Wireless Network Security

Maghen Smith

315 E. Magnolia Avenue Apt J237 Auburn, AL 36830

256 777 8119

mjs0026@auburn.edu

**ABSTRACT**

Over the past decade wireless networks have become an essential part of both business and personal computer user. Since the emergence of the first Wireless local area network, ALOHAnet, in 1971, the cost of wireless internet has significantly decreased and the popularity of wireless internet has significantly increased. Wireless communications are convenient, cheap, and fast. In contrast, there are physical limits to the distance that a electrical signal can propagate through a wire, and thus, wired networks are not as convenient or as fast. With the emergence and growing popularity of wireless networks, significant growth in security mechanisms is required in to ensure the protection of our information. Suddenly our personal information is flying through the air instead of moving through a wire that we can physically see. Should we trust that our information is sent where we think it is? Who can intercept our information as it is transmitted? Is the information arriving at its destination in the same state we sent it?This paper contains explanations of the major security risks of connecting to a wireless network in hopes that the reader will better understand the vulnerabilities in computer networks. This paper is meant to inform the reader of the major risks involved in using today’s popular wireless technologies, as well as what can be done to ensure the security of wireless networks.

**Categories and Subject Descriptors**

D.3.3 [**Programming Languages**]: Language Contructs and Features – *abstract data types, polymorphism, control structures.* This is just an example, please use the correct category and subject descriptors for your submission*.* The ACM Computing Classification Scheme: <http://www.acm.org/class/1998/>

**General Terms**

Algorithms, Performance, Design, Reliability, Security, Standardization, Theory.

**Keywords**

Networks, security, WLAN, Wifi, WEP, WPA/2, OSI, VPN, SSL, LEAP, vulnerabilities, attacks, cryptography, encryption.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*Conference’04*, Month 1–2, 2004, City, State, Country.

Copyright 2004 ACM 1-58113-000-0/00/0004…$5.00.

# INTRODUCTION

According to Singh, “A Wireless Network is a wireless communication system that allows computers and workstations to communicate and exchange data with each other using electromagnetic waves as the transmission medium.”[OSI] Wireless communications have become popular because of their price, speed, flexibility, mobility, and convenience.[COMP, OSI] They especially rocketed around 2003, as the prices of laptops and smart phones declined and IEEE standards emerged.[PD] Wireless networks are now decidedly established and are even an expected convenience for most businesses, schools, homes, hospitals, airports, etc.[OSI]

Thus, it is essential that wireless communications shield our information as it travels through the air, and this introduced a new field of security in the early 1990s. Pre-1990s computer and network security in general were ignored.[PD] Obviously this is no longer an option. Wireless communications differ from wired communications in that the transmission medium is now air instead of cables. To expose wired communications, simply “tap” the physical cable. [COMP] How can we insure that the information we send via the air is kept secure?

Various wireless technologies have emerged since 1970, the most-notable of which is the Wireless Local Area Network, equipped with accompanying IEEE standards that offer average protection against exposure. In Section 2 we will discuss general network information, in particular the OSI network model, that we will use in the succeeding sections. We will then outline the most popular wireless technologies available today in Section 3, the most common attacks against wireless networks in Section 4, and defenses against those attacks in Section 5. We will draw conclusions in Section 6.

# NETWORK OVERVIEW

<Figure 1 … >

The two most common network reference models are the Open Systems Interconnection (OSI) Reference Model and the Transmission Control Protocol/ Internet Protocol (TCP/IP) reference model. The models are created as stacked layers to promote data encapsulation. Each layer offers services to the layer above, and, in turn, each layer can request services from the layer below according to the protocols needed in each layer. Each unit of information created from each respective layer will be encapsulated with information from the layer beneath until the bottom layer is reached and the units are physically sent “across the wire” or in the air.[CN] We will refer common layers on the OSI and TCP/IP reference models, and thus outline the basic functions of each starting from the bottom. Figure 1 shows the OSI Reference Model on the left and the TCP/IP model’s protocols on the right. This illustrates the differences in layers between the two models. The basic network information covered in this section creates a foundation for the rest of the information presented in the paper.

## Physical Layer

The bottommost layer of the OSI model is the Physical Layer. This layer is comprised of the hardware components necessary for the communication. The Physical Layer is responsible for transporting the bits from one machine to another; this can be done through guided media, such as a coax cable, or wirelessly, through electromagnetic waves. This layer is referred to as a point-to-point layer; the physical layer is responsible only for transmitting the information to the next machine on its path towards the final destination. This could include a router, network interface on a laptop or a repeater. [CN]

