IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-17, May 2019 E-ISSN: 2347-2693

Wireless Security Network Using Authentication and Encryption

M. Dukitha[1*], G. Sheeba[2]

[1,2]Dept. of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur

Corresponding Author: dukitham@gmail.com, Tel- 9486344558

Available online at: www.ijcseonline.org

***Abstract*—** The 21th Century is defined by human scientific breakthroughs. One of them is the global use of the Internet. Almost every educated person nowadays knows more or less about the internet. Thereby, a large percentage of the human populations make use of the internet on a daily basis. Wireless internet access is thereby made affordable and accessible for everyone and that has boosted human communication and economy development into a new era. However, along with benefits, wireless internet access also possesses several risks and threats of security. The Internet has become a fertile land for criminals of all kinds to operate. Most of the time what they try to take is personal information, some of them of extreme values and sensitivity, from naive and unaware users. In that sense, a comprehensive study on how cybercriminal carry out their attacks and how to avoid and actually prevent such attacks if possible would be beneficial for the righteous netizens.

***Keywords*—** Wireless, WLAN, Security, Internet, Protection, Cyber threats

I. INTRODUCTION

Wireless networks are too inexpensive to ignore. But, security has stymied many network managers looking to bring wireless into the corporate fold. There's a lot of information and misinformation out there about types of wireless network security technologies. This chapter will help to clear up some of that confusion, and present some common types of wireless network security technologies to help guide your path. The first thing you have to do is educate yourself. The Internet has a lot of data and opinions on wireless security technologies, but it's difficult to get a perspective on things without a good background primer (like this book). You need to put this into the context of corporate security. What threats are you worried about? How sensitive are the data on the wireless- local area network (LAN) or wide area network (WAN)? What vulnerabilities do you need to guard against? Sniffing? Denial of service? Freeloading? Impersonation? You'll never establish an appropriate 802.11 security policy for your corporate network if you don't think about these technologies now Second, you must do something to get started. Wired Equivalent Privacy (WEP) is still an awful technique to use. It's like giving everyone in the company the same password and never changing it. But, that doesn't mean you shouldn't use it. The theoretical attacks on WEP exploited by various tools are blocked by modem firmware. In some recent testing, using current releases of 10 different enterprise-class access points and eight different client cards, Initialization Vector-based attacks on WEP were no longer effective. Third, you should arm yourself with wireless security tools. Most wireless security tools are fabulous for enterprise network managers. If you only have a few access points to worry about, a laptop with some public domain your enterprise's data is secure. tools is a fine start. But, without at least some tools, you'll be left completely in the dark about the wireless data speeds that are beginning to surround your network [10]. Fourth, you should prepare your wireless security strategy. Today, the 802.1 X-based authentications is up-and-running technology to help resolve basic wireless security problems. Or, you can go down the virtual private network (VPN) path and treat wireless users the same way you treat remote access VPN clients. Either works fine with off-the-shelf hardware [11]. Over the long run, the Institute of Electrical and Electronics Engineers (IEEE) 802.111 standard will lay out a path to higher security for wireless networks that combines 802.IX authentication with better key management than is available on WEP. But that standard is still being cooked, and it will be a year or more before things completely settle. So, with the preceding in mind, many wireless networks are not properly secured or-even worse-are completely unsecured. Naturally, security is a top concern among those interested in deploying wireless networks. Fortunately, both user knowledge about security and the solutions offered by technology vendors are improving. Today's wireless networks feature comprehensive security capabilities and, when these networks are properly protected, enterprises can confidently take advantage of the benefits they offer. This first part of the chapter will help you gain a better understanding of wireless LAN security elements and best practices that can go a long way toward enabling you to reap the benefits of wireless networking. And, you get peace of mind, know

II. WIRELESS NETWORK SECURITY AND TECHNOLOGY

Vendors are doing a good job of improving security features, and users are getting an understanding of wireless security. "But, all threats are still considered important, and vendors continually need to address the lingering perception that wireless LANs are insecure. Indeed, security is the biggest barrier to the adoption of wireless LANs. And, it's not just a big-enterprise worry. When it comes to wireless networking, security is still the number one concern for enterprises across all sizes. Gaining a better understanding of wireless LAN security elements and employing some best practices can go a long way toward enabling you to reap the benefits of wireless networking. And, you get peace of mind, knowing your enterprise's data is secure.

