

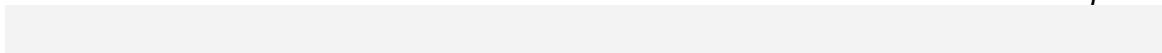
George Mason University
ECE - 646 Fall 2003
Analytical Project

Jay A. Crossler
(240) 498-7774
jay@crossler.com

Project Specification Document

Defensive Strategies for Establishing a Secure Wireless Network

Third Draft of Proposal



Objective and Table of Contents

The objective of this paper is **to find the best possible wireless configuration and methodology**, based on assessing the actual security levels offered by different configuration procedures.

Objective and Table of Contents	2
Comparisons	3
Wireless Protocols.....	3
Installation Procedures.....	3
Problems to be investigated	4
Security Administration.....	4
Vulnerability Testing	4
Key Questions	5
Protocol Questions	5
Hardware Questions.....	5
Software Questions	5
Security Questions	5
Legality Questions	5
Morality Questions.....	5
Procedure for Verifying Results	6
Experimental Methods.....	6
Publications	6
Tentative Table of Contents	7
Time Schedule.....	8
Possible changes to Specification	9
Changes from original idea.....	9
Possible future changes	9
List of Literature.....	10

Comparisons

There are many recommended procedures for securing a wireless network. Most of the commonly distributed ones from technical magazines, websites and product brochures are mostly worthless. Wireless configuration procedures will be compared in terms of ease of install, implied security, actual security and average time to break into.

Wireless Protocols

The following procedures wireless protocols will be considered for analysis.

- 802.11a
- 802.11b
- 802.11g
- 802.11i
- Bluetooth

Installation Procedures

The following categories of installation procedures will be compared for security.

- Default Settings (using systems right out of the box)
 - Physical Security (location of receiver, access to physical breach)
 - Obscurity (turning off SSID broadcasts)
 - Access Control Lists (MAC Address restrictions and IP filtering)
 - Wireless Encryption Protocol (56-bit WEP, 128-bit WEP, AES)
 - Virtual Private Networks
-

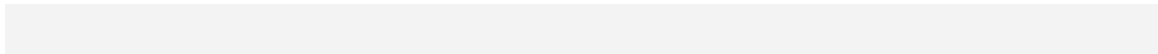
Problems to be investigated

There are many conflicting methods for establishing a secure wireless network. The problems to be investigated are largely related to a lack of understanding of how difficult it is to gain unauthorized access to a wireless network. These problems can be divided into two conceptual categories: Security Administration and Information Vulnerability Testing.

Security Administration

- Wireless Protocols
- Wireless Hardware
- Wireless Broadcast power and location
- Basic intrusion avoidance
- Encryption methodology
- Managerial Oversight

Vulnerability Testing

- Basic Access Attempts
 - Locating Networks (SSID Sniffing)
 - Wireless Router intrusions
 - MAC/IP Address sniffing
 - WEP key sniffing
 - Physical Intrusion Methodology
- 

Key Questions

Protocol Questions

What are the differences between the 802.11a, b, g and I standards? What ranges do they operate at? What frequencies do they use? Are they interchangeable? Are they rated as secure? What major companies use them?

Hardware Questions

What is the range of different wireless hardware? Can this range be expanded? What's the cheapest way of extending listening/broadcasting range? What's the cheapest access hardware? What are the most commonly used network access points?

Software Questions

What software is available to aide in wireless network intrusion? What platforms are required to run this software? How much does professional intrusion detection software cost?

Security Questions

What is the most common wireless network configuration? What are the default passwords of these access points? What are the default configurations of these access points? How can you detect a hidden wireless network? How long on average would it take to find a WEP 56-bit key? A WEP 128-bit key? Are there any tools for denying service to wireless networks? Are they detectable?

Legality Questions

How far is it legal for me to carry out this research? How much is it legal for me to document? Am I allowed to spy on my neighbors, even when they aren't securing their broadcasts?

Morality Questions

When I detect unsecured networks, should I inform the users? Should people be allowed to take advantage of unsecured networks for free internet access? Should any legal measures be taken against "warchalkers" or "wardrivers"? Should I tell my neighbor that he left his Microsoft Money file with no password access and 5 credit card account numbers and over \$50k in bank accounts unsecured?

Procedure for Verifying Results

Experimental Methods

In order to test the “ease of access” of wireless configurations, multiple attempts to access wireless networks with varying configurations will be attempted.

A map of 30 local wireless networks has been developed. Attempts will be made to gain read access to at least one machine on all 30 of these networks. Write access will only be attempted on machines owned by the experimenter.

A “Pringle Can” antenna has been constructed to drastically extend the wireless range of access equipment from 10 meters to approximately 1000 meters. The antenna cost \$11 to construct and provided a refreshing snack for many of my classmates.

