How Secure is Wireless?

South Carolina Chapter of HIMSS
Annual Conference
April 24-25, 2003

Richard Gadsden
Director of Computer and Network Security
Medical University of South Carolina
gadsden@musc.edu

Overview

- Wireless concepts
- Brief history of wireless networking
- Vulnerabilities and threats
- Risk management
- Defense in depth
- Conclusions

Why Do Wireless?

- Demands for mobility
  - Physicians, nurses, other care providers
  - Patients
- Desire to avoid cabling expense
- Evolution towards 'ubiquitous' computing

Brief History

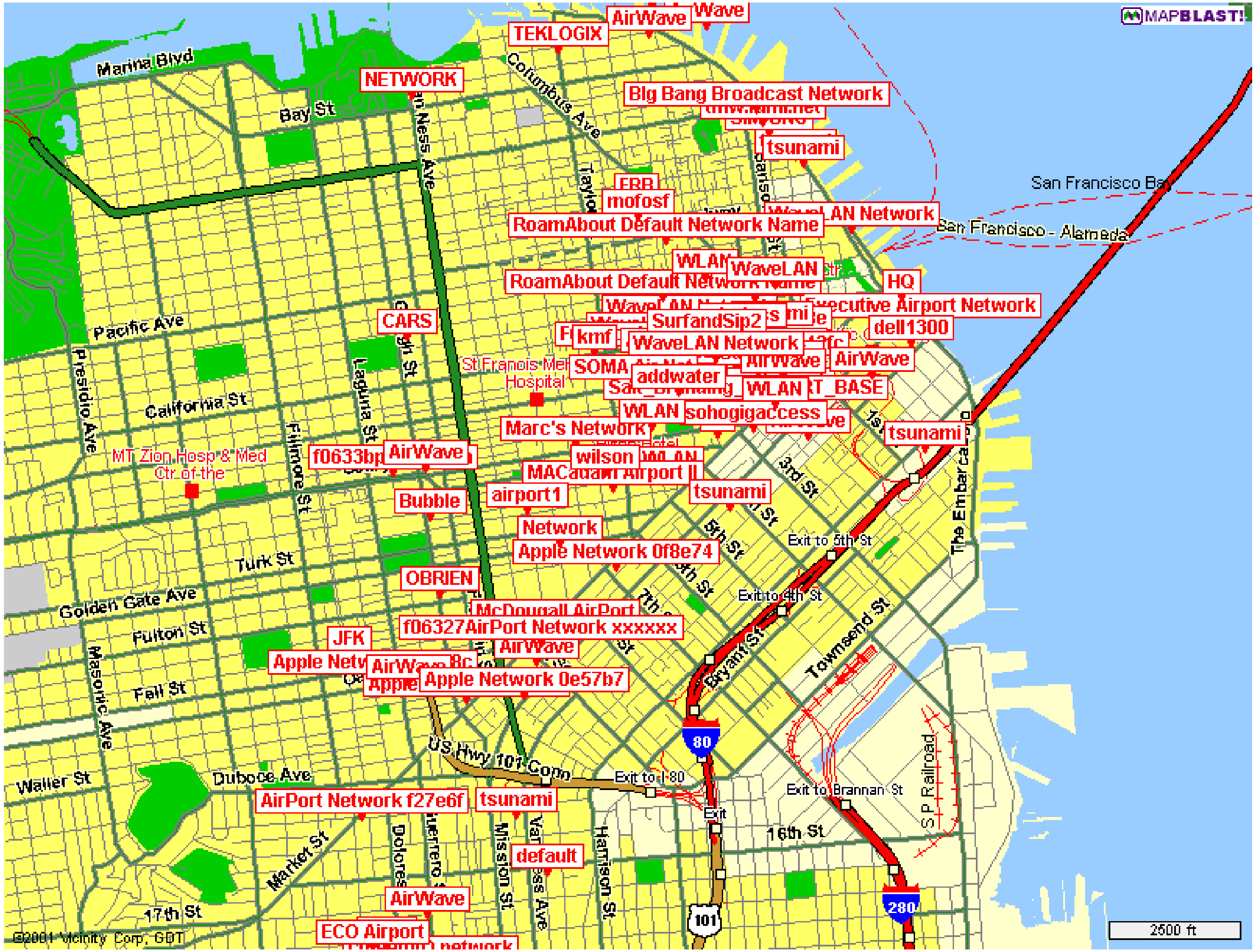
- 1997
  - IEEE 802.11 (2.4GHz, 1-2Mb/s)
- 1999
  - IEEE 802.11b (2.4GHz, 11Mb/s)
- 2000-present: rapid growth
  - 2002 market est $2B
  - 2006 market projected at $5B

