SOC007

ochwifi

00:21:D8: [REDACTED]

linksys

ochwifi

Laird

00:21:D8: [REDACTED]

00:21:D8: [REDACTED]

ochwifi



**OFSC**

---

**Number:** 2  
**SSID:** OFSC  
**BSSID:** 00:12:17 [REDACTED]  
**Channel:** 6  
**Encrypted:** false  
**Carrier:** IEEE 802.11g  
**Cloaked:** false  
**Datasize:** 0  
**Maxseenrate:** 6000  
**Firsttime:** Thu Apr 2 19:46:20 2009  
**Lasttime:** Thu Apr 2 19:54:52 2009  
**Type:** infrastructure  
**Maxrate:** 54.0  
**Have Clients:** true

---

Generated with KisGearth 0.01f  
Website: <http://mytv.org/kisgearth/>  
Directions: To here From

Image © 2009 DigitalGlobe  
© 2009 Tele Atlas

N [REDACTED] W elev 342 ft

File Edit View Go Capture Analyze Statistics Help



Filter: http &amp;&amp; http.request

+ Expression...

Clear

Apply

No.	Time	Source	Destination	Protocol	Info
9918	154.759071	[REDACTED]	66.114.51.21	HTTP	GET /i/w/logo.gif HTTP/1.1
9925	154.783471	[REDACTED]	66.114.51.21	HTTP	GET /graphics/ical.gif HTTP/1.1
9932	154.794254	[REDACTED]	66.114.51.21	HTTP	GET /graphics/rss/rssmini.gif HTTP/1.1
9934	154.795483	[REDACTED]	66.114.51.21	HTTP	GET /graphics/smash/blue_warning.gif HTTP/1.1
9937	154.802697	[REDACTED]	74.126.6.130	HTTP	GET /xmlrequest.html HTTP/1.1
9952	154.829573	[REDACTED]	66.114.51.21	HTTP	GET /graphics/wu2/headerBlue-right.gif HTTP/1.1
9955	154.833224	[REDACTED]	66.114.51.21	HTTP	GET /graphics/wu2/subBlue-left.gif HTTP/1.1
9957	154.835579	[REDACTED]	66.114.51.21	HTTP	GET /i/c/a/nt_tstorms.gif HTTP/1.1
9962	154.852357	[REDACTED]	66.114.51.21	HTTP	GET /graphics/wu2/subBlue-right.gif HTTP/1.1
9963	154.853855	[REDACTED]	66.114.51.21	HTTP	[TCP Out-Of-Order] GET /graphics/wu2/subBlue-right.g
9964	154.854698	[REDACTED]	66.114.51.21	HTTP	[TCP ACKed lost segment] GET /graphics/360arrows_blu
9970	154.865589	[REDACTED]	66.114.51.21	HTTP	GET /graphics/wu2/headerBlue-left.gif HTTP/1.1
9991	154.897853	[REDACTED]	66.114.51.21	HTTP	GET /graphics/smash/blue_localRadar.gif HTTP/1.1

```

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.7) Gecko/20080213 Firefox/3.0.7
Accept: image/png,image/*;q=0.8,*/*;q=0.5\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
Referer: http://www.wunderground.com/cgi-bin/findweather/getForecast?query=39759&MR=1\r\n
If-Modified-Since: Wed, 16 Apr 2008 21:27:35 GMT\r\n
Cache-Control: max-age=0\r\n
\r\n