## Link Layer

The next layer building upwards in the OSI Model is the Link Layer, which is also a point-to-point layer. This layer is further split into two sublayers, the Medium Access Control Layer, and the Data Link Layer. The Medium Access Control layer is directly “above” the physical layer in the model, and thus communicates directly with the hardware to provide means to share the transmission medium optimally. This includes the management of broadcast channels and multiple access protocols, which determine when and how often frames can be sent. One of the first and simplest multiple access protocol, ALOHA, was created and used in the first wireless network ALOHAnet. Any time a client has information to send, it simply sends and (hopes for/) waits for a confirmation, or more commonly referred to as an ACK, short for acknowledgement, that the next machine got the messages. One of the more efficient protocols in the Carrier Sense Multiple Access/ Collision Detection Protocol. The goal of this protocol is to stop the transmission of damaged frames through collision avoidance; this is accomplished through listening to the transmission medium after sending. If a collision is heard, then the sender immediately stops sending.[PD, CN] The Data Link Layer must perform basic framing, or the forming of a distinct unit of information that is to be transmitted, and handling some error detection/correction through the use of checksums and timeouts. The checksum is computed by adding all the bytes in the message. The checksum is then sent along with the message; the receiver must compute a checksum of the frame it received and then compare to the checksum it received. If there checksums differ it is likely that there was an error in transmission. It should also be noted that this is not the most reliable way to check for errors in that errors could occur in the checksum itself. Timeouts occur when a frame is sent across the wire, and a response is not received in a reasonable amount of time. If a reasonable amount of time passes without an ACK, it is safe to conclude something went wrong and then choose whether or not to retransmit. [CN]

The Link Layer in general is responsible for the delivery of information to the correct MAC address on the recipient machine. This MAC address corresponds to a specific network adapter, and “allow computers to uniquely identify themselves on a network at this relatively low level". [EE]

**2.3.Network Layer**

The last point-to-point layer is the Network Layer. The Network Layer receives services from the Data Link Layer and provides services to the Transport Layer. The key functions of the Network layer are addressing the units of information, which are called packets in the Network Layer, routing and congestion control. Here it is important to note that there are two methods of addressing depending on the type of connection used. Connection-oriented services will send information over a set path, called a virtual circuit, that coverts the entire path form the sender to the receiver; connectionless services will simply send information one “hop” at a time. In other words, the connection-oriented service will know exactly which stops to take along the way and the connectionless service will simply send information to the next stop and hope that that host will know where to send from there. Thus, routing is introduced: each “stop” on the path from the source to destination will need to know where send next. Routing tables in each machine keep track if the most efficient routes to destinations in the network. [CN]

The most important protocol in the Network Layer is the Internet Protocol (IP). This protocol routes between networks instead of inside networks and is found on every host connected to the internet, router on a Local Area Network (LAN), and router on the Internet backbone. We will focus on IPv4, where each IP address is split into bits for the network address and bits for the host address within the network. Routers must look at the network portion of the IP address to determine which network is appropriate. Thus the idea of subnets are necessary; subnets are created to split up networks into smaller portions, make routing easier, and thereby reduce traffic within a specified region.[CN]

**2.4.Transport Layer**

The Transport Layer is serviced by the Network Layer and offers services to the Application layer of the TCP/IP model or the Session Layer of the OSI model. This is the first layer that we classify as truly offering end-to-end services. This layer houses two important protocols, both of which are used frequently on the internet, the Transmission Control Protocol and the User Datagram Protocol, or TCP and UDP, respectively. TCP provides reliable, in-order, delivery of information units, now called segments, to the correct port number of the receiver. A single host may have multiple connections, so the transport layer differentiates between applications on the host through the port number. [CN]

**2.5.Application Layer**

The Application Layer on the TCP/IP reference model encompasses the session, presentation, and application layers on the OSI reference model. This layer handles high-level protocols such as FTP, HTTP, Telnet, etc. This layer does the “real work” for users. In reality the lower layers only function to server this layer, and this is the layer that most computer users know about and interface with.[CN]

To conclude this summery of the computer networks, consider an example of a telnet server. Telnet servers are identified by the port number 53. The server will prepare information to send to a client, then pass this unit of information to TCP in the Transport Layer below. TCP is identified by the protocol number 6. The transport layer will add information around the packed passed down from the Telnet Server \*\*\*\*\* FINISH THIS. [CN]

# WIRELESS TECHNOLOGIES

Doshi states “It seems that there are a wide variety of wireless network technologies out there in the market but the one which out stands is wireless LAN based 802.11” [WNS1] We will discuss the

## WLAN

Please use a 9-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

## VPN

The title (Helvetica 18-point bold), authors' names (Helvetica 12-point) and affiliations (Helvetica 10-point) run across the full width of the page – one column wide. We also recommend phone number (Helvetica 10-point) and e-mail address (Helvetica 12-point). See the top of this page for three addresses. If only one address is needed, center all address text. For two addresses, use two centered tabs, and so on. For more than three authors, you may have to improvise.[[1]](#footnote-1)

## SSL

Please leave 3.81 cm (1.5") of blank text box at the bottom of the left column of the first page for the copyright notice.

## LEAP

For pages other than the first page, start at the top of the page, and continue in double-column format. The two columns on the last page should be as close to equal length as possible.

Table 1. Table captions should be placed above the table

|  |  |  |  |
| --- | --- | --- | --- |
| **Graphics** | **Top** | **In-between** | **Bottom** |
| Tables | End | Last | First |
| Figures | Good | Similar | Very well |

## References and Citations

Footnotes should be Times New Roman 9-point, and justified to the full width of the column.