History (cont'd)

- Security awareness
  - April 2001, Peter Shipley 'WarDriving' (WSJ)
  - May 2002, "Best Buy closes wireless registers" (MSNBC)
  - Sep 2002, "Heard of drive-by hacking? Meet drive-by spamming" (ZDNet)

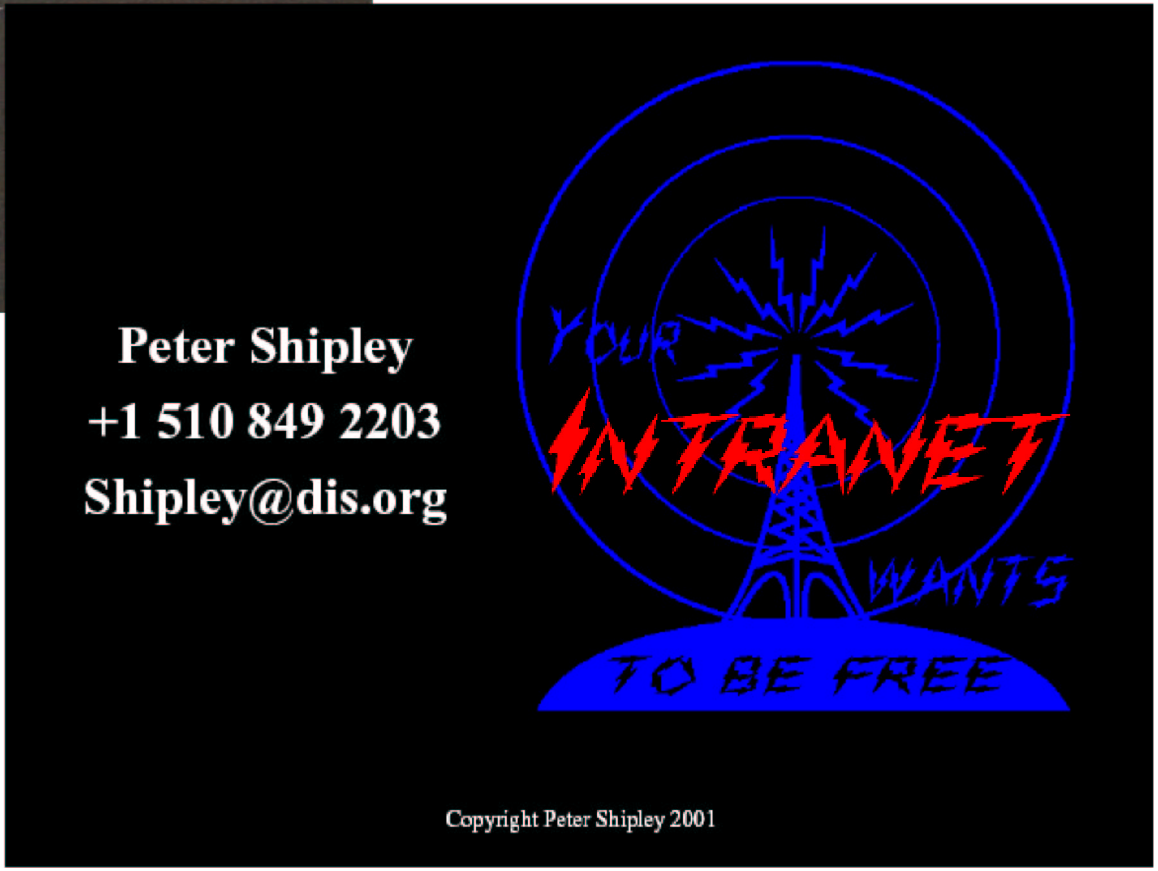
WarDriving

http:/www.dis.org/wl/maps



Peter Shipley

Father of WarDriving?



Peter Shipley
+1 510 849 2203
Shipley@dis.org

YOUR
INTRANET
WANTS
TO BE FREE

Copyright Peter Shipley 2001

History (cont'd)

- 2003
  - Higher speeds
    - IEEE 802.11a (5GHz, 54Mb/s)
    - IEEE 802.11g (2.4GHz, 54Mb/s, b/c 802.11b)
  - New security standard expected
    - IEEE 802.11i

802.11 Topologies

- Independent Basic Service Set (IBSS)
  - Peer-to-peer wireless network
- Basic Service Set (BSS)
  - Access Point (AP), one or more associated nodes
- Extended Service Set (ESS)
  - Multiple cooperating APs
- Modes: Ad-Hoc, Infrastructure

Why NOT Do Wireless?

