Wireless Security

Survey Paper

Kevin Kuo

Department of Computer & Information Sciences

Towson University

Towson, USA

kkuo1@students.towson.edu

*Abstract*—There has been an increased demand for wireless networks due to the proliferation of laptop computers and mobile devices such as smart phones, tablets, and watches. With the development and release of new wireless devices as well as improvements in wireless technology, wireless security has been increasingly important. This survey paper will explore the improvement made to wireless security and make suggestions where future effort should be directed.

Keywords—public safety; Land Mobile Radio (LMR); FirstNet; First Responder Network; Middle Class Tax Relief and Job Creation Act (MCTRJC) of 2012; First Responder Network Authority; Quality of Service (QoS); Long Term Evolution (LTE); firewalls; Department of Homeland Security; Department of Defense; National Institute of Standards and Technology; 3rd Generational Partnership Project; hotspot; smart phones; tablets; laptops; interference; operation; security; IP security (IPsec); eNodeB; Open Systems Interconnection (OSI) model; TCP/IP; data corruption; data theft; user credential theft; Universal Integrated Circuit Card (UICC); SIM card; International Mobile Subscriber Identity (IMSI); second-generation wireless telephone technology (2G); third-generation wireless telephone technology (3G); Virtual Private Network (VPN);

# Introduction

Wireless network connections are quickly becoming the most common way to connect personal devices to the network for Internet connectivity. Wireless netowkr are a part of daily life. They are prevalent in cafes, bookstores, airports, fitness gyms, work places, restaurants, etc. We did not get to today’s implementation of wireless networks without having learned some invaluable lessons along the way. The goal of this survey paper is to research existing protocols of wireless security and how the latest standard can be improved.

# Related Work

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

# Methodology

## Open System Authentication

Open System authentication is the default authentication protocol for 802.11. It authenticates anyone requesting authentication. A client will send an authentication request to an Access Point and the Access Point responds with an authenticate response. The client then sends an Association Request to which the Access Point replies with an Association Response. The connection between the client and Access Point is then established.

### Tools – Wireshark: Wireshark is an open source multi-platform graphical user interface network traffic analysis tool that can be used to capture wireless network packets. With an open an unsecured wireless network, an actor can eavesdrop and capture all packets transmitted among clients of wireless network. Any data within those packets that is not ecrypted at the application level will appear as plaintext. For example, if a user were to log into a server using Telnet over an open wireless network connection, the username and password would be exposed and parsed by Wireshark or any other network traffic analysis utility.

## Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) protocol was an initial attempt to secure wireless network traffic. The goal was to restrict access to clients having the private, shared WEP key. The way shared key authentication works is by following this sequence of steps:

* The client sends an authentication request to the Access Point.
* The Access Point responds to the client with a 128-bit challenge text.
* The client returns the challenge text encrypted with a shared key
* The Access Point validates the encrypted response.
* The connection between the client and Access Point is established if the challenge matches.

However, WEP has a critical weakness. The Acess Point text is sent as plain text. This means that the encryption is XOR’d with the encryption stream and the known initialization vector simplifies cracking.

### Tools – Wireshark: Wireshark is an open source multi-platform graphical user interface network traffic analysis tool that can be used to capture wireless network packets. With an open an unsecured wireless network, an actor can eavesdrop and capture all packets transmitted among clients of wireless network. Any data within those packets that is not ecrypted at the application level will appear as plaintext. For example, if a user were to log into a server using Telnet over an open wireless network connection, the username and password would be exposed and parsed by Wireshark or any other network traffic analysis utility.

## Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) ...

### Tools – Wireshark: Wireshark is an open source multi-platform graphical user interface network traffic analysis tool that can be used to capture wireless network packets. With an open an unsecured wireless network, an actor can eavesdrop and capture all packets transmitted among clients of wireless network. Any data within those packets that is not ecrypted at the application level will appear as plaintext. For example, if a user were to log into a server using Telnet over an open wireless network connection, the username and password would be exposed and parsed by Wireshark or any other network traffic analysis utility.

## Wi-Fi Protected Access II

Wi-Fi Protected Access II (WPA2) ...

### Tools – Wireshark: Wireshark is an open source multi-platform graphical user interface network traffic analysis tool that can be used to capture wireless network packets. With an open an unsecured wireless network, an actor can eavesdrop and capture all packets transmitted among clients of wireless network. Any data within those packets that is not ecrypted at the application level will appear as plaintext. For example, if a user were to log into a server using Telnet over an open wireless network connection, the username and password would be exposed and parsed by Wireshark or any other network traffic analysis utility.

## Wi-Fi Protected Access-Enterprise

Wi-Fi Protected Access-Enterprise (WPA-Enterprise) ...

### Tools – Wireshark: Wireshark is an open source multi-platform graphical user interface network traffic analysis tool that can be used to capture wireless network packets. With an open an unsecured wireless network, an actor can eavesdrop and capture all packets transmitted among clients of wireless network. Any data within those packets that is not ecrypted at the application level will appear as plaintext. For example, if a user were to log into a server using Telnet over an open wireless network connection, the username and password would be exposed and parsed by Wireshark or any other network traffic analysis utility.

# Improvements

## Quality of Service (QoS)

Quality of service is needed to ensure Public Safety users have access to their mission critical services and applications at the required level of quality for individual needs. Quality of service requires discrimination in the assignment of properties such as bandwidth guarantees, usage limits, latency, accuracy, accessibility and retention.

# Conclusion

Security in Public Safety Communications is a massive challenge of integrating multiple organizations and ensuring that mission critical data remains secure. The application of existing technologies, techniques, and protocols into the First Responder network has great potential of making such mission critical data secure in an Unclassified For Official Use Only environment.

##### Acknowledgment *(Heading 5)*

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

##### References

1. “FirstNet First Responder Network Authority Guiding Principles,” *FirstNet will have effective security controls that protect data and defend against Cyber Threats.* [Online]. Available: https://www.firstnet.gov/content/firstnet-will-have-effective-security-controls-protect-data-and-defend-against-cyber-threats#Security. [Accessed: 15-May-2017].

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi TIFF or EPS file, with all fonts embedded) because, in an MSW document, this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on your frame, use the MSWord “Format” pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.

1. B. Schrier, “Band 14 in every cellular device?,” *View from the Top,* 12-Jun-2013. [Online]. Available: http://urgentcomm.com/blog/band-14-every-cellular-device. [Accessed: 15-May-2017].
2. “700 MHz Public Safety Spectrum,” *Federal Communications Commission,* 27-Jun-2016. [Online]. Available: https://www.fcc.gov/general/700-mhz-public-safety-spectrum-0. [Accessed: 15-May-2017].
3. P. Donegan, “White Paper Authentication as a Service for LTE Base Stations,” *Heavy Reading on behalf of Symantec*, May-2012. [Online]. Available: <https://www.symantec.com/content/en/us/enterprise/white_papers/heavy-reading-authentication-as-a-service_WP.en-us.pdf> [Accessed: 15-May-2017].
4. “What Is IPSec?,” *Microsoft TechNet*, 28-Mar-2003. [Online]. Available: https://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx. [Accessed: 15-May-2017].
5. “How IPSec Works,” *Microsoft TechNet*, 28-Mar-2003. [Online]. Available: https://technet.microsoft.com/en-us/library/cc759130(v=ws.10).aspx. [Accessed: 15-May-2017].
6. M. Bartock, J. Cichonski, J. Franklin, “LTE Security – How Good Is It?,” *National Institude of Standars and Technology*. [Online]. Available: <http://csrc.nist.gov/news_events/cif_2015/research/day2_research_200-250.pdf> [Accessed: 15-May-2017].
7. “SSL versus TLS – What’s the difference?,” *The LuxSci FYI Blog, LuxSci*, 19-Jul-2016. [Online]. Available: https://luxsci.com/blog/ssl-versus-tls-whats-the-difference.html. [Accessed: 15-May-2017].
8. “S/MIME for message signing and encryption,” *Microsoft TechNet*, 09-Dec-2016. [Online]. Available: https://technet.microsoft.com/en-us/library/dn626158(v=exchg.150).aspx. [Accessed: 15-May-2017].
9. “Transport Layer Security protocol,” *Microsoft TechNet*, 12-Jun-2014. [Online]. Available: https://technet.microsoft.com/en-us/library/dn786441(v=ws.11).aspx. [Accessed: 15-May-2017].
10. T. Messer, “HTTP vs. HTTPS: What's the Difference and Why Should You Care?,” *Entrepreneur*, 15-Sep-2016. [Online]. Available: https://www.entrepreneur.com/article/281633. [Accessed: 15-May-2017].
11. “AT&T Selected by FirstNet to Build and Manager America’s First nationwide Public Safety Broadband Network Dedicated to First Responders,” *AT&TNewsroom*, 30-Mar-2017. [Online]. Available: http://about.att.com/story/firstnet\_selects\_att\_to\_build\_network\_supporting\_first\_responders.html. [Accessed: 15-May-2017].
12. “Priority, Pre-emption, and Quality of Service Tutorial: LTE Basic Concepts,” *First Responder Network Authority*, 29-May-2015. [Online]. Available: https://www.firstnet.gov/newsroom/blog/priority-preemption-and-quality-service-tutorial-lte-basic-concepts. [Accessed: 15-May-2017].
13. “Priority, Pre-emption, and Quality of Service Tutorial: LTE Key Concepts,” *First Responder Network Authority*, 09-Jun-2015. [Online]. Available: https://www.firstnet.gov/newsroom/blog/priority-pre-emption-and-quality-service-tutorial-lte-key-concepts. [Accessed: 15-May-2017].