Wirelss Security on Security Standard Policy: A Case Studty

Reza Amirpoor
IMED, Dep. of Computer Management,
Bharati Vidyapeeth,
PUNE, 411008, INDIA
reza_amirpoor@yahoo.com

Ajay Kumar
Director, Institute of Computer Applications,
JSPM's JAYAWANT,
Tathawade, PUNE, 411033, INDIA
ajay19_61@rediffmail.com

Satish R. Deavne
Principal, Institute of Technology,
Dr. D. Y. Patil Ramrao Adik, Nerul,
Navi Mumbai, 400706, INDIA
satish@rait.ac.in

***Abstract*— Administrators of a network have a variety of different authentication and encryption technologies to choose from. Administrators must also take into account a variety of organizational factors, not just of technical factors and must rank what their risks are and then design a security policy that is cost effective and manageable. This paper shows variety of systems security on different network systems and then and provide a solution to adjust security systems of wireless network on security standard and also analyze case studies of how to deployed security systems.**

Keywords- Security standards; Security Policy; Wireless

I. INTRODUCTION

Security in organization is one of the important parts in manager's view. Security system in today's internet era is interconnected on different networks, and on various type of network systems required to apply proper security model. Table 1 shows taxonomy of various security systems on networks; it shows area for each security system. Manager should select the best security model depend on the type of systems for own network. These security systems are distinguished by facilities, cost, area, information sensitivity, etc… Organization must design a security policy and this policy may be different for each information systems. The creation of security policy required the understanding of vulnerable in that network. Each information data evaluation will be considered with respect to others view? What is value of the data in security view? To mitigate security concern, a security policy in good write-up and implementation is required.

II. SECURITY POLICY

Protection of assets is critical part of each organization. Wireless vulnerable can give anxious to organization about the data. Despite benefit of wireless is always an enthusiasm to remain in organizations. Changes in technological solutions should be based upon a security policy. Without a policy, security practices will be undertaken without any clear strategy, purpose or common understanding.

A. Why Policy?

Organizations can benefit from the conveniences of wireless but it's risky from a security standpoint not to have a policy in place to help to guide the users in the appropriate implementation and use of the technology [1]. A well-written wireless security policy will provide a reference document that will answer users' questions about security and is a document that can be referenced if conflicts arise during the implementation or daily use of the technology.

In any case, poor security architecture can create conflicts and tensions by unnaturally restricting the user's options. Inferior security components can hinder application growth, and applications might be forced into choosing between business feature support and security. Well-designed applications can catch and address many of these issues successfully at the architectural review. [2]

The major purpose of the security policy is to select the appropriate security solutions to face those threat events while ensuring that the cost of protecting the infrastructure does not exceed the benefit it provides.

B. Information Technology Security Evaluation criteria (ITSEC)

The Information Technology Security Evaluation Criteria (ITSEC) was the standard European security evaluation criteria. The ITSEC addressed an expanded view of confidentiality, integrity and availability with the aim of more explicitly addressing both military and commercial requirements. The ITSEC defined confidentiality as prevention of unauthorized disclosure of information; integrity as prevention of the unauthorized modification of information; and availability as prevention of the unauthorized withholding of resources. Trusted Computer Security Evaluation Criteria (TCSEC) or Orange Book looks specifically at the operating system and not other issues like networking and databases, etc…, Orange Book addresses confidentiality and does not address Integrity.

The orange book provides a graded classification of systems that is divided into divisions of security levels A, B, C,

D. The classification A represents the highest level of security. Each Division can have one or more numbered classes. The class with higher numbers indicates a great degree of trust and security, Example B2 is higher than B1, C2 is higher than C1.