- Limited, shared network bandwidth per AP
- Limited RF spectrum (FCC rules)
- Limited signal strength (interference likely)
- Immature standards and technology
  - Rapid obsolescence
- *Many* security issues
  - All the risks of wired networks, plus more

Vulnerabilities and Threats

- WLANs are *designed* to broadcast traffic
  - Radio waves want to be free
- Unauthorized users
- Unauthorized disclosure or modification
- Denial of service
- *Tools are readily available to receive, modify, and disrupt wireless network traffic*

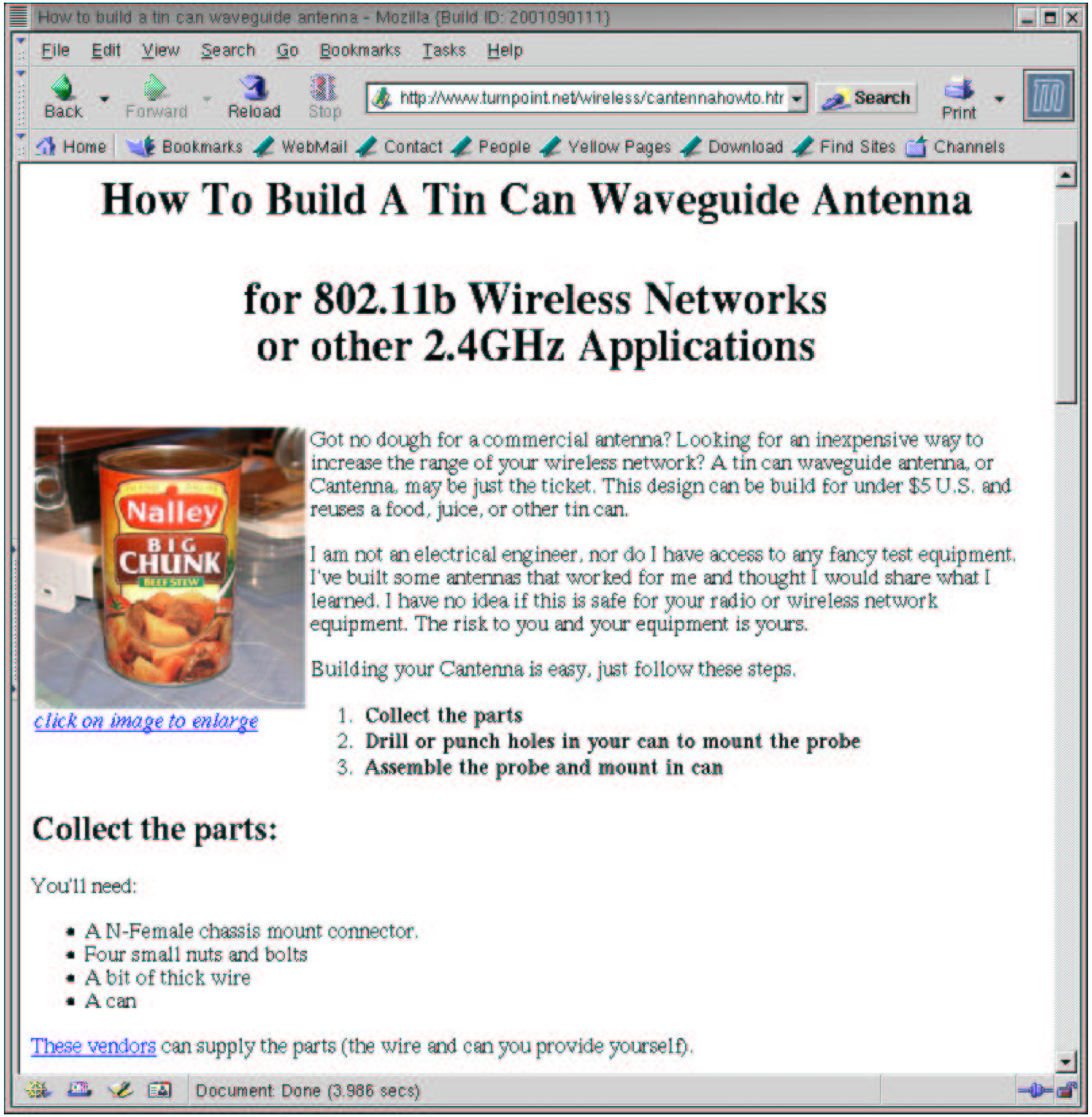
Wireless Hacking Tools

- Hardware
  - Laptop or handheld with wireless NIC
- Software (freely available)
- Antenna(s)
  - To eliminate the need for physical trespass
- Transportation (optional)
- GPS (optional)

