Hartwick College

An In-depth Analysis of Hartwick's Network Security

Is Hartwick College keeping students and staff safe online?

Nicholas Adamou

3 December 2016

An In-depth Analysis of Hartwick's Network Security:

Is Hartwick College keeping students and staff safe online?

Purpose

There are different standards for security of networks such as: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access version 2 (WPA2). Each protocol has their own unique way of authenticating a user into a network. Determining which protocol is the best choice for a particular organization can be challenging. Hartwick College has a total student body of approximately 1,550 students with 500 or so faculty members and staff, so keeping its user-base secure is a keen issue that its system and network administrators have to consider. The IT department at Hartwick College has utilized all of this knowledge to develop and provide a secure network for its student body and faculty.

Background

At Hartwick College students and staff can connect to many different wireless access points, such as "Hawks-Secure", "Hawks-Guest", "Hawks-Device", to gain access to the internet. Just like a corporation, universities have to design and develop wireless access points so that the students and staff can connect to the internet. There are a lot of aspects to consider when setting up a network, most importantly network security. "A network is defined as a group of two or more computer systems linked together" (Beal, Network). There are a plethora of network types, such as local-area networks (LANs), wide-area networks (WANs), campus-area networks (CANs), metropolitan-area networks (MANs) and home-area networks (HANs). "The main difference between these types of networks is the range they cover" (Furht). A network has three

characteristics, topology, protocol and architecture. Topology is “the geometric arrangement of a computer system” (Beal, Network). In other words, a set of computers either connected together, in a series, or to a central location of some sort. Protocol “is a set of rules that governs the communications between computers on a network” (Winkelman). Simply put, the protocol is the language used that allows the computers to communicate with each other. Architecture is the design and framework of a network. “Networks can be broadly classified as using either a peer-to-peer (P2P) or client/server architecture” (Beal, Network). P2P architecture is a type of network with which each computer or device on the network partitions tasks or workloads between other computers on the network. Client/server architecture is when certain computers are dedicated to serving others. A computer on a network is commonly called a “node” and a set of computers on a network uses the plural, “nodes”. If the computers and other devices on the network allocate their resources for the network they are called “servers”.

Wi-Fi Security Protocols

Various wireless security protocols have been developed by the Wi-Fi Alliance to protect home wireless networks. These protocols include WPA, WEP and WPA2, each has their own strengths and weaknesses. These protocols not only prevent uninvited guests from connecting to a network, they also encrypt, or conceal, private data as it is transmitted across the network so that attackers cannot eavesdrop on the data that is transmitted.

Networks are inherently insecure. “The out-of-the-box configuration for most wireless networking equipment provided easy (but insecure) access to a wireless network” (Miller). Even though the security flaws found in previous generations of Wi-Fi security protocols, wireless

networks are not as secure as wired networks. “Wired networks, at their most basic level, send data between two points, A and B, which are connected by a network cable” (Miller). Wireless networks work differently. Instead of sending data from point A to point B, they broadcast data in every direction to every Wi-Fi enabled device within the vicinity of the network.

WEP: The original Wi-Fi security standard, called Wired Equivalent Privacy (WEP), was designed to provide the same level of security as wired networks (LANs) and was defined in 802.11b. 802.11b is a standard for wireless local area networks (WLANs) that defines the data transfer speeds of the network in the 2.4GHz band. “WEP used two keys to encrypt data sent across the network, the first key is the password to the network and the second key, called an IV, was used to encrypt all data sent across the network” (Explained! Wireless Security). However, WEP had a major security flaw. Because of WEP’s use of a short IV key, over time patterns amongst IV keys emerged and computers could then decode the key through a process called password cracking. Cracking is “The process of attempting to guess or crack passwords to gain access to a computer system or network” (Beal, Password Cracking). Once the attacker gains access to the network he/she can start implementing advanced man-in-the-middle attacks.

