An IT and Security Comparison Decision Support System for Wireless LANs

Kevin T. Reynolds

Universal Publishers
Boca Raton, Florida

An IT and Security Comparison Decision Support System for Wireless LANs

Universal Publishers/uPUBLISH.com
Boca Raton, Florida
USA • 2004

ISBN: 1-58112-541-0

AN IT AND SECURITY COMPARISON DECISION SUPPORT SYSTEM FOR WIRELESS LANS

A Final Project

Presented to the

Faculty of the

Kennedy-Western University

School of Business Administration

Kennedy-Western University

In Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy in

Management Information Systems

by

Kevin T. Reynolds

Plano, Texas

ABSTRACT

AN IT AND SECURITY COMPARISON DECISION SUPPORT SYSTEM FOR WIRELESS LANS

By

Kevin T. Reynolds

Kennedy-Western University

Problem:

Are all Wireless LANs equal?

A network administrator is faced with a plethora of wireless services, complex radio issues, and products for wireless data. There are brand new protocols and products that could become obsolete a day after installation. Over 40% of all deployed WLANs do not even have minimum security activated, exposing the company's network and records to easy outsider access.

The WLAN industry is characterized by rapidly changing, incomplete or proprietary standards, which can impact interoperability goals.

There are complicated ownership costs, performance limitations, and security configurations that exist for WLANs which many network administrators may not understand or know how to compare.

This dissertation presents a decision support system (DSS) that enables a novice network administrator to compare WLAN protocol capabilities, rank security configurations, rate IT cost efforts and use an extensive feature list.

Method:

An in-depth discussion, concerning WLAN protocols, virtual private networks (VPNs), various encryption algorithms, 802.1X authentication mechanisms, and compilation of network selection criteria provides the foundation to construct a small DSS to aid WLAN network administrators.

The DSS uses a set of rules to evaluate a series of potential requirements and provides pertinent WLAN decision-making information.

The DSS environment allows a number of specific what-if scenarios to be reviewed and compared; multiple solutions can be tried without having to deal with the consequences.

The DSS is developed using Microsoft Visual Basic and Access. The DSS stores various features that can be applied to specific vendors

by the network administrator. Alternative technologies are listed by the DSS to educate the decision maker about other options.

Findings:

Over the course of the study, IT ownership costs became a focus in parallel with performance and security analysis. Factors such as 802.11i encryption obsolescing new WLAN equipment, VPNs offering more security while sometimes easier to install, and a simplified vendor model were such significant impacts, that each aspect of the data output was additionally analyzed with respect to IT Effort Level.

There are three main contributions made by this dissertation. The first contribution is the categorization of WLAN comparisons based upon a compilation of risks and selection criteria. The second contribution is implementing this framework in an user interface with a set of network-oriented questions that result in ranked network configurations and costs. The third contribution is the DSS information that allows a decision maker to possibly realize they have overlooked requirements that impact the WLAN.

ACKNOWLEDGEMENTS

I wish to express thanks to my advisor Dr. George Meghabghab, who shared his enthusiasm and insights into the realm of artificial intelligence. I can only hope that I emulate his unfailing pursuit of knowledge in the area of Information Systems.

I would like to dedicate this dissertation to my wife May Reynolds, who has helped me in so many ways with unfailing support that goes beyond words.

Finally, I am grateful to my parents for their inspiration to go to college. Thank you.