III. ELEMENT OF WIRELESS SECURITY

Intentionally or not, enterprises and individuals may set up wireless networks with no security at all. That happens because most wireless access points come from the factory in open access mode by default, meaning that all security features are turned off It's the buyer's responsibility to turn them on. Three actions can help to secure a wireless network:

• Discouraging unauthorized users through authentication
• Preventing unofficial connections through the elimination of rogue access points
• Protecting data while it's being transmitted through encryption [3]

Not coincidentally, these are also important issues to companies. The number one wireless LAN security concern is users from outside the company (illicitly or maliciously accessing the enterprise wireless LAN. Number two is internal rogue access points, and number three is encryption.

IV. USING AUTHENTICATION

When you want to make sure that the individuals who use a wireless network are authorized to do so, use authentication (sometimes called access control). Unique logins and passwords are the basis of authentication, but additional tools can make authentication more secure and reliable. The best authentication is per-user, per-session mutual authentication between the user and the authentication source.

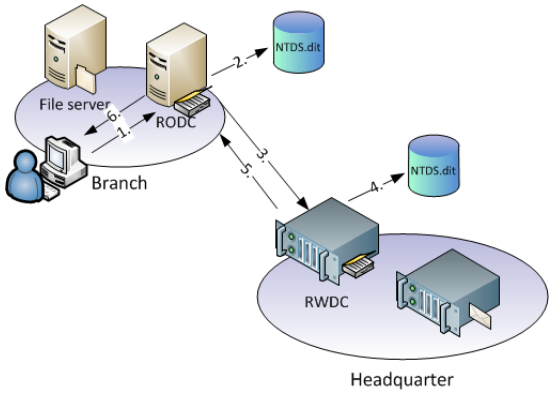

Fig. 1

Checking For Rogue Access Points

A well-meaning employee who enjoys a wireless network at home might want to enjoy the same freedom at work. He or she might purchase a cheap access point and plug it into a network jack without asking permission. These are known as rogue access points, and the majority of these are installed by employees—not malicious intruders. Even company-sanctioned access points, when configured improperly, can be security risks. Checking for rogue access points isn't difficult. There are tools that can help, and checking can be done with a wireless laptop and software in a small building or by using a management appliance collecting data from your access points. You can have technical personnel scan for new wireless access points. And, if they do a daily scan, they can pick these things up early.

V. USING ENCRYPTION

To make sure that data can't be read, and to protect data from being altered as it's transmitted between an access point and a wireless device, use encryption. In a basic sense, encryption is like secret code: It translates your data into gibberish that only the intended recipient understands. Encryption requires that both the sender and receiver have a key to decode the transmitted data. The most secured encryption uses very complicated keys, or algorithms, that change regularly to protect data.

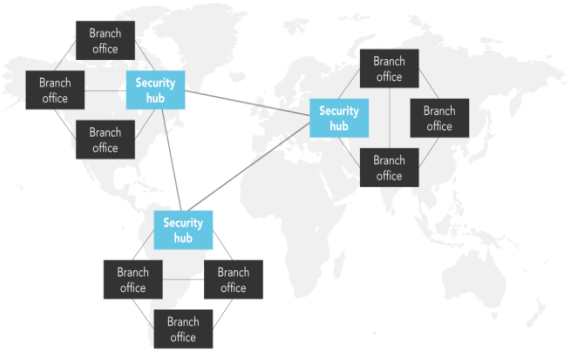

Fig. 2

Available Solutions For Wireless Security

Three solutions are available for secure wireless LAN encryption and authentication:

• Wi-Fi Protected Access (WPA)
• Wi-Fi Protected Access 2 (WPA2)
• Virtual private networking (VPN) [3]

The solution you select is specific to the type of wireless LAN you're accessing and the level of data encryption required.

VI. POLICIES FOR WIRELESS SECURITY

In some cases, you may have different security settings for different users, or groups of users, on your network. These security settings can be established using a virtual LAN (VLAN) on the access point. For example, you can set up different security policies for distinct user groups within your enterprise such as finance, legal, manufacturing, or human resources. You can also set up separate security policies for customers, partners, or visitors accessing your wireless LAN. This allows you to cost effectively use a single access point to support multiple user groups with different security settings and security requirements—all while keeping your network secure and protected. It is also important to consider wireless network security in the context of overall network security and network management. The majority of enterprises that deploy, or will deploy, wireless LANs want to do it in a way that complements the wired LAN. They want it integrated with common management.

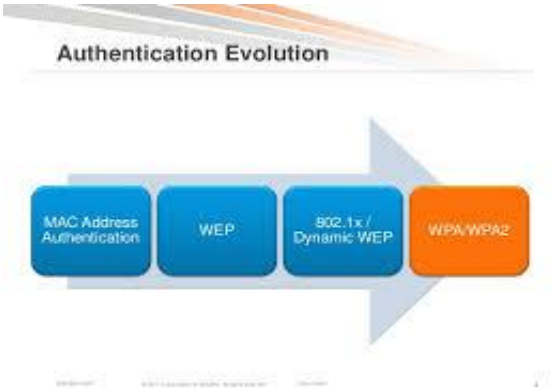

Fig. 3

A common management system increases efficiency for network administrators. Resource-strapped SMBs can use management tools to simplify and automate many repetitive and time-consuming administrative tasks. Wireless LAN security (even when integrated with overall network management) only works if it's turned on and used consistently across the entire wireless LAN. That's why user policies are also an important part of good security practices. Resist the temptation to overact when setting a wireless LAN security policy. The first policy is often 'no wireless. The problem with that is, there are so many massive gains from having wireless in place. The challenge is to devise a wireless LAN user policy that's simple enough that people will abide by it, but secure enough to protect the network. Today that's an easier balance to strike because WPA and WPA2 are built into Wife certified access points and client devices.

Your wireless LAN security policy should also cover when and how employees can use public hot spots, the use of personal devices on the enterprise wireless network, the forbidding of rogue devices, and a strong password policy.

VII. WIRELESS SECURITY ARCHITECTURE RECOMMENDATION

There is a clear need for a security solution that embraces the world of mobile and wireless computing with an approach that addresses all forms of connectivity, including Wi-Fi on premises, Wi-Fi off premises, cellular data, public kiosks, home access, and whatever else may become available. But before you can specify effective security architecture, there are other important security features that you will probably need, including the ability to:

• Allow conformance with government regulations that protect items such as financial and medical information.
• Have control over the end-point node to check for proper software configuration such as virus protection, to scan the system for dangerous code, and to clear caches.
• Provide granular control to resources, rather than just providing access to a network.
• Support both managed and unmanaged nodes as well as accommodate a wide range of device types, including desktops, portable computers, PDAs, and smart phones [1].

The security architecture that meets all of these needs is an SSL-based VPN. SSL VPNs take advantage of the browsers and the SSL security layer that are available for nearly all computing platforms, including notebook platforms, PDAs, and smart phones.

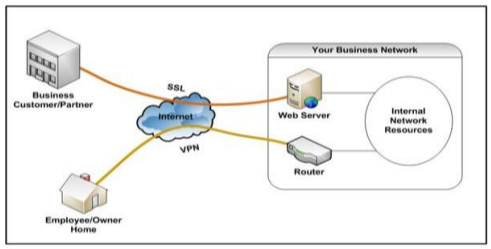

Fig. 4

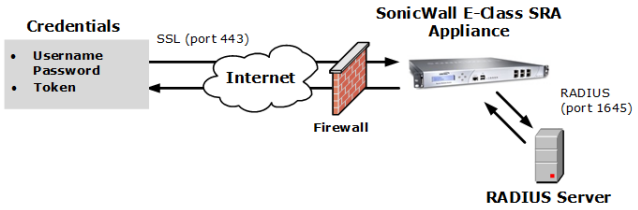

Fig. 5

Fig. 2-1 shows an SSL appliance securing all forms of wireless access and shows how IP traffic is redirected into an SSL tunnel.