TABLE I. TAXONOMY OF NETWORKS ON SECURITY SYSTEMS

	Stand Alone	**Wired Networks**							**Wireless Network**	
		Wide Area Network			**Local Network**					
Systems / Security	Stand Alone	P2P	Distributed	Client Server	Intranet Base	Internet Base	Web Base	Server Base	Wireless LAN	Mobile Network
VPN		*	*		*	*			*	*
Firewall			*		*	*			*	*
Virus Guard	*	*	*	*	*	*	*	*	*	*
Intrusion Detection			*	*	*	*	*	*	*	*
MPLS					*	*			*	*
DMZ					*	*			*	*
SSID									*	*
MAC Filtering		*	*	*	*	*	*	*	*	*
WEP			*						*	*
RADIUS			*		*	*			*	*
TKIP									*	*
Kerberos			*						*	*
IPSec		*	*	*	*	*	*	*	*	*
SSL		*	*	*	*	*	*	*	*	*
SSH			*	*	*	*			*	*
Antenna radiation zone									*	*

* indicates possibility of the applying security

ITSEC Functionality Classes showed as below:

- D (Minimal Protection)
- C1 (Discretionary Security Protection)
- C2 (Controlled Access Protection)
- B1 (Labeled Security Protection)
- B2 (Structured Protection)
- A1 (Verified Design)
- Systems that provide high integrity
- Systems that provide high availability
- Systems that provide data integrity during communication
- Systems that provide high confidentiality
- Networks with high demands on confidentiality and integrity

We can see ITSEC is equal to TCSEC plus integrity and availability. Where D is minimal security and the last level is highest security. [3]

III. SECYRITY LEVELS IN WIRELESS SYSTEMS

Fig 1 shows the levels of security in wireless system; WPA2 with AES is the most secure level.

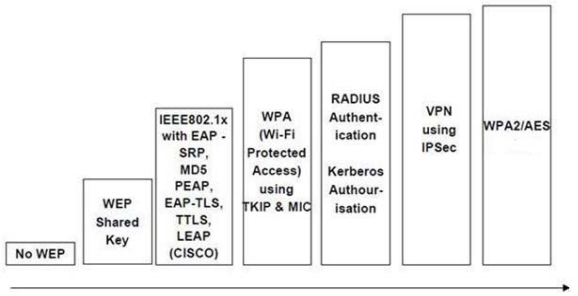

Figure 1. 802.11 Security Level [4]

A. Security Level Techniques

Security level and techniques used in wireless are shown in Fig. 1, which explained as below:

- No Security

  No security is like leaving your door wide open. Anyone can come in and use the network access, No WEP.

- WEP

  At minimum, you should turn on WEP, password protect shared drives and resources, change the network name from the default (SSID), use MAC address filtering, and turn-off broadcasts if possible.

- WPA

  WPA provides user authentication, since WEP lacks any means of authentication. Designed to secure present and future versions of IEEE 802.11 devices, WPA is a subset of the IEEE 802.11i specification. WPA replaces WEP with a strong new encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). It also provides a scheme of mutual authentication using IEEE 802.1X/Extensible Authentication Protocol (EAP) authentication or Pre-Shared Key (PSK) technology.

- WPA 802.1x

  802.1x uses EAP, an existing protocol that works on Ethernet, Token Ring, or WLANs for message exchange during the authentication process. IEEE 802.1x is not a single authentication method; rather, it utilizes EAP as its authentication framework. The 802.1x specification itself does not specify or mandate any authentication methods.

- RADUIS

  IEEE 802.1x integrates well with open standards for Authentication, Authorization, and Accounting (AAA). Through RADIUS, IEEE 802.1x permits the management of authorization on a per-user basis. Per-user services include filtering (layer 2 or layer 3), tunneling, dynamic virtual LANs (VLANs), rate limits, and so on. Two specifications make up the RADIUS protocol suite: authentication and accounting.

- KERBEROS

  Kerberos provides robust security, uninterrupted network connectivity for voice and data devices. Kerberos provides both user authentication and encryption key management, and can guard networks from attacks on data in transmission, including interruption, interception, modification, and fabrication.

  Kerberos provides confidentiality, authentication, integrity, access control, and availability.

- VPN

  A VPN enables a specific group of users to access private network data and resources securely over the Internet or other networks. VPNs are characterized by the concurrent use of tunneling, encryption, authentication, and access control over a public network.

- IPSec

  IPSec VPNs have nearly become accepted as the de facto standard for securing IP data transmission over shared public data networks since VPN software has been developed for a wide variety of clients. It addresses authentication, data confidentiality, integrity, and key management, in addition to tunneling. Basically, IPSec encapsulates a packet by wrapping another packet around it. It then encrypts the entire packet. This encrypted stream of traffic forms a secure tunnel across an otherwise unsecured network.

- WPA2

  WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES).

B. Downfall of Security Levels

Table II shows control mechanisms, business benefits, convenience features, and threats in relation to available safeguard technologies.

TABLE II. CONTROL MECHANISMS AND THREATS

Control Mechanisms \ Safeguards	Wired VPN	Mobile VPN	Firewall	WEP	Dynamic WEP	WPA-TKIP-PSK	WPA2-CCMP-PSK	WPA2-CCMP-EAP	Sensors
Server-side authentication	3	3			3	2		3	
Strong user authentication	3	3			3			3	
System authentication (PSK)	3	3		2	2	3	3		
Wireless encryption	3	3		1	1	2	3	3	
Wired encryption	3	3							
Integrity protection	3	3				2	3	3	
Segmentation, packet filtering			3						
Segmentation, user authentication	3	3							
Rogue device detection									3
Publicly reviewed security protocols	3	3				1	3	3	
Authorization and audit log	2	2			2	1	1	2	2
Policies and training									

The intersections indicate to which level a safeguard includes a particular control mechanism, business benefit, or convenience feature, where 3 = full, 2 = partial, and 1 = marginal support [5]. As showed in Table II VPN is full support for integrity and authentication but WEP is only marginal support for integrity and no authentication; so these are weak on WEP system. We will describe some more downfalls of security systems in this part and in the next part we will compare and adjust security system by security standard through these downfalls and robust.

Downfall of security levels are shown as below [6],[7]:

- WEP
  - o Data can be compromised and forged without key
  - o No effective way to prevent key compromise
  - o Theft or compromise of one device compromises all

WEP is vulnerable in Integrity, confidentiality and availability. So it becomes the first level of security systems.

- WPA
  - o Theft or compromise of one device compromises all
  - o Password-based keys can be found by search
  - o Turns active attack into Denial-of-Service

WPA-PKS is vulnerable in availability and confidentiality; but it solved WEP problems. WPA-TKIP is vulnerable in integrity too.

- 802.1x/EAP
  - o Lack of supplicants.
  - o 802.1X is only a perimeter security technology that means that once a supplicant is successfully authenticated; the system will not control his network traffic.
- VPN

VPNs are touted as a secure solution for WLANs, VPNs using one-way authentication are still vulnerable to exploitation such as man-in-the-middle attacks. Almost all VPN solutions shipping today are proprietary in some form or another and are generally not interoperable. Because of this fact, not all devices may have client software available for any one VPN supplier. Also, it is often the case that once a VPN is installed, a different VPN won't operate on the same machine. Thus, VPNs are impractical for securing a public access WLAN.

VPN is costly methodology, so it should use only for those networks which require more security.

IV. ADJUST SECURITY POLICY WITH SECURITY SYSTEM AND CASE STUDY

We can classify the data on base on security standard; for this reason we should know about value of the data. Through this knowledge we can compare and apply the properly security system on our data.

Fig. 2 elaborates taxonomy of ITSEC and security levels; minimum security is No WEP belongs to F1, which f1 equal to D in TCSEC standard. F2-F5 is C1 to A, which cover an ACL for security. F10 is maximum security which covers by RADIUS and VPN and WPA2 levels.

Administrators of a network have a variety of different authentication and encryption technologies to choose from. But administrators must also take a variety of organizational factors into account, not just technical factors. Administrators must rank what their risks are and then design a security policy that is cost effective and manageable. To select the best security level for our organization, administrator should know about cost and weakness of security levels and value of the data on own organization [8].