```

```

p-alive. .Referer
: http://www.wun
derground.com/cg
i-bin/fi ndweathe

```

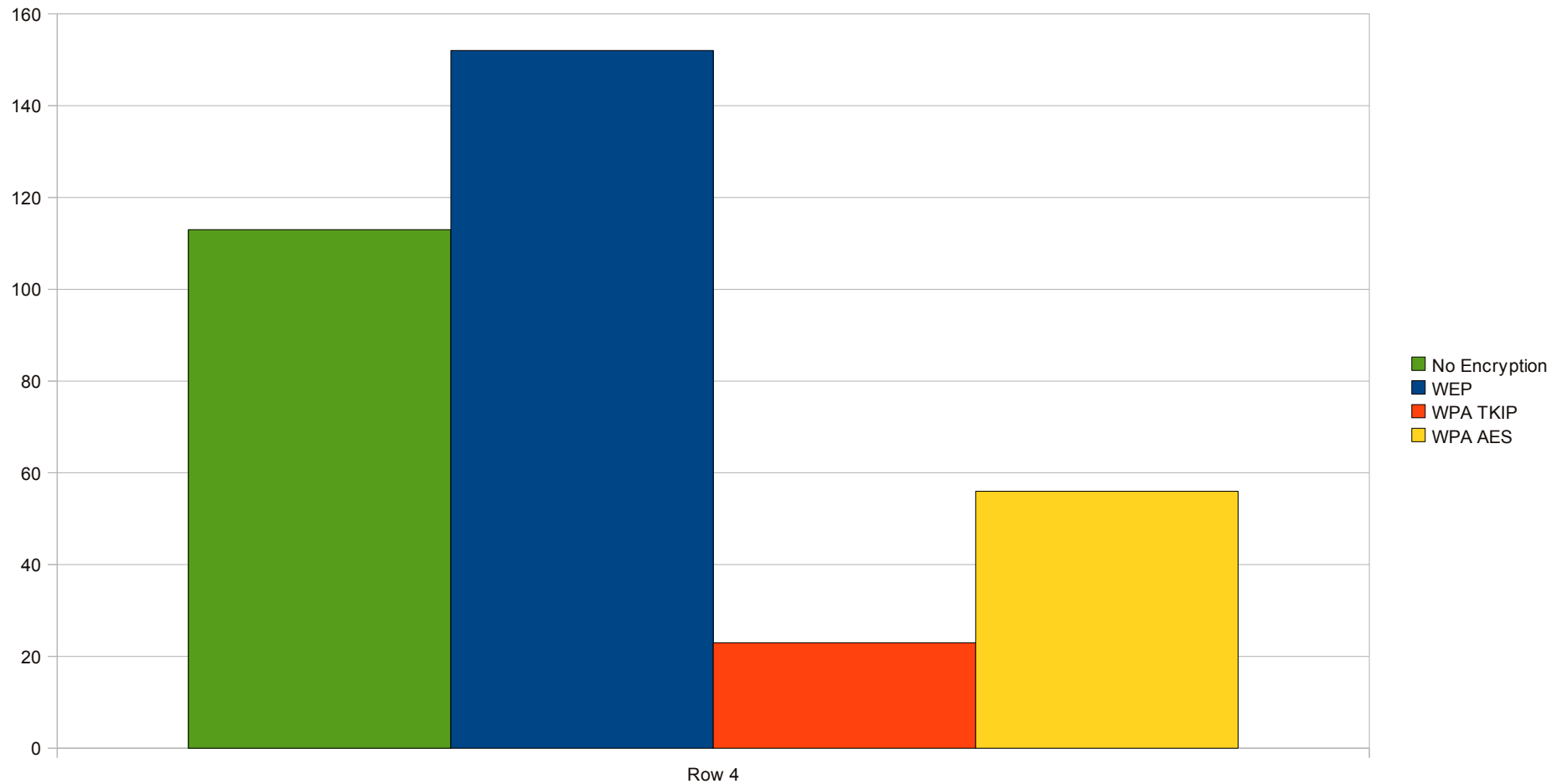
Network 7: "gastro" BSSID: "00:17:5A [REDACTED]"

Type : infrastructure  
Carrier : 802.11g  
Info : "gastro\000\000\000\000\000\000\000\000\000\000\010\0"  
Channel : 11  
Encryption : "WEP "  
Maxrate : 18.0  
LLC : 101  
Data : 6  
Crypt : 6  
Weak : 0  
Dupe IV : 0  
Total : 107  
First : "Thu Mar 5 14:21:51 2009"  
Last : "Thu Mar 5 14:22:31 2009"  
Min Loc: Lat 90.000000 Lon 180.000000 Alt 0.000000 Spd 0.000000  
Max Loc: Lat -90.000000 Lon -180.000000 Alt 0.000000 Spd 0.000000

Network 8: "<no ssid>" BSSID: "00:13:10: [REDACTED]"