WPA: The Wireless Protected Access (WPA) was the successor of the WEP protocol. It was introduced as a security patch over WEP. “All of the known shortcomings of WEP are addressed by WPA, which features packet-key mixing, a message integrity check, an extended initialization vector and a rekeying mechanism” (Burns). WPA provided longer encryption keys and the use of TKIP as the standard encryption protocol. TKIP improves upon WEPs’ static password, as it “regenerates its passwords for each piece of data that is sent across a network” (Explained! Wireless Security). TKIP would protect against the forging or altering of

data-packets sent across the network. However, because WPA was wrapped around the WEP security standard, it wasn't as secure as it could be. This is because, much like WEP, an attacker could use a method that is a variant of password cracking known as brute force cracking. Brute force cracking is a trial and error process used by a hacker to rapidly decode a piece of encrypted data, such as a password.

WPS: Wi-Fi Protected Setup (WPS) was "originally known as Wi-Fi Simple Config" (Chauhan). It is a standard that is used on top of WEP or WPA routers, which attempts to allow easy establishment of a secure wireless network. The entire purpose of the protocol is providing usability along with strong security. However, "In December 2011 a freelance information security researcher Stefan Viehböck reported a design and implementation flaw in WPS that makes it vulnerable to a very basic hacking technique: brute-force attacks, feasible to perform against WPS-enabled Wireless networks" (Chauhan). Using that technique, a hacker can rapidly try thousands of different combinations of the 8-digit pin associated with a WPS-enabled network until he/she lands on the right PIN. Once the attacker has the correct 8-digit PIN, he has access to the entire network and all the nodes associated with it.

WPA2: The most recent standard is the Wireless Protected Access version 2 (WPA2). The main difference between WPA and WPA2 is the fact that WPA2 uses the Advanced Encryption Standard (AES) for encryption rather than TKIP. WPA2-Personal, a variant of WPA2, features the use of a preshared key (PSK) and the use of the AES for encryption. A preshared key is the encrypted form of the password used to connect to a WPA2-Personal network. Using AES as the encryption protocol, the Wi-Fi plain-text passphrase along with the network's name (SSID) would be used to generate encryption keys for each wireless client on

the network. These keys are constantly regenerated over time. WPA2-Enterprise is another variant of WPA2. It is different than that of WPA2-Personal because it uses an external server to authenticate its user-base. This server is known as the 802.1x authenticator, which is used to validate a device that wishes to connect to the network.

802.1x Authentication: An authenticator is used to make sure something is legitimate. For example, when online shopping, the shopper wants to make sure that the remote server is actually the store, and not someone trying to pretend to be the store in order to steal valuable information. The purpose of 802.1x is to accept or reject users who want full access to a network based on a security protocol that was developed by the Institute and Electrical Electronics Engineers (IEEE) for wireless LAN technology. "802.11 specifies an over-the-air interface between a wireless client and a router or between two wireless clients" (Beal, 802.11x). There are three main components to 802.1x authentication. The first is the end-user who wishes to connect to the network. The second is the authenticator, which is like a liaison between the end-user and the server. The last component is the authentication server, which ultimately decides whether or not to accept the request to connect. 802.1x utilizes the Extensible Authentication Protocol (EAP) to facilitate the communication from the end-user to the authenticator and from the authenticator to the authentication server. EAP supports a variety of authentication methods, such as TLS, MD5, PEAP, etc. At Hartwick College, the system administrators utilize PEAP (Protected EAP) or more specifically, MS-CHAP v2, which is the most common form of PEAP in use today, to authenticate its user-base. PEAP authenticates clients using a Public Key Infrastructure (PKI) known as a certificate. PEAP is a secure form of authentication because it is a protocol that encapsulates EAP within an encrypted authenticated

Transport Layer Security (TLS) tunnel. This encrypted tunnel is used to transport the certificate to and from the authentication server ensuring that the end-user's data is secure.