Use the “ACM Reference format” for references – that is, a numbered list at the end of the article, ordered alphabetically and formatted accordingly. See examples of some typical reference types, in the new “ACM Reference format”, at the end of this document. Within this template, use the style named *references* for the text. Acceptable abbreviations, for journal names, can be found here: <http://library.caltech.edu/reference/abbreviations/>

The references are also in 9 pt., but that section (see Section 7) is ragged right. References should be published materials accessible to the public. Internal technical reports may be cited only if they are easily accessible (i.e. you can give the address to obtain the report within your citation) and may be obtained by any reader. Proprietary information may not be cited. Private communications should be acknowledged, not referenced (e.g., “[Robertson, personal communication]”).

## Page Numbering, Headers and Footers

Do not include headers, footers or page numbers in your submission. These will be added when the publications are assembled.

# ATTACKS

“Unauthorized and poorly secured access points are the main areas where attackers look to mount an attack” [WNS1]

Captions should be Times New Roman 9-point bold. They should be numbered (e.g., “Table 1” or “Figure 2”), please note that the word for Table and Figure are spelled out. Figure’s captions should be centered beneath the image or picture, and Table captions should be centered above the table body.

# DEFENSE AND PREVENTION

The heading of a section should be in Times New Roman 12-point bold in all-capitals flush left with an additional 6-points of white space above the section head. Sections and subsequent sub- sections should be numbered and flush left. For a section head and a subsection head together (such as Section 3 and subsection 3.1), use no additional space above the subsection head.

## Subsections

The heading of subsections should be in Times New Roman 12-point bold with only the initial letters capitalized. (Note: For subsections and subsubsections, a word like *the* or *a* is not capitalized unless it is the first word of the header.)

### Subsubsections

The heading for subsubsections should be in Times New Roman 11-point italic with initial letters capitalized and 6-points of white space above the subsubsection head.

#### Subsubsections

The heading for subsubsections should be in Times New Roman 11-point italic with initial letters capitalized.

#### Subsubsections

The heading for subsubsections should be in Times New Roman 11-point italic with initial letters capitalized.

# CONCLUSIONS

Our thanks to ACM SIGCHI for allowing us to modify templates they had developed.

# REFERENCES

1. Halil Ibrahim Bulbul, Ihsan Batmaz, and Mesut Ozel. 2008. Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols. In *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop* (e-Forensics '08). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, , Article 9 , 6 pages.. [COMP]
2. Singh, Rajinder. 2012. Wireless Network Security main threats at different layers. in *International Journal or Wired and Wireless Communications Vol.1,Issue1*. [OSI] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
3. Partha Dasgupta and Tom Boyd,[Wireless Network Security](http://cactus.eas.asu.edu/partha/Papers-PDF/2004/WirelessSecurityBoyd.pdf)*,* Annual Review of Communications, Volume 57, International Engineering Consortium.[PD]
4. Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth, SANS Institute, 2004. [IPS/IDS]
5. Seys, Stefaan, Dave Singelee, Bart Preneel. Wireless Network Security. [WNS2]\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
6. Gerald A. Marin. 2005. Network Security Basics. *IEEE Security and Privacy* 3, 6 (November 2005), 68-72. DOI=DE65FB44-50A6-4739-AAAC-64C11E07B30E <http://dx.doi.org/DE65FB44-50A6-4739-AAAC-64C11E07B30E> [NSBASICS]
7. Minho Shin; Ma, J.; Mishra, A.; Arbaugh, W.A., "Wireless Network Security and Interworking," *Proceedings of the IEEE* , vol.94, no.2, pp.455,466, Feb. 2006 doi: 10.1109/JPROC.2005.862322 keywords: {3G mobile communication;internetworking;security of data;telecommunication security;wireless LAN;3G systems;WLAN systems;communication system security;computer network security;data security;security architectures;wireless communications;wireless network security;wireless technologies;Authentication;Bandwidth;Communication system security;Computer security;Data security;Land mobile radio cellular systems;Paper technology;Wireless LAN;Wireless communication;Wireless networks;Communication system security;computer network security;data security;internetworking;land mobile radio cellular systems;wireless LAN}, URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1580513&isnumber=33381> [WNSI]
8. Saleh, Mariwan Omar. November 28, 2012. Wireless Network Security [EE] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
9. Yasir Zahur and T. Andrew Yang. 2004. Wireless LAN security and laboratory designs. *J. Comput. Sci. Coll.* 19, 3 (January 2004), 44-60. [CCSC]
10. Doshi, Bhavik. 2009. Wireless Network Security [WNS1] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
11. Tanenbaum, Andrew S, David J Wetherall. Computer Networks, 5th \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*[CN]
12. [http://technet.microsoft.com/en-us/library/cc750854.aspx[](http://technet.microsoft.com/en-us/library/cc750854.aspx%5B)PIC]

Columns on Last Page Should Be Made As Close As Possible to Equal Length

1. If necessary, you may place some address information in a footnote, or in a named section at the end of your paper. [↑](#footnote-ref-1)