Wireless Exploits Hit The News!

ZDNet Where Technology Means Business

August 2nd, 2007

Hamster plus Hotspot equals Web 2.0 meltdown!

Posted by George Ou @ 2:03 pm
Categories: Security, Infrastructure, Mobile/Wireless, Networking, Servers, News, Desktop, Browsers
Tags: Web, Google Gmail, HotSpot, Web 2.0, Attacker, Wi-Fi Hotspot, Wi-Fi, Tool, George Ou

TALKBACK ADD YOUR OPINION Worthwhile? +7 7 VOTES

Robert Graham (CEO Errata Security) gave his Web 2.0 hijacking presentation to a packed audience at Black Hat 2007 today. The audience erupted with applause and laughter when Graham used his tools to hijack someone's Gmail account during an unscripted demo. The victim in this case was using a typical unprotected Wi-Fi Hotspot and his Gmail account just popped on the large projection screen for 500 or so audience members to see. Of course had the poor chap read my blog about email security last week he might have avoided this embarrassment. But for the vast majority of people using Gmail or any other browser or "Web 2.0" application, they're all just a bunch of sheep waiting to be jacked by Graham's latest exploit.

NETWORKWORLD

BLACK HAT - Researchers: Web apps over Wi-Fi puts data at risk

By Jeremy Kirk, IDG News Service, 08/01/07

Start a discussion Print article

Users who access Google's Gmail or the Facebook social-networking site over Wi-Fi could put their accounts at risk of being hijacked, according to research from Errata Security Inc., a computer security company.

tgdaily

Masters of technology return for BlackHat/Defcon

Security

By Humphrey Cheung

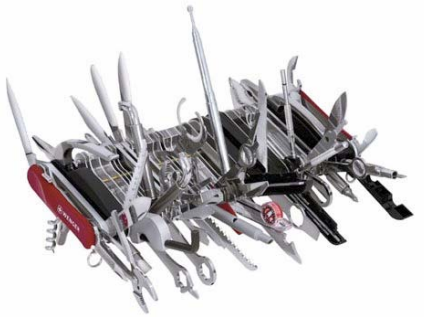
Tuesday, July 24, 2007 15:47

The scheduling will be just as rigorous at Defcon which has added a new "Wireless Village" run by the folks at the Church of the Wifi. Wireless hacking has been a huge part of security conventions and the new village provides a centralized place for people to share ideas. Members of the "Church" will also have a session and plan on introducing their own wireless hacking distribution. In previous years, the group released Rainbow Tables - long list of pre-computed password combinations - to ease WPA cracking.

Public WiFi Hotspots - Benefit or Bane?

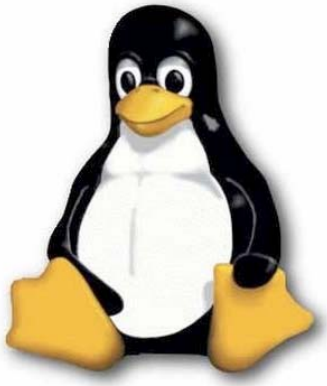
- Public WiFi Hotspots are everywhere
  - Coffee shops, Airports, Train Stations, Urban parks, Resort areas
- Extremely convenient - Inherently insecure
  - WEP and WPA encryption methods are ineffective
    - Both advertise the private encryption keys
    - Most public WiFi operators don't enforce authentication or encryption
  - Real-Time network traffic is visible to anyone "listening" exposing;
    - Unencrypted social security, credit card and bank account info
    - Login information to unsecured (non-ssl) sites, along with content
    - Login info and content of services such as POP email and FTP
    - Website activity of everyone associating with the Hotspot
  - Exposes wireless clients to a potentially hostile network environment
    - Wireless system scanning and exploit tools abound
    - Wireless clients can become low hanging fruit very quickly
      - Unpatched OS or application
      - File sharing
- WiFi vulnerability detection and penetration tactics
  - A concrete threat - advancing with the technology

Wireless Hacking Tool Kit



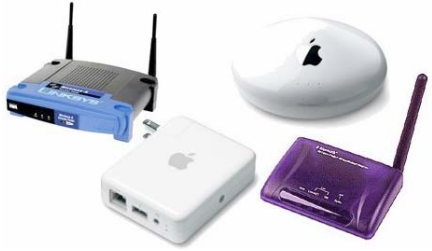
- **PDA's and Laptops**
  - **There is a range of popular PDA devices**
    - **Sharp, HP and Nokia devices ship with embedded linux, or it can be installed**
    - **Nintendo DS and PSP can be loaded with Linux - Both support WiFi**
    - **PDA's are good for discovery, Laptops for penetration testing and attack**
  - **Specialized laptop hardware specifically geared towards WiFi**
    - **Allows researchers to monitor all WiFi traffic as well as enabling customized traffic injection**
- **Operating Systems and Popular Software**
  - **Notable Windows packages**
    - **Commercial**
      - **Airmagnet - http://www.airmagnet.com**
      - **Airopeak - http://www.wildpackets.com**
      - **Sniffer Wireless - http://www.networkgeneral.com**
      - **AirPcap - http://www.cacetech.com**
    - **Open Source - FREE!!!!**
      - **Cain!!! - http://www.oxid.it**
      - **NetStumbler - http://www.netstumbler.org**
      - **Wireshark - http://www.wireshark.org**
      - **Packetyzer - http://www.networkchemistry.com/**

Wireless Hacking Tool Kit



- **Linux**
  - **Currently the preferred OS for wireless research and attacks**
    - **Most popular tools are developed for Linux**
    - **Wide support for powerful WLAN adapters and chipsets**
    - **Extremely configurable OS from kernel up**
  - **Powerful research and attack applications**
    - **WiCrawl - http://midnightresearch.com/products/wicrawl**
    - **MADWiFi - http://madwifi.org**
    - **AiroPeek - http://wildpackets.com**
    - **Airodump-ng - http://www.aircrack-ng.org**
    - **Kismet - http://www.kismetwireless.net**
    - **WireShark - http://www.wireshark.org**
  - **Live Distributions - Work out of the box!**
    - **BackTrack2 - http://remote-exploit.org - Extremely powerful attack platform!**
    - **LiveCD, LiveDVD, USB Flash Drive - http://www.livedistro.org**

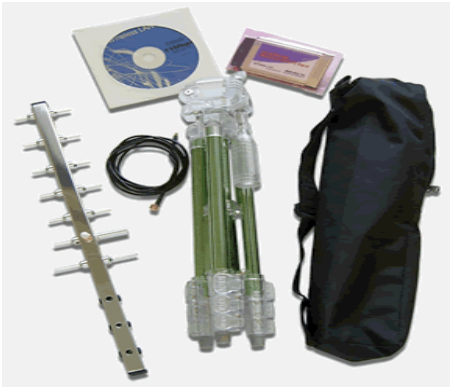
Wireless Hacking Tool Kit



- **Wireless Adaptors and Access Points**
  - **Wireless Adaptors are abundant - some tools require specific chipsets**
  - **Most popular WiFi adaptors include**
    - **Hermes (Orinoco)**
      - **One of the first to offer external antenna connections**
      - **Good receiving sensibility**
    - **Atheros - Currently one of the most powerful research chipsets**
      - **Most common dual band card (802.11a/b/g)**
      - **5GHz radio on chip**
      - **Drivers included with most, if not all, Linux distributions**
  - **Wireless Access Points (WAPs) can be turned into research platform**
  - **Major vendors - NetGear, D-Link, Linksys (Cisco) and Buffalo**
  - **Off the shelf WAPs can be turned into powerful attack systems by loading available packages**
    - **OpenWRT - Functional, extensible Open Source project puts Linux on WAP**
      - **Overwrites WAP operating system and puts linux based package in its place**
      - **Packages like FreeRadius,Samab, dsniff, Kismet, OpenVPN, etc. can be installed**
      - **Originally for the Linksys WRT54G**

Wireless Hacking Tool Kit

- **Antennas - The right tool for the right job**
- **The proper Antenna gives enormous edge to the attacker**
  - **Receiving**
    - **Distance, stealth, better data capture, etc.**
  - **Transmitting**
    - **Enables traffic injection, DoS and MiTM attacks**
  - **High-Gain Parabolic Grid and Yagi antennas for low $$$**
  - **Patch antennas work well in backpacks**
- **Quality amplifiers, cables and connectors available**



Wireless Hacking Tool Kit

- MADWiFi - an Open Source WiFi project
  - Linux kernel driver for Wireless LAN chipsets from Atheros
  - Code repository, bug tracking system, extensive documentation and support
  - Can be used to create multiple Virtual Access Points (VAPs)
    - VAPs can either be clients or APs
  - WLAN card will appear as a normal system NIC although it's much more…..
  - Operational Modes:
    - sta - Station. Acts as a typical WLAN client station
    - ap - Access Point (master). Acts as an AP for WLAN client stations
    - ad-hoc - Operates in peer-to-peer WLAN mode w/o the need for an AP
    - monitor - This mode "sniffs" all WiFi traffic available to it!
    - wds - Wireless Distribution System. Transparent bridging of multple AP's over WLAN links
  - Enables interesting tools for WiFi researchers
    - airmon-ng
    - airodump-ng
    - aircrack-ng
  - Supports WEP and WPA/802.11i
  - Supports 802.1x authentication in AP mode
  - One driver for miniPCI and cardbus devices
  - USB devices not *yet* supported

Hacking is a State of Mind

Demo

- Why these attacks are dangerous
- Demonstrate interception of
  - Web HTTP traffic
  - Aim Traffic
  - Email messages
- Demonstrate interception of email credentials
- Countermeasures
- Evolution of wireless attacks/auditing tools

Why are these attacks dangerous?

- Attacker can be located far away from the Access Point
- Attacks are difficult to detect
- The attacks are not new and are trivial to implement
- Free tools exist to implement them

Demonstration

- We are just another unprivileged user on the network
- These are not vulnerabilities in the websites or the services in general, but a byproduct of an open and shared access point.
- For the purpose of this demo, we are assuming the attacker is on this open access point, but even encryption won't necessarily help.
  - Many attacks exist for the various types of wireless encryption
  - Hardware acceleration is one of the latest tools in an attackers arsenal

Web Demonstration

- HTTP Interception
  - Information can be gleaned from the URL
  - Valuable information can be found in the images alone

IM Demonstration

- IM Interception
  - Many commercial and open-source programs available to archive all chat messages
  - Much information can be derived from the raw packet dumps

Mail Demonstration

- Email Interception
  - Messages can be intercepted over the air
  - Credentials are often tied into a central authentication data-store
  - Credentials can be stolen and used to log into mail server, and likely other key infrastructure elements
  - The same technique can be applied to other services that use these same authentication credentials.
  - Encryption does not necessarily help

Recommendations for Remediation

- Use non-split tunnel VPN
- Use SSL and encrypt where possible
  - Pay attention to certificate verification (application specific)
- Use WPA2 Enterprise mode, or WPA2 Pre-shared key (for home use) with a strong password (13+ mixed class characters)
- General rules apply (patch-levels, firewall, anti-virus, etc)

Future of auditing tools

- Full automation
  - Silica
    - Everything we talked about today in the palm of your hand
  - Wicrawl
    - Designed as an automated security auditing tool
  - FPGA (hardware acceleration)
    - WEP cracking went from 24 hours down to 5 minutes
    - FPGA is likely to see the same advances for other encryption technologies (brute-force attacks)
- More Demos (Time permitting)