TABLE OF CONTENTS

List of Tables ..... **xvi**

List of Figures ..... **xvii**

CHAPTER

1. INTRODUCTION **1**

Statement of the Problem 1

Purpose of the Study 3

Importance of the Study 3

Scope of the Study 5

Rationale of the Study 6

Definition of Terms 6

Overview of the Study 6

CHAPTER

2. REVIEW OF RELATED LITERATURE **9**

Introduction 9

Local Area Networks 9

WLAN System Overview 10

Standards 11

CHAPTER

2. REVIEW OF RELATED LITERATURE (continued)

OSI Model 11

802.11 Layers Overview 12

802.11 Topology Overview 13

802.11 Mobility and Roaming 16

802.11 Services 19

Station Services 19

Distribution System Services 20

802.11MAC Layer Frames 21

Management Frames 21

Control Frames 24

Data Frames 26

Access Operating Modes 28

CSMA Contention Mode 28

CTS/RTS Contention Mode 29

Contention Free Mode 30

MAC Operational Aspects 31

Timing Interval 31

SSID 31

Power Management 31

CHAPTER

2. REVIEW OF RELATED LITERATURE (continued)

Varying Data Speeds 32

MIB 32

802.11 PHY Layer Overview 32

802.11 Radio Spectrum 32

802.11 Radio Technologies 36

802.11 Frequency Hopping 36

802.11 Direct Sequence 37

802.11 OFDM 39

802.11a 39

802.11g 40

PHY Layer Protocol Description 42

Physical Layer Functions 44

802.11 Security 44

WLAN Security Background 45

Layer 3 Security versus Layer 2 46

Some Best Security Practices 47

Security Policy for WLAN Additions 50

WLAN Authentication 51

CHAPTER

2. REVIEW OF RELATED LITERATURE (continued)

Disable SSID Broadcasts 51

Open Authentication 52

MAC Based Authentication 52

WEP (Shared Key) Authentication 53

WEP Algorithm Overview 53

Open Authentication with WEP Activated 55

MAC Authentication with WEP Activated 56

802.1X Network Authentication & Key Management 56

EAP Authentication Overview 60

Mutual 802.1X Authentication Sequence 62

WPA – WEP Revision 64

Key Hierarchy 65

WEP Software Patch: TKIP 66

TKIP: 4 Improvements 67

TKIP Algorithm Specifics 68

802.11i Planned Security Evolution 70

AES Overview 71

Authentication Protocols 73

CHAPTER

2. REVIEW OF RELATED LITERATURE (continued)

Common Authentication Protocols used by WLANs 74

EAP-TLS 74

PEAP 75

EAP-TTLS 76

LEAP 76

Kerberos 77

VPNs 78

Advantages of VPNs 79

Disadvantages of VPNs 80

Typical VPN Types 82

Hardware Based VPNs 83

Firewall Based VPNs 83

Software Based VPNs 84

VPNs Commonly Available 85

WLAN VPNs 86

IPSec Overview.....89

Personal Firewalls 90

Network Firewalls.....91

Some Typical VPN WLAN Configurations 91

CHAPTER

2. REVIEW OF RELATED LITERATURE (continued)

VPN Encrypts and Separate RADIUS server 92

AP Embedded VPN Authenticates and Encrypts 93

Totally Separate VPNs 94

Remote Office VPN Configuration 94

Intrusion Detection 95

Other Wireless Technologies 95

Wireless Data Services 95

Circuit Switched Cellular or PCS Data Service 97

Packet Data Cellular or PCS Service 97

Packet Data Services 97

802.11 Hotspot Data Services Overview 98

Alternative WLAN Technologies 102

Bluetooth 102

HIPERLAN2 103

Infrared IrDA 104

WLAN Operational Factors 106

WLAN Advantages 106

WLAN Disadvantages 107

CHAPTER

2. REVIEW OF RELATED LITERATURE (continued)

Cost of Ownership 107

Total Cost of Ownership 109

Deployment Factors 110

Number of APs 111

Implementations 112

WLAN Risk Analysis 114

Risk: Staff Competency 115

Risk: RF Interference 115

Risk: Interoperability Issues 116

Risk: Security Holes 118

Risk: Application Interfaces 118

Risk: Unclear Requirements 119

Risk: Product availability 121

Selection Criteria Review 121

Summary 126

CHAPTER

3. METHODOLOGY 129

Approach 129

CHAPTER

3. METHODOLOGY (continued)

Data Gathering Method....129

Database of Study....129

Protocol/Spectrum Analysis....132