Standard Level (ITSEC) / Security level	F10 Confidentiality + Integrity	F9 High Confidentiality	F8 Data Integrity during communication	F7 High Availability	F6 High Integrity	F5-F2 ACL	F1
No Security							√
WEP						√	
WPA + PSK					√		
(WPA+TKIP) OR (Dynamic WEP+ Firewall) , 802.1X /EAP		√	√	√			
RADIUS(Authentication) Kerberos Authorization)	√	√	√				
VPN + IPSec	√	√					
WPA2 -AES	√						

Figure 2: Classification of Security Levels and Standards

The large insurance firm that we interviewed installed 802.11wireless hardware across the majority of their

domestic sites. As part of our interview, we had to keep their name and the specific wireless vendor they chose confidential. Their data is in F8 level of security standard, they felt that VPN did not scale well enough because of licensing costs for the VPN digital certificates and the cost to put in more VPN gateways. They used 802.1x EAP-TLS and RADUIS and WPA TKIP encryption.

Initially they had a lot of problems getting WPA-TKIP working correctly. There were a lot of bugs in the wireless equipment and the driver software as well. They got both the driver developers and the hardware developers to jointly fix the bugs. But eventually they moved away from WPA and went to WEP with rotating keys (Dynamic WEP) and firewall. They were secure and cost effectiveness method.

Another company we already interviewed was a industrial company which according to our research, they have limit value on their data and they used ACL for control of users and WEP security system for their organization. They have selected best policy and security system, depend on our research.

V. CONCLUSION AND FUTURE AREAS OF RESEARCH

An effective wireless security policy is based on many factors. These factors could be sensitivity of data, cost of security level, total cost of ownership, etc. We classified security policy in one table to check out and select the proper security level on same table. As shown by our case studies, different types of organizations have vastly different needs. Understanding the authentication and encryption technologies is vital to create an effective and manageable security policy. The need for security level with respect to the organization and behavior is reflected in this paper. Using the case studies one can decide the level of security for a particular organization.

REFERENCES

[1] Michael Manley, Cheri McEntee, Anthony Molet, and Joon S. Park. A framework of an effective wireless security policy for sensitive organizations. In Proceedings of the 6th IEEE Information Assurance Workshop (IAW), IEEE Computer Society West Point, New York, June 15-17, (2005), 150–157.

[2] Jay Ramachandran, Designing Security Architecture Solutions, WILE, 2006.

[3] DigitalSherlock.com , systems evaluation methods, GNU Free Documentation License, 2005.

[4] Ray Hunt, Security in Mobile and Wireless Networks, University of Canterbury, New Zealand , 2006.

[5] Columbitech, Security Threats and Risk Mitigation in a Retail Network Environment, Feb. 2008.

[6] Raul Bodea, Wireless Security – The Downfall of WEP, March 2009.

[7] Jesse Walker, Selecting the Optimum 802.11 Security Level, Intel Corporation, 2003.

[8]. Dan Ziminsky and Bill Davidge, Computer Security,Usability and Privacy, August 2004.

AUTHORS PROFILE

Reza Amirpoor received the B.E. degree from Sharif University of Technology in 1996 and MBA (IT) degrees, from Symbiosis International Univ. in 2006. He is Ph.D. student in Bharati Vidyapeeth, PUNE since 2007. His research interest includes Wireless Systems, Network Security, Quality.

Dr. Ajay Kumar has completed M.Sc. Engg. in Computer Science and Ph.D. He is having 21 years of teaching and research experience. Presently he is working as Director, JSPM's JAYAWANT Institute of Computer Applications, Pune, India, He has published 4 books in Information Technology. He has also published more than 35 papers in National / International Conferences and Journals. His area of research is Computer Networks, mobile computing, wireless systems, security systems and Software engineering.

Dr. SATISH R. DEVANE has completed M.E. Electronics, from Dr. B.A. M University, Aurangabad and Ph.D. in Information Technology from IIT Bombay 2006. Presently he is working as Principal, Dr. D. Y. Patil Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, India, He has published one book in Computer programming He has also published more than 20 papers in National / International Conferences and Journals. He has Life Membership in IEEE, ISTE, CSI, IETE, ISACA, and Security Technology Forum of CSI. His area of research is E-Commerce, Computer Organization, Network Communication, Web Technology, Smartcard, System Analysis and Design, Operating System, Network Security, Software Engineering.