Wireless Hacking Software

- Network discovery
  - AirMagnet (commercial, Windows)
  - NetStumbler (free, Windows)
  - Kismet, Wellenreiter (open source, Linux)
- Cracking WEP encryption keys
  - AirSnort (open source, Linux)

http://www.turnpoint.net/wireless/cantennahowto.html


How to build a tin can waveguide antenna - Mozilla {Build ID: 2001090111}
File Edit View Search Go Bookmarks Tasks Help
Back
Forward
Reload
Stop
http://www.turnpoint.net/wireless/cantennahowto.htr
Search
Print
Home
Bookmarks
WebMail
Contact
People
Yellow Pages
Download
Find Sites
Channels
Nalley
BIG CHUNK
BEEF STEW
Document: Done (3.986 secs)

How To Build A Tin Can Waveguide Antenna

for 802.11b Wireless Networks or other 2.4GHz Applications

click on image to enlarge

Got no dough for a commercial antenna? Looking for an inexpensive way to increase the range of your wireless network? A tin can waveguide antenna, or Cantenna, may be just the ticket. This design can be build for under $5 U.S. and reuses a food, juice, or other tin can.

I am not an electrical engineer, nor do I have access to any fancy test equipment. I've built some antennas that worked for me and thought I would share what I learned. I have no idea if this is safe for your radio or wireless network equipment. The risk to you and your equipment is yours.

Building your Cantenna is easy, just follow these steps.

1. **Collect the parts**
2. **Drill or punch holes in your can to mount the probe**
3. **Assemble the probe and mount in can**

Collect the parts:

You'll need:

- A N-Female chassis mount connector.
- Four small nuts and bolts
- A bit of thick wire
- A can

These vendors can supply the parts (the wire and can you provide yourself).

Security Controls: Bare Essentials

- Access control (user authentication)
  - Prevent unauthorized users
- Encryption
  - Protect confidentiality and integrity
- Monitoring and auditing
  - Prevention, detection

Wired Equivalent Privacy (WEP)

- 802.11, intended to provide authentication and encryption
- Developed during the dark years of US govt export controls on crypto (aka "munitions")
- Seriously flawed
  - Key distribution left as an exercise for the reader
  - Fundamental flaws in cryptographic design (revealed in a series of papers in 2000-2001)

WEP cont'd

- Aug 2001: WEP is toast
- AirSnort, WEPCrack
- WEP today
  - Equivalent to 'No Trespassing Please' sign
  - At least prevents accidental trespass
- Default configuration?

802.11 Access Control... Not

- Two options in 802.11 standard
  - Open authentication
  - Shared key authentication (WEP)
- Additional (non-standard) options
  - Closed authentication (Lucent and others)
  - ACLs (lists of allowed client MAC addresses)
- All can be easily defeated
- Default configuration?

Impact of 802.11 Flaws

- You cannot control access to your WLAN
  - Any attacker can associate his wireless device with your APs
  - Shared network (like hub) means he can eavesdrop on any other wireless user's traffic
- Your WEP encryption keys can be cracked
  - Attacker can eavesdrop on encrypted traffic
  - Attacker can modify encrypted traffic
- Attacks are undetectable and untraceable

Fixing 802.11

- IEEE 802.11i (expected late 2003)
  - Clients must authenticate prior to L2 association
  - Leverages 802.1x port-level authentication
  - Extensible Authentication Protocol (EAP)
  - RADIUS is the usual back-end authN service
  - Temporal Key Integrity Protocol (TKIP)
  - WEP/TKIP allowed for backward compatibility
  - AES encryption to replace WEP going forward

Fixing 802.11 (cont'd)

- Wi-Fi Alliance
- Wi-Fi Protected Access (WPA)
  - Encryption: WEP/TKIP
  - Authentication: 802.1x/EAP
- WPA being promoted as an interim 'standard'