Interoperability Selection....133

Security Level Selection....135

Validity of Data....136

Originality and Limitation of Data....136

Summary....137

CHAPTER

4. DATA ANALYSIS....139

Decision Support System Overview....139

Performance Description of Inputs....143

Security Description of Inputs....147

Interoperability Description of Inputs....148

Evaluation Criteria of Performance Selection....152

Evaluation Criteria of Security Selection....152

Evaluation Criteria of Interoperability Selection....153

Feature List Overview....153

User Interface Description....155

CHAPTER

5. Summary, Conclusion & Recommendations.....172

Summary 172

Conclusion.....174

Recommendations for Further Research.....175

BIBLIOGRAPHY.....177

GLOSSARY 215

LIST OF TABLES

Table **Page**

2.1 ISM Spectrum 35

2.2 Spectrum and Protocol Traffic Capacity 41

2.3 PLCP Protocol Data Units 43

2.4 Wireless Data Services.....98

2.5 Popular WLAN Technologies 105

2.6 Selection Criteria for LAN, Router, and WLAN.....122

2.7 Selection Criteria for Technology, Wireless Network Equipment, and 802.11 Protocol Factors 123

2.8 PC Magazine WLAN Feature Set 124

2.9 WLAN Feature Set Comparison Factors 125

4.1 Protocol Supportability Factors for Users with Selection Assessments 146

4.2 Security Cost Factors Used in the DSS.....147

4.3 IT Interoperability Cost Factors Used in the DSS.....151

4.4 Feature List Stored in the DSS.....154

LIST OF FIGURES

Figure **Page**

2.1 OSI and 802.11 Layers 12

2.2 MAC and PHY 802 Layers.....13

2.3 WLAN System.....15

2.4 Distribution System, Portal and LAN.....17

2.5 Roaming between APs and ESS 18

2.6 Authentication and EAP Layers 59

2.7 Mutual 802.1X Authentication Sequence 64

2.8 Key Hierarchy Sequence 65

3.1 Requirements and Selection Process.....130

3.2 Requirements, Selection and Feature Process.....137

4.1 DSS Structure 140

4.2 Performance and Security Relationships 141

4.3 Feature and Alternative Relationships 142

4.4 User Interface – Main Menu 155

4.5 User Interface – Requirements & Comparisons Menu 156

4.6 User Interface – Feature List Menu.....157

LIST OF FIGURES (continued)

Figure		Page
4.7	User Interface – File Name Assignment	158
4.8	UI - Performance Requirements Selection	159
4.9	UI - Security Level Selection	160
4.10	UI -VPN Question	161
4.11	UI – AES Question	162
4.12	UI - Interoperability Roaming Selection	163
4.13	UI – Feature Product List Name	164
4.14	UI – New Vendor Feature List	165
4.15	UI –View Existing Product Feature List	166
4.16	UI – Updated Product Feature List	167
4.17	UI – Results of IT Requirements, Performance	168
4.18	UI– Results of IT Requirements, Security	169
4.19	UI –Results of IT Requirements, Interoperability	170
4.20	UI –Results of the Product Features	171

AN IT AND SECURITY COMPARISON DECISION SUPPORT SYSTEM FOR WIRELESS LANS

Chapter 1

Introduction

A Gartner analyst recently told a packed room of technology conference attendees that the average company has a wireless network without their management's knowledge. A director of security strategies for Hurwitz Group described the growth of wireless LANs as organic, due to ease of installation and advertised low costs.

Today, wireless LAN equipment can be purchased for as cheap as two hundred dollars and easily installed; allowing outsiders for miles around the company open access to the company's most sensitive network and records. That same wireless LAN can cause the entire company's wireless inventory control system to create invalid records as well as severely impact the company's wireless PBX.

Statement of the Problem

A network administrator is faced with a plethora of wireless services, gadgets and products for wireless data.

