

# Auditing Wireless Networks

Neal E. Weatherspoon, CPA, CISA, CISSP  
IT Audit Manager  
Oregon Secretary of State – Audits Division

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Introduction

Why should I be concerned about  
Information technology controls?

and

What do I need to know about  
wireless networking?

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# Agenda

- Risk
- Audit Objectives, Tools, Methodology
- Findings
- Audit Impact

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Risk – What's in Your Wallet?

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# Security Attributes

- Availability
- Confidentiality
- Integrity
- Tradeoff:

Cheap & Convenient \_\_\_\_\_ Expensive & Restrictive

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# Guess Who's Listening?

The screenshot shows the WIGLE.NET website in a Windows Internet Explorer browser. The page features a navigation menu with links for Home, Download, Forums, Post File, Query, Screenshots, Stats, Uploads, Web Maps, MapPacks/Trees, Wiki, and Login. The main content area includes a globe icon, the WIGLE.NET logo, and a tagline: "Wireless Geographic Logging Engine. Making maps of wireless networks since 2001. 13,427,221 points from 827,764,781 unique observations." Below this is a login section with fields for user and password, and a "login" button. A central menu offers various actions: "Find a wireless network by [searching] (must be registered) or [browsing the interactive map]", "Add a wireless network to WIGLE [from a stumble file] or [by hand]", "Add [remarks] to an existing network(must be registered)", "See statistics: [general], [personal] (must be registered), or [group] (must be registered)", and "Download [interactive clients], [location data for clients] (must be registered), [screenshots], or [random pictures]". On the left, there is a "news" section with a headline "lucky 13" and a "WIGLE Millionaire" section. On the right, there are "Ads by Google" for a "802.11n Wi-Fi Analyzer" and "Discover your Network". The browser's taskbar at the bottom shows several open applications and the system clock at 11:15 AM.

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# The Ultimate Denial-of-Service Attack!

“A team of computer security researchers plan to report Wednesday that it had been able to gain wireless access to a combination heart defibrillator and pacemaker. They were able to reprogram it to shut down and to deliver jolts of electricity that would potentially be fatal – if the device had been in a person. The researchers also said they were able to glean personal data by eavesdropping on signals...”

*NY Times March 12, 2008*

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## So What?

- Sensitive and Confidential information could be broadcast in the clear (compliance)
- At increased risk of Denial of Service (DOS) attacks
- Expose internal networks to potential external exploitation

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Legal Compliance (SB 583 – Section 12)

Any person that owns, maintains or otherwise possesses a consumer's personal information must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data.

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# Audit Tools & Methodology

Measuring your WiFi Footprint

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Background

- 2006 did a risk assessment of the state's use of WiFi
- Established a baseline
- We wanted to know the extent of use, whether users were adhering to best security practices, whether WiFi use was controlled by policy.

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Tools

- Laptop (linux)
- GPS
- Wireless card
- Scanning software found on the Internet (kismet)
- Umbrella and a dry pair of shoes!

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Methodology

- Performed preliminary scan (war walk)
- Sent a survey to agencies
- Performed numerous follow-up scans to validate discrepancies (scans vs survey info)
- Interviewed responsible parties (officials and technicians)

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Methodology

- Did not capture packets (we could have)
- Did not exploit the vulnerabilities we found
- Notified state officials & state police prior to scans
- Generally did not enter buildings (unannounced)
- Used NIST Criteria

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# Objectives

Determine:

- Extent of WiFi use
- Implementations followed best security practices
- WiFi use was supported by framework security policy

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# Findings

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Audit Results

- Use of WIFI was widespread
- Vast majority of implementations did not fully implement NIST security recommendations
- Policies generally did not address or regulate WIFI use

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Specific Weaknesses

- Broadcast signals were set too high
- Utilized no or weak encryption protocols
- Broadcast SSID
- WIFI networks not segregated (fire walled) from secure wired networks
- Intrusion detection not utilized
- No monitoring (rogue access points)
- No risk assessment prior to deployment

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# Audit Impact

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

## Lessons Learned

- Watched pots seldom boil over.
- Children behave better when watched closely.
- It's harder to pick out the good guys in a crowd.
- It's hard to feel like a winner when they keep changing the rules.
- IT technicians are generally not the problem nor do they always provide the solution.

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# What Should We Do?

“Foremost, corporations need to:

- Recognize the risk and commit resources to take decisive actions that will control the vulnerabilities.
- Inventory the high-value data and most serious exposures
- Evaluate which countermeasures directly and cost-effectively reduce their highest risks.
- Implement a reasonable strategy that phases in improvements in information security
- Commit ongoing resources to revise and refine over time as circumstances evolve.”

*Information Systems Control Journal – volume 1 2008. “Business Risks and Security Assessment for Mobile Devices” by Patrick Mayer Milligan, PhD., and Donna Hutcheson, CISA.*

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008

# Questions?

Pacific Northwest Intergovernmental  
Audit Forum - Spring 2008