https://doi.org/10.48009/2_iis_2007_379-382

A SURVEY ON CURRENT PRACTICES IN ENTERPRISE WIRELESS NETWORKING AND SECURITY MANAGEMENT

Ruidong Zhang, University of Wisconsin – Eau Claire, zhangr@uwec.edu
Julia Welch, Sentry Insurance, Wisconsin

ABSTRACT

Wireless networks, based on IEEE802.11x family of standards, have been deployed as an extension to the wired networks in many enterprises. It has been seen the widespread use of wireless networks in hospitals, universities, airport, hotels, restaurants, libraries, warehouses, factory floors, and convention centers. However, it is unclear what applications are run over wireless networks, and whether these wireless networks are being used for mission critical applications or just for casual convenient Internet access; most importantly, how the wireless networks are secured, what security protocols or technologies are used to protect information transmitted across wireless networks. The purpose of this study is to conduct a survey to understand the current industry practices in using wireless networks and wireless security management.

Keywords: WLAN security; WLAN industry practice; Enterprise WLAN security

INTRODUCTION

Wireless networks have been deployed as an extension to the wired networks in many enterprises. It has been seen the widespread use of wireless networks in hospitals, universities, airport, hotels, restaurants, libraries, warehouses, factory floors, and convention centers. For example, Cisco provided WiFi coverage across the 46 floors of the Hearst Midtown Manhattan tower -- a gross area of 856,000 square feet in total -- with over 288 thin access points installed, covering 2000 employees [2]. In this study, we define wireless networks as networks built with IEEE802.11a, IEEE802.11b, IEEE802.11g, or IEEE802.11n access point technologies. These wireless networks may cover from a spot (hot spot) to a campus (hot zone).

There are still a lot issues that hinder the enterprise use of wireless technologies, such as security issues, appropriate applications, connection stability and transmission capacity. A study by Internet Security Systems (ISS) identified the following security problems related to WLAN implementations [1]:

- Insertion attacks
- Interception and unauthorized monitoring of wireless traffic
- Jamming
- Client-to-Client attacks
- Brute force attacks against access point passwords
- Encryption attacks
- Misconfigurations

Another study has demonstrated that a 104-bit WEP key used by WLAN WEP protocol can be cracked using less than 40.000 frames with a success probability of 50%, and in order to succeed in 95% of all cases, 85,000 packets are needed [3]. With a free network Sniffer such as Ethereal, it is easy to capture thousands of packets in minutes.

These security concerns effectively limit the use of WLAN technologies in mission-critical business applications. For example, ISS suggested in the same study that wireless technology will complement wired connectivity in enterprise environments for a foreseeable future [1]

The purpose of this study is to understand current business practices with respect to WLAN deployment and security management. The overall research methodology will be a questionnaire survey of companies that might have a wireless network deployed. Five hypotheses were made to be tested by the data collected. At the time this paper is written, some preliminary data have been collected. It is expected that the conclusions drawn in this study can help us understand how wireless networks are being deployed, managed and used in what areas, meanwhile offer perspectives that will help the design and development of wireless networks in more organizations,

RESEARCH METHODOLOGY

The research methodology was a questionnaire survey mailed to about 200 organizations nationwide. The followings describe the research methodology in detail.

Creating a database of companies. Currently, a database of over 400 corporate contact addresses and information have been collected, including some Fortune 500 companies and some universities. This database is expected to be expanded to include 1000 more organizations.

Hypotheses Development. Research hypotheses were developed based on our understandings on industry practices**.** These hypotheses are presented in the next section.

Survey instrument development. A sample survey form has been developed for this study. See the survey form enclosed. The survey instrument has been pilot tested and will be further revised.

Sampling. About 100 companies were randomly selected from the database. The questionnaire then was mailed to these companies or organizations.

RESEARCH HYPOTHESES

The following hypotheses have been developed based on above discussions:

H1: IT-related businesses are more likely to have wireless networks than other types of businesses.

H1a: Financial Services would be least likely.

H2: The main concern in deploying wireless networks would be security concerns.

H2a: Those wireless networks that have AP self-broadcasting feature enabled would be less likely to have encryption implemented.

H3: An important consideration in enterprise use of wireless networks is whether the wireless network is used for business or for non-business activities.

H3a: Many companies will prefer to deploy a wireless network for non-critical or non-business applications.

H4: If an organization wants to restrict network access, it would be more likely to have one or more authentication methods implemented.

H5: If a business was monitoring its wireless usage, it would be more likely to track the wireless users.

H5a: A wireless network should have security equivalent to wired networks to be considered for critical business applications.

DATA ANALYSIS AND PRELIMINARY RESULTS

The survey were mailed to about 100 organizations and 18 valid responses received. The following tables are preliminary analysis of data collected.

Company size vs. response rate

# of employees	# of respondents
Less than 100	0
100 – 500	2
500 – 1000	1
1000 – 5000	5
Over 5000	9

Company size vs. WiFi deployed

# of employees	WiFi	No WiFi
100-500	1	1
500-1000	0	1
1000-5000	3	2
over 5000	9	0

Type of industry vs. Wireless Deployment

Type of industry	have WiFi	no WiFi	avg # APs
financial services	1	2	33
higher education	2	1	44
oil and gas	1	1	10
manufacturing	7	0	64
wholesale/retail	2	0	12

Type of industry vs. Wireless Use for Business Applications

Type of industry	Business	non-bus	both
financial services	0	0	1
higher education	1	1	0
oil and gas	1	0	0
manufacturing	7	0	0
wholesale/retail	1	0	1

Self-broadcasting off vs. encryption implemented

AP Broadcasting	Encryption	no encryption
on	1	0
off	12	1

Access Restriction vs. Authentication Implemented

Use Authentication	use restriction	no restriction
Yes	7	3
No	2	2

WLAN monitoring vs. User Tracking

WLAN monitoring	user tracking	user tracking	don't know
YES	6		1
NO	2	3	

From the above data collected, the following Observations can be made:

- Out of 18 respondents, 14 had WLAN deployed.
- Most of responses came from manufacturing companies.
- Financial Services businesses indeed seemed to be under-involved with Wireless – out of 3 responses, only 1 had Wireless deployed.
- It appears that there is no strong correlation between the business type and the type of wireless usage, aside from Higher Education entities which deploy Wireless primarily for student's use.
- Most of respondents have AP self-broadcasting feature disabled,.
- Companies that restrict Wireless access are more likely to use authentication.
- Businesses that monitor their Wireless network are more likely to track individual wireless users.
- It was unexpected that most manufacturing companies have wireless networks deployed.

FUTURE DIRECTION

To run statistical analyses more data need to be collected and the response rate need to be improved too. As the next step, the survey database will be expanded. More questionnaires need to be mailed out. We anticipate that once the study is completed, its results will help describe the scope of various concerns organizations may have regarding the use of Wireless technologies. Also, the most prevalent business practices could be identified and inferences could be made regarding the future use of wireless technologies.

REFERENCES

1. ISS Technical White Paper, "Wireless LAN Security: 802.11b and Corporate Networks," available at http://www.iss.net/documents/whitepapers/wireless_LAN_security.pdf, accessed March 3, 2007.

2. Jones, Dan, "Cisco Goes Green in Hearst Tower," Sept. 21, 2006. Available at http://www.hearstcorp.com/tower/news/092106.html, accessed March 19, 2007.

3. Tews, Erik, Ralf-Philipp Weinmann, and Andrei Pyshkin, "Breaking 104 bit WEP in less than 60 seconds," available at http://eprint.iacr.org/2007/120.pdf, accessed Feb. 1, 2007.