Type : infrastructure  
Carrier : 802.11g  
Info : "None"  
Channel : 11  
Encryption : "None"  
Maxrate : 11.0  
LLC : 6  
Data : 1  
Crypt : 0  
Weak : 0  
Dupe IV : 0  
Total : 7  
First : "Thu Mar 5 14:21:51 2009"  
Last : "Thu Mar 5 14:22:19 2009"  
Min Loc: Lat 90.000000 Lon 180.000000 Alt 0.000000 Spd 0.000000  
Max Loc: Lat -90.000000 Lon -180.000000 Alt 0.000000 Spd 0.000000

# Encryption of Wireless Access Points



# How HIPPA is Violated

---

- Under one of the five security standards enacted by HIPPA one of them states that health care providers must "Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of"
  - This includes encrypting electronic health information over the wire for these wireless access points which 113 don't do at all
-

# Danger of these results

---

- Even if you buy into the lie that just because you're behind a firewall you are safe, most of these wireless access points act as the firewall and once broken into are bypassed
- WEP access points are easily defeated
- WPA TKIP can be cracked

# Danger of these results continued

---

- Peoples social security numbers and personal medical records (such as what medicines they are allergic to) are constantly going across the wire
- Medical equipment is starting to get hooked up to the network



# Hacker Tools

---

- SpoonWEP/SpoonWPA – It's as easy as making soup! Crack WEP keys in about 5 minutes!
- Metasploit – Hundreds of exploits, automated hacking of exploitable machines
- Crypters – You think virus scanners will save you? They won't. Hackers have tools to encrypt their software so that most anti-virus programs will not recognize them anymore.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHE
00:1A:73:E8:D4:46	-73	2	0 0	3	54	WEP	WEP
00:23:69:BB:2D:0F	-35	5	1 0	3	54	WEP	WEP

**SpoonWep / Wep Finder / SV 2K8**

**Victim Mac**

**ClientLess Attack**   **Client**

**NET CARD**   **Ath**

**Channel**

1 3 5 7 9 11 13

**Inj Rate**

200 400 600 800 1000

**ABORT**

**Deauth**

**Currently : CRACKING WEP** **Captured : 10520 IVS**

**WEP Key : Not Found**

CCMP  
WEP  
WEP  
CCMP  
WEP  
TKIP  
ets  
1  
11  
2  
2  
2

# Metasploits db autopwn feature

```
Fast-Track Metasploit Autopwn Automated
[*] 10.10.10.10:80 exploit/windows/http/belkin_bulldog
(port match)
[*] 10.10.10.10:21 exploit/windows/ftp/sasser_ftpd_port
(port match)
[*] 10.10.10.10:80 exploit/unix/webapp/tikiwiki_graph_formula_exec
(port match)
[*] 10.10.10.10:80 exploit/windows/vnc/winvnc_http_get
(port match)
[*] 10.10.10.10:80 exploit/unix/webapp/tikiwiki_jhot_exec
(port match)
[*] 10.10.10.10:80 exploit/windows/isapi/nsislog_post
(port match)
[*] 10.10.10.10:80 exploit/windows/http/intersystems_cache
(port match)
[*] 10.10.10.10:80 exploit/windows/http/hp_power_manager_login
(port match)
[*] 10.10.10.10:80 exploit/windows/http/xitami_if_mod_since
(port match)
[*] 10.10.10.10:80 exploit/windows/http/sapdb_webtools
(port match)
```

> Fast-Track Main  
> Fast-Track Updates

Fast-Track Loading Page

Scripts Currently Forbidden | <SCRIPT>: 3 | <OBJECT>: 0

Done

root@bt Fast-Track Fast-Track 1 2 11:51

# Contact Information & Questions

---

- Email: [Dantevios@gmail.com](mailto:Dantevios@gmail.com)
- Website: <http://www.Dantevios.com> (Will put slides here)
- Twitter: <http://www.twitter.com/Dantevios>
- Facebook: <http://www.facebook.com/Dantevios>
- AIM: Dantevios
- MSN: [Dantevios@hotmail.com](mailto:Dantevios@hotmail.com)
- Yahoo: [Dantevios@yahoo.com](mailto:Dantevios@yahoo.com)
- Skype: Dantevios
- Skype #: 662 – 524 – 3653