CERIAS

Creation of a Security Solution Selection Matrix for WLAN Implementations Using Real Options

A.R. Scheller, P.T. Rawles, J.E. Goldman[1]

[1] *Department of Computer Technology, School of Technology, Purdue University, West Lafayette, IN 47907*

Abstract

The purpose of this project was to create a Security Solution Selection Matrix for WLAN implementations using Luehrman's Real Options methodology. The methodology was used to evaluate the effectiveness of WLAN security techniques for the following environments: Small Office Home Office (SOHO)/Home, Corporate, and Public Access. The matrix allowed for the security techniques to be compared to one another so that a WLAN user or network administrator could select the appropriate technique, or a combination of techniques, to implement based on the individual's environment. Through this project a method is developed for applying Real Options to a technologically-associated, assessment paradigm. This poster presents this approach of employing Real Options for a technologically-associated, assessment paradigm.

Methodology

A two dimensional options space was created defining vulnerability and difficulty of use as appropriate axes. Vulnerability quantified the amount of protection a security technique offered. Difficulty of use quantified how difficult a technique was to implement and maintain.

Suitable metrics were defined to evaluate each axis. These metrics caused either a positive or negative effect on the value of each axis. Scores between zero and two were assigned for each metric. Each score was verified based on the research of each WLAN security technique and whether or not the metric was supported. The layout of the options space quantified a higher score as a negative impact on the metric. Zero indicated the metric was fully supported; one represented partial support; and two signified no support. The value along each axis was calculated by adding up the corresponding metric scores. This process is illustrated in **Figure 1**.

The quantitative data was represented by dividing the options space into nine sections. Each section was labeled with the level of vulnerability versus the difficulty of use, respectively. An assumption was made to clarify the primary function of a security technique, which is to protect the WLAN from vulnerabilities regardless of how difficult it is to use. The options space was broken down further by dividing it into three sections that define the different levels of an effective security technique. This allowed for the quantitative data to be represented qualitatively. **Figure 2** is the result of this process.

A security technique was placed in the options space at the point of intersection for the two calculated axis values. This placement represented the effectiveness of that technique. Effectiveness was found to be optimal where the two axis cross (both difficulty of use and vulnerability are zero), whereas optimal ineffectiveness is the point where both values are at their max (both difficulty of use and vulnerability are ten). **Figure 3** illustrates the Real Options diagram for a Corporate WLAN. A square symbolizes a "partial" security technique; a dashed circle symbolizes an estimated guess since the technology of the security technique was not established at the time the project was completed. The arrows signify a possible change in the direction of the arrow. **Figure 4** was used to qualify the assessment of each security technique based on their placement in the options space.

Axis	Metrics	Score	Total	Real Options Assessment
Vulnerability	Authentication/Authorization	1	5	Validation of a username and password is required to access corporate network from home WLAN. The type of authentication protocol used (i.e. PAP, CHAP, etc.) as well as the appropriate security settings, such as requiring a secure password, will enhance the level of security provided by a VPN
	Encryption	0		Encryption is supported, but the level of encryption is dependent upon the protocol used and supported by a company (i.e. PPTP, IPSec, etc.)
	Nonrepudiation	2		Not supported
	Susceptible to Hacker Tools	1		Certain protocols are fallible, and if the security settings do not require a secure password or encryption, then the VPN can be compromised.
	Mode Dependency	1		The level of security offered by a VPN is dependent on the authentication and encryption protocol used. VPNs can also support EAP/802.1x authentication
Difficulty of Use	Implementation/Configuration	2	5	While a VPN client comes with many OSes, proper configuration is necessary for it to work correctly and provide the best security offered by a company
	Adoption	1		A company most likely has a VPN infrastructure already in place
	Additional Resources	0		A user only needs a VPN Client, which is provided by many OSes
	Administration Overhead	1		Unless changes have been made to the VPN Server that require a change in the properties of a VPN client, there is no overhead for a home user
	Interoperability/Incompatibility	1		Problems may occur (such as a laptop freezing) based on the combination of the WLAN hardware and the type of VPN software

Figure 1 – Metrics Evaluation (Home - VPN)

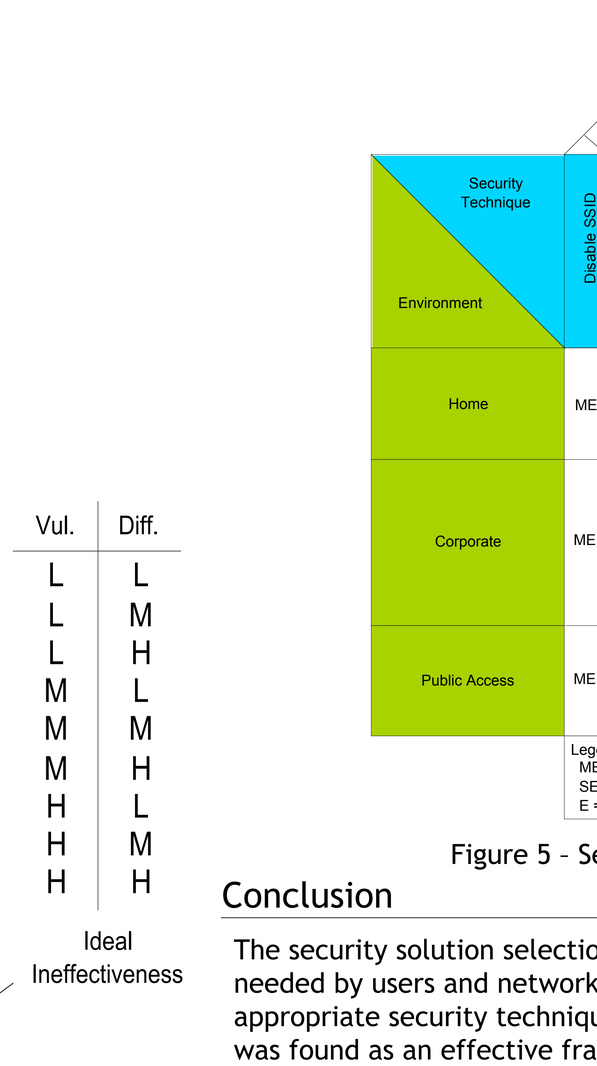

Figure 3 – Corporate Real Options Diagram

Corporate	Security Technique	Vulnerability	Difficulty of Use	Real Options Assessment	Impact
1	SSID Broadcasting	9	3	ME	Allows for users to associate to an AP by typing it in or selecting it from a list. If broadcasting is disabled then the WLAN may be obscurely secure, but the 802.11 standard and some OSes do not support it. Disabling the SSID will slightly decrease the vulnerability
2	MAC Address Filtering	7	3	ME	A MAC address can be spoofed but most likely not as easy or as accessible as it is to crack WEP. Difficulty of use will increase due to administration overhead as the amount of WLAN users increases
3	WEP Encryption	7	5	ME	Static WEP has been cracked and is basically used as a deterrent to network intruders. However, the longer the key, the longer it takes to crack, thus decreasing vulnerability slightly.
4	VPN	5	3	E	Most often used to connect to a corporate network from a home environment, but the amount of security it can offer is highly dependent upon the protocol used (IPSec vs. PPTP). A more secure protocol will decrease the vulnerability of the technique, but increase the difficulty of use
5	802.1x/EAP	3	6	SE	As the amount of WLAN users increases, the difficulty of use will increase due to administration overhead. Vulnerability can decrease based on the type of authentication method used (password vs. certificate)
6	WPA	3	8	SE	While TKIP is based on RC-4, it provides better encryption than static WEP. This technique is an interim solution on the path to 802.11i that will hopefully decrease the vulnerability in its next installment, WPA 2.0. The difficulty of use should decrease because network administrators already know how to support it.
7	IPSec	4	5	E/SE	If a company already has IPSec in place then the difficulty of use will decrease.
8	IEEE 802.11i (AES-based) *Expected value*	2	6	SE	Migration from TSN infrastructure may be too expensive. If IPSec is already in place at a company then the difficulty of use will decrease

Legend: E = Effective; SE = Somewhat Effective; ME = Minimally Effective

Figure 4 – Qualifying Corporate Real Options

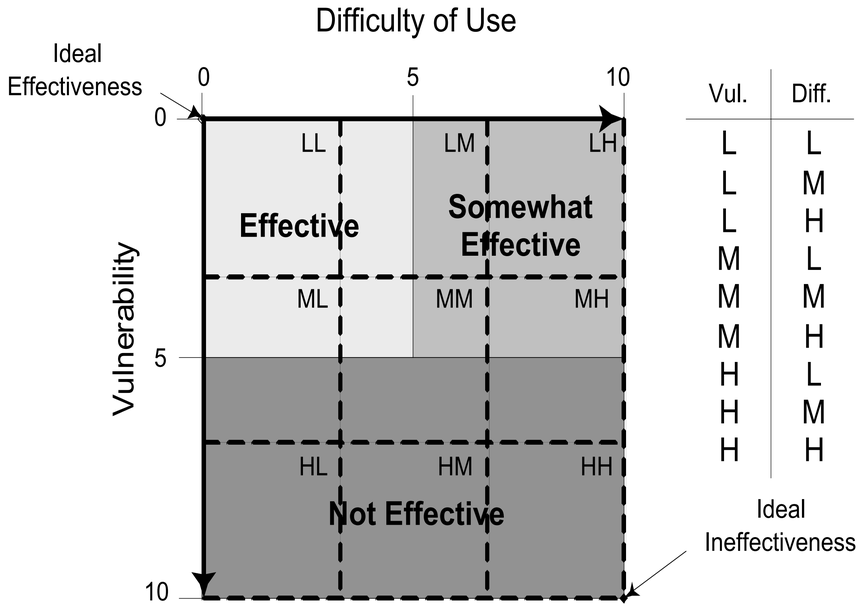

Figure 2 – Options Space Divisions

Result

Creation of the Security Solution Selection Matrix outlined the effectiveness of each security technique evaluated by Real Options. A home user or business can use the matrix to decide what security technique(s) to incorporate on a WLAN. Correlation between the WLAN security techniques is provided in the top pyramid-like portion. Additional "non-WLAN" security techniques were also suggested for each environment.

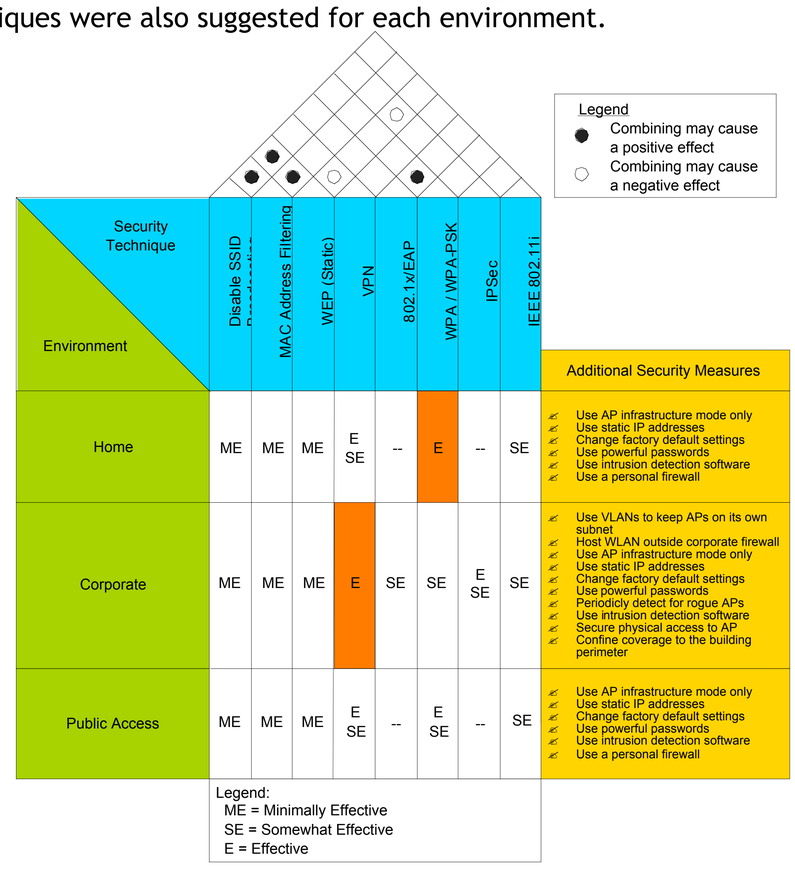

Figure 5 – Security Solution Selection Matrix

Conclusion

The security solution selection matrix provided the necessary information needed by users and network administrators to select and implement appropriate security techniques for specific WLAN environments. Real Options was found as an effective framework for technological evaluations that is adaptable to the rate of technology inception and flexible to fit the needs of a home user or corporate network administrator. This research can be used to implement a Wireless LAN Security Methodology for any of the environments discussed.

PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center