VIII. Wireless Network Security

There is a clear need for a security solution that embraces the world of mobile and wireless computing—^with an approach that addresses all forms of connectivity, including Wi-Fi on premises, Wi-Fi off premises, cellular data, public kiosks, home access, and whatever else may become available. But before you can specify an effective security architecture, there are other important security features that you will probably need, including the ability to:

• Allow conformance with government regulations that protect items such as financial and medical information.
• Have control over the end-point node to check for proper software configuration such as virus protection, to scan the system for dangerous code, and to clear caches.
• Provide granular control to resources, rather than just providing access to a network.

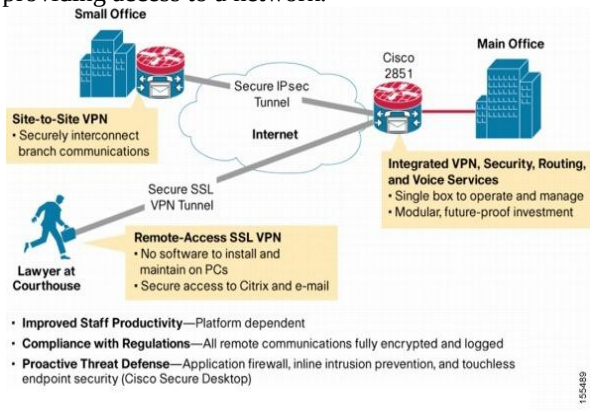

Fig. 6

• Support both managed and unmanaged nodes as well as accommodate a wide range of device types, including desktops, portable computers, PDAs, and smart phones [1].
The security architecture that meets all of these needs is an SSL-based VPN. SSL VPNs take advantage of the browsers and the SSL security layer that are available for nearly all computing platforms, including notebook platforms, PDAs, and smart phones.

IX. Conclusion

Open VPN needs to connect to a single TCP or UDP port on the remote side. Once established, it can encapsulate all data down to the Networking layer, or even down to the Data-Link layer, if your solution requires it. You can use it to create robust VPN connections between individual machines, or simply use it to connect network routers over untrusted wireless networks. VPN technology is a complex fled, and is a bit beyond the scope of this section to go into more detail. It is important to understand how VPNs ft into the structure of your network in order to provide the best possible protection without opening up your organization to unintentional problems. Since the tools are freely available and run over standard TCP, any educated user can implement SSH connections for themselves, providing their own end-to-end encryption without administrator intervention. OpenSSH (http://openssh.org/) is probably the most popular implementation on Unix-like platforms.

References

[I] Peter Rysavy, "Secure Wireless Networking Using SSL VPNs," Rysavy Research, [© 2005 Aventail Corp. All rights reserved. Aventail Corporation, 808 Howell St., Second Floor, Seattle, WA 98101], Rysavy Research, PO Box 680, Hood River, OR 97031U.S.A., 2005
[2] Robert Whitely, Stan Schatt and Benjamin Gray."SSL Is the Future of Remote Access VPNs," © 1997-2005, Forrester Research, Inc. All rights reserved. Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139, USA), June, 2004.
[3] Fred Sandsmark, "Securing Wireless Networks," Copyright © 2005 Cisco Systems, Inc. All rights reserved. Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134, USA [iQ Magazine (vil. VI,No. 1)., 2005.
[4] Jupitermedia Headquarters, Jupiter Research, 23 Old Kings Highway South, Darien, CT 06820, 2005.
[5] Scott Robinson, "Strengthen Your Wireless Security By Avoiding These Missteps," Copyright ©2005 CNET Networks, Inc. All rights reserved. TechRepublic, 235 Second Street, San Francisco, CA 94105, 2005.
[6] "End Point Control: Secure Anywhere Access With Reduced Risk And Increased IT Control," © 2004 Aventail Corp. All rights reserved. Aventail Corporation, 808 Howell St., Second Floor, Seattle, WA 98101, 2004.
[7] John R. Vacca, Firewalls : Jumpstart for Network and Systems Administrators, Digital Press, 2004.
[8] John R. Vacca, Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan, McGraw-Hill, 2001.
[9] John R. Vacca, The Essential Guide To Storage Area Networks, Prentice Hall, 2002.
[10] John R. Vacca, Wireless Data Demystified (Mcgraw-Hill Demystified Series) (Paperback)s, McGraw-Hill Professional, 2003.