EAP Soup

- Flavors so far...
  - EAP-MD5, LEAP, EAP-TLS, EAP-TTLS, PEAP
- Flavors du jour...
  - EAP-TTLS, PEAP
- IEEE and IETF
  - Will flavor wars be resolved in 802.11i?
  - Will all known protocol flaws be addressed?
    - especially Compound Authentication Binding problem

Mobile Device Vulnerabilities

- Portable devices easily lost, stolen
  - Encryption of stored data is dodgy
  - User passwords are too often 'remembered'
- OS issues
  - Inherently insecure (PalmOS)
  - Impossible to configure securely (Windows)
- Temptation to store PHI is overwhelming

Other Vulnerabilities

- Vendor implementation decisions
  - Stupid SNMP tricks
  - Insecure AP management interfaces
- Fault tolerance (availability)
  - Wireless sessions easily disrupted
  - Roaming between APs is not standardized

Risks

- Wireless networking of portable, mobile devices is inherently risky
- Will always be more risky than wired networking of non-portable devices
- Are the risks manageable today?

Risk Management

1. Assess risks
2. Develop policies
   - Must address wireless security as an extension of enterprise security
3. Implement procedures and controls
4. Education and awareness
   - Users must follow policies and procedures

Security Policies

- Explain what needs protection and why
- Define responsibilities and consequences
- Some policy tips
  - A good policy now is better than a great policy later.
  - A simplistic policy that is well distributed and understood is better than a complete policy that has never been seen or accepted.
  - An updated policy is better than an obsolete one.

Security Policies cont'd

- Examples of security policy directives
  - All wireless access points must be centrally managed
  - All wireless access points must be managed in accordance with a set of clearly defined principles
  - No RF networking devices may be operated on campus without written authorization
  - All portable computing devices are subject to enterprise computer security policies

Procedures and Controls

- Infrastructure controls
  - All APs on separate 'untrusted' wired segment
  - Encrypt all WLAN traffic, authenticate all users
    - Safest option: VPN (Layer 3)
    - Alternative: 802.1x/EAP with dynamic WEP (Layer 2)
    - Others: Fortress, Vernier, Blue Socket, etc.
  - Monitor airspace
  - Monitor network
  - Detect and respond to intrusions

Procedures and Controls cont'd

- Mobile device controls
  - Disallow ad-hoc networking mode
  - Require up-to-date AV software
  - Require personal (host-based) firewalls, IDS
  - Local storage of information, e.g. PHI?
    - Disallow
    - Require encryption
  - Educate users on policies and procedures
  - Audit for compliance

Defense in Depth

- *All* of the currently available 802.11 'Layer 2' controls for authentication and encryption are still evolving, still unproven
- Safest to use them only if combined with additional, proven controls at 'Layer 3' and up
  - VPN
  - SSH, SSL, etc.
- Understand the risks if single line of defense

Conclusions

Q: Is wireless networking worth all the risks?
A: It depends!

- Potential benefits? *Significant*
- Known risks? *Significant*
- Costs of risk mitigation? *Significant*
- *Proceed with caution, using a sound risk management approach to safeguarding information.*

References

- W. Arbaugh, N. Shankar, Y.C. Wan, Your 802.11 Wireless Network has No Clothes. Technical report, Dept. of Computer Science, University of Maryland, March 2001. http://www.cs.umd.edu/~waa/wireless.pdf.
- D. Baker, Wireless (In)Security for Health Care. HIMSS Advicacy White Paper, Science Applications International Corporration, January 2003. http://www.himss.org/content/files/WirelessInsecurityV11.pdf.
- N. Borisov, I. Goldberg, and D. Wagner, Intercepting Mobile Communications: The Insecurity of 802.11. Proceedings of MOBICOM 2001, 2001. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

References cont'd

- S. Fluhrer, I. Mantin, A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4. Presented to the Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.http://www.crypto.com/papers/others/rc4_ksaproc.ps.
- J. Puthenkulam, V. Lortz, A. Palekar, D. Simon, The Compound Authentication Binding Problem. Internet-Draft, March 2003. http://www.ietf.org/internet-drafts/draft-puthenkulam-eap-binding-02.txt
- P.Shipley, Open WLANs: the early results of WarDriving.http://www.dis.org/filez/openlans.pdf.
- J. Walker, Unsafe at any key size: an analysis of the WEP encapsulation, Tech. Rep. 03628E. IEEE 802.11 committee, March 2000. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip.