Abstract Type: Tutorial

Classification: Intermediate (Basic networking familiarity assumed)

Title: Wi-Fi. Why Try? A hands on exploration of the vulnerabilities in flawed 802.11 implementations.

Authors: Dane Brown, U.S. Naval Academy, (VT Ph.D. applicant); Christopher Anderson, Ph.D. (VT), U.S. Naval Academy; T. Owens Walker, Ph.D., U.S. Naval Academy

Address: 121 Blake Rd, Annapolis, MD 21402

Email: dabrown@usna.edu, canderso@usna.edu, owalker@usna.edu

Phone: 410-293-6168

Abstract:

As a consumer technology, Wifi is about as pervasive as one gets. Just about everyone connects to a Wifi network at home, at work, at school, or on the go. One can connect to a Wifi hotspot with a laptop, a tablet, a smart phone, a surveillance camera, or a plethora of alternate devices that benefit from interconnectivity. The fact that individuals are comfortable connecting to these various hotspots with their personal devices and sharing personal data shows there is an implicit expectation of security and privacy. Unfortunately, these two things are rarely guaranteed on a wireless network.

Average consumers would be surprised to know how insecure their wireless communications really are. Even technically savvy individuals - who know that Wifi security is severely flawed - often have never personally witnessed the ease with which these systems can be compromised. This hands-on workshop will demonstrate many of the weaknesses that exist and show how easily they can be implemented by a layman with freely available tools. Participants will perform the following on an isolated and insulated network expressly set up for demonstrating these attacks:

- Passive eavesdropping on clients within an open access point
- Reconfigure a poorly secured access point
- Setup and implement a rogue access point
- Crack the key for a WEP encrypted network and gain access to its resources
- Capture the encrypted key during a WPA2 key exchange
- Exploit the WPA2 Wifi Protected Setup flaw
- Bypass individual user privacy on a WPA2 network by performing a Man in the Middle attack

Though strong security technologies exist which solve the majority of these problems, implementations have been historically weak. This workshop will conclude with a discussion of improvements that could be made in modern implementations as well as suggestions for eliminating the weakest security link, the human. Unsophisticated users will generally choose poor encryption or no encryption and they will almost always use weak passwords. Security would be vastly improved with properly implemented device based authentication methods to connect clients to access points without burdening the user to create, memorize, and protect a long and random password.

Speaker Bios:

Dane Brown

Dane Brown is a 2005 graduate of the U.S. Naval Academy in Electrical Engineering. He received his M.S. in Electrical Engineering in 2006 from the Naval Postgraduate School. After serving as a Division Officer aboard a nuclear submarine, he returned to the U.S. Naval Academy as a military instructor in 2010. He immediately began teaching courses covering Electrical Engineering and Cyber Security. In 2012, Brown was hired as a Professor of Practice and began a new role of leading development in the new Cyber Security program at the U.S. Naval Academy.

Dane Brown's research interests include computer system design and control, communications and networking, and development and testing of secure information system hardware and software. He is a member of the National Society of Black Engineers and has received the Black Engineer of the Year Award as a Modern Day Technology leader. Brown has spoken about Cyber Security at multiple conferences and has led tutorials on the topic for diverse audiences ranging from grade school students to academic professionals. He plans to pursue a Ph.D. in the Fall of 2014.

Owens Walker

Owens Walker is a Commander in the United States Navy and an Assistant Professor. He serves as the Associate Chair in the Electrical and Computer Engineering Department of the United States Naval Academy in Annapolis, Maryland. He received his B.S. in Electrical Engineering from Cornell University in 1987 and both his M.S. and Ph.D. in Electrical Engineer degrees from the Naval Postgraduate School in 1995 and 2009, respectively. His research interests include wireless network security, wireless sensor networks, and wireless medium access. He is a member of the IEEE and Eta Kappa Nu.

Chris Anderson

Christopher R. Anderson joined the United States Naval Academy from Virginia Tech as an Assistant Professor in 2007. In 2013, he was promoted to Associate Professor of Electrical Engineering. He is the founder and current director of the Wireless Measurements Group, a focused research group that specializes in spectrum, propagation, and field strength measurements in diverse environments and at frequencies ranging from 300 MHz to over 20 GHz.

Anderson’s current research interests include radiowave propagation measurements and modeling, embedded software defined radios, dynamic spectrum sharing, and ultra wideband communications. He is a Senior Member of IEEE, has authored or co-authored over 30 refereed publications, and his research has been funded by the National Science Foundation, the Office of Naval Research, NASA, and the Federal Railroad Administration.