A robotic aiming mechanism is being constructed to automate aiming the antenna, as the very small target makes repeat aiming very cumbersome. The aiming mechanism is being constructed using a “Lego Mindstorms” kit and the NQC (Not Quite C) programming language.

A database of common wireless router configurations and passwords is being developed to aid in achieving access.

A special Linux-enabled laptop running “AirSnort”, “Kismet”, “Ethereal” and other utilities will be used as the experimental device.

Initial results indicated that only 5 of the 30 wireless networks have enabled any security beyond the initial settings. 4 of these networks had their SSIDs hidden, and 2 have WEP keys. 3 of these networks have changed configuration since the beginning of this experiment, and are being reevaluated.

Current attempts to crack the WEP keys are taking place, though neither of the networks have generated enough bandwidth to crack the keys (600Mb - 2Gb of packets are usually required for a 56-bit key).

An initial test to generate a Denial of Service attack against an 802.11b network was cancelled due to legality/morality reasons. The procedures for successfully completed previous tests will be described.

Publications

Many wireless security publications, programs, magazines and websites were consulted during the generation of these experiments. Some of these sites had actual checklists for gaining access to a wireless network. These checklists and intrusion steps are comparable to the experiments listed above.

Tentative Table of Contents

- Abstract
- Introduction
 - Quick story describing access to neighbors checking accounts
- Background on wireless protocols
 - Describe 802.11a, 802.11b, 802.11g, 802.11i, Bluetooth
- Wireless security requirements
 - Categories levels of required security
- Wireless security checklists
 - Describe and detail reasons for checklist contents
 - Multiple checklists based on required security levels
 - Describe tradeoffs between cost/scalability/security/time
- Recommended wireless hardware and configuration
 - Describe differences between hardware and protocols
- Analysis of wireless intrusion software
 - Describe different freeware and configurations needed
- Details of wireless intrusion experiments
 - Detail experiment in accessing 30 networks
- Conclusion
 - Recommendations for security, Summary

Time Schedule

October 4 Project Specification Submitted by email

October 15 First Progress Report

Completed map of 30 target networks

November 5 Second Progress Report

November 10-18 Out of country business trip

November 19 Third Progress Report

Goal: November 21 - Complete Lego Mindstorms antenna aiming device

Goal: November 22 - Gain access to 20 networks

Goal: November 29 - Have enough packets to break into 1st WEP network

Goal: December 2 - Have enough packets to break into 2nd WEP network

Goal: December 1 - Gain access to 30 networks

December 3 Final Report Presentation

December 6 Reports Submitted by Email

December 12 Final Oral/written reports

Possible changes to Specification

Changes from original idea

Due to an unexpected and sudden business trip, the main experimenter is scaling down the initial goal to find 100 wireless networks and assess their security statures.

The internal objective has been expanded to provide recommended configurations beyond those given in various trade magazines and product descriptions.

The original objective has changed to no longer focus on 802.11b networks and denial of service attacks against those networks for legal reasons.

Possible future changes

The goal to gain read access to 30 wireless networks might fluctuate due to time constraints.

A future change might be to concentrate more on the mathematical models of cracking the WEP key IVs, and proposed changes to hardware manufacturers.

I am still debating the morality of publishing a “how-to” guide on gaining access to wireless networks.

List of Literature

Internet Sources

802.11 Security, O'Reilly Network -- http://wireless.oreilly.com/pub/q/wireless_chapters

Wireless LAN Security: A Short History --
<http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html>

Seven Security Problems of 802.11 Wireless --
<http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html>

The Art of Wardriving --
<http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20265777,00.htm>

Cisco Aironet Wireless Security - <http://www.iirg.org/12.pdf>

Unsafe at any Size; an Alaysis of WEP Encapsulation -- <http://www.iirg.org/03628E-Unsafe%20at%20any%20key%20size.doc;%20an%20analysis%20of%20the%20WEP%20encapsulation.doc>

Kismet wireless network detector -- <http://www.kismetwireless.net/>

Linux 802.11b and wireless (in)security --
http://www.linuxsecurity.com/feature_stories/wireless-kismet.html

AirSnort WEP cracker -- <http://airsnort.shmoo.com/>

Antenna on the Cheap (er, Chip) -- <http://www.oreillynet.com/cs/weblog/view/wlg/448>

Department of Defense Sources

Denial of Service Techniques in IEEE 802.11b Wireless Networks, Dr. John McEachen -
-7/29/02

Department of Defense Wireless Policy: 8100.bb -- 04/15/03

Technical Guide for Implementation of Department of Navy Afloat, Submarine and Ashore
Wireless Local Area Networks, WLAN Technical Requirements Document -- 6/19/03