The Wireless LAN Alliance (WLANA) conducted a study and concluded that only 50% of the costs were capital equipment. Similarly, Gartner expressed office wireless replacement cost breakdown comprising of 11% capital, 47% end user operational, 16% administration, and 26% IT operation. It is foreseeable that network administrators can easily face large maintenance and operation issues, after selecting and distributing a WLAN not meeting their requirements and goals.

Consulting firms describe companies as typically deploying enterprise wireless LANs that have security features deactivated or degrading their bandwidth by adding more wireless LAN nodes.

Further complicating the selection criteria, magazine articles announce the failure of wireless LAN security. The WLAN business sector is a quickly evolving industry with partially proprietary products, security risks, large lists of specifications, and changing protocols.

Antenna coverage, frequency channels, frequency hopping, direct sequence, orthogonal frequency division multiplex, multipath reflections, RC4 encryption techniques, and war driving are topics that are not typically encountered by a network administrator when selecting routers and Ethernet LAN equipment.

This research study examines the research question: are all wireless LANs equal?

Purpose of the Study

This study discusses the information technology and security metrics used in a decision support system (DSS) to compare wireless LANs.

This study identifies specific metrics to compare wireless LANs with respect to a network administrator's requirements: WLAN protocol options, and the respective performance, security configurations, as well as the cost of ownership that is significantly impacted by the depth of interoperability goals.

In addition to requirements selections, a feature list allows a network administrator to compare vendors WLAN models and store the comparisons.

Importance of the Study

According to Gartner wireless LANs (WLANs) will continue to impact companies.

- By the end of 2002, 30% of all enterprises will risk security breaches due to improper 802.11b wireless deployments.

- At least 20% of large businesses already have rogue WLANs installed by employees, unknown by their IT department.
- At only 9% in 2000, by 2007, WLAN will surpass 90% market penetration into the professional mobile PC installed base.

New standards, protocols, and partially proprietary product configurations are announced monthly for WLANs. Just like any other network components, WLANs have a set of capabilities, a finite life cycle and ownership costs. Unlike other network components, WLANs can become obsolete overnight due to radio interference.

Magazines provide extensive feature set comparisons for WLANs, but do not incorporate risk, consider scenarios that can degrade performance, incorporate a user's preference or provide an assessment of IT ownership costs which can outstrip capital equipment costs.

Selecting certain WLAN attributes can limit or eliminate network alternatives for a network administrator resulting in high maintenance and operations support or even worse, unusable equipment. This study presents a DSS that can compare metrics of WLAN with respect to a DSS user's preference, using facts about risks, protocol differences, and ownership support.

Scope of the Study

This study is limited to referenced standards, published texts, and vendor specifications. The focus will be on 802.11 wireless RF LANs, rather than competing technologies such as Bluetooth, HomeRF, or the very similar HiperLAN2.

Emphasis on security by the industry has been a significant component of this study, due to protocol inadequacies. Emerging products based on nearly complete standards such as the 802.11g standard or the access controller option present a moving target to research.

As with routers, switches and other capital equipment, this study is biased toward performance in terms of data speed and flexibility.

An emphasis on RF interference is another significant factor within the study and metrics.

Finally, rather than a distributed database with several servers and a large data warehouse, a Microsoft Access program will be used to store the various data tables that are derived during this study to support the user's pre-defined queries, as well as storing feature comparisons.

Rationale of the Study

This research study intends to evaluate and analyze WLAN metrics that impact performance and affect risk. It is intended to use the derived metrics within a DSS.

The DSS will allow a user planning to purchase and install a WLAN to evaluate areas that affect architecture, performance, and risks.

Definition of Terms

See the glossary provided at the end of this paper.

Overview of the Study

During the review of literature review stage, (section two) of the study: 802.11 standards, 802.11 modes of operation, security authentication, encryption algorithm evolution, authentication types, and VPNs, will establish the protocol performance characteristics and levels of security available to an administrator. Next wireless data services and WLAN technologies will be reviewed to compare what is available beyond the 802.11-based WLANs.

Aspects of cost of ownership, risk analysis, and selection criteria from nine different sources will be provided to set the stage for structured data used in a decision support system.