An insecure Wi-Fi network poses a threat not only to the owner but to every user that connects. A network's first line of defense is its use of a strong encryption protocol, like the Advanced Encryption Standard (AES). A network utilizes its encryption protocol to encrypt all the data that is being transmitted between the Wi-Fi enabled device (tablet, smartphone, laptop) and the wireless router. The Wireless Protected Access (WPA) protocol and its successor WPA2 have replaced the less-secure and older protocol of Wired Equivalent Privacy (WEP). Many institutions have switched to WPA2 from WEP because attackers can easily gain access to a WEP network through the act of "password cracking" and "brute force cracking". Hartwick utilizes the technology of WPA2 to provide a more secure and safer environment for its students and faculty.

Types of Network Attacks

Attackers can use many different techniques to gain access to a network. These methods of attack can be prevented by creating a strong password for a network because each of these attacks takes time due to the length of the network passphrase and the security protocol used by the network. The two most common types of network hijacking is password cracking and brute force cracking. Hackers utilize the technique of network and vulnerability scanning to quickly assess a network's vulnerabilities; to see if the network is using an in-secure security protocol such as WEP or WPS. Because Hartwick uses the WPA2 security protocol for the college's

network security, the students and staff will stay protected from potential attackers eavesdropping on their data.

Password Cracking: Password cracking requires a piece of software known as a password cracker to decrypt a piece of data that contains a special algorithm known as a worm. "According to Don Seely, these algorithms have four parts: the first part, gathers password data, the second and third parts trivially break passwords that can be easily broken using" (Kizza, 73-74) the information gathered by the first part. This method was most commonly used with figuring out the master password associated with a WEP network. Because of the security enhancements of AES and WPA2, cracking the master passphrase associated with a WPA2 network is now difficult. This is because a WPA2 key contains the SSID, Service Set Identifier or network name, the length of the SSID in number of characters and the network's password.

Brute Force Cracking: The process of brute force cracking is very similar to password cracking; however, it requires an external document known as a "word-list". A word-list contains possible guesses for the password or encrypted piece of data. The document is sent through a password cracker to compare the password to each of the words in the word-list line-by-line. "This may prove to be very time consuming and also a little harder. But with time it may yield good guesses" (Kizza, 74).

Network and Vulnerability Scanning: This type of attack is commonly used to pick a target machine within a network to attack. "Scanners are programs that keep a constant electronic surveillance of a computer or a network looking for computers and network devices with vulnerabilities" (Kizza, 73). By utilizing this type of software attackers can quickly find loopholes within the various nodes on the network.

Network Security in Simpler Terms

Networks can be related to the concepts displayed in medieval technology. In essence, a network with encryption enabled is like a castle built to protect our personal belongings. Back in medieval times, in order to protect oneself from external threat, many civilizations created "technologies", such as the castle or fortress that would act as a blockade from the outside world. "The singular purpose for these … fortifications was defense. Humans needed to protect themselves by keeping attackers out" (DeVries, 172). The idea behind building a successful fortress lies in its geographical location. "Choosing a site that was in the first place geographically and physically difficult to reach and then improving those hindrances with the addition of artificial barriers" (DeVries, 172). Computer networks use a variety of tactics to keep intruders from entering. Most networks nowadays use encryption and a type of security protocol like WPA or WPA2 to tactically block invaders from entering. In medieval Europe, the tactics that civilizations used to keep attackers in check, was stone walls, as well as, a tactically placed guard tower to watch for potential attackers. "For example, the fortifications of Jericho, … consisted of an earth and stone wall. There was also a large solid tower inside the wall" (DeVries, 172) to allow archers to be on the lookout for potential attackers. "That these walls provided substantial security for Jericho's inhabitants is evident from the fact that the town itself did not fall until 1,250 BC, more than 6,000 years after the walls were constructed" (DeVries, 172). Hopefully the networks of today are able to our keep information safe.

Interview

Interviewee: Jonathan Dono - Systems Administrator at Hartwick College

Interviewer: Nicholas Adamou - Student

Can you tell me a bit about your background and how you came to work at Hartwick?

I graduated from Syracuse University with a BA in music industry with a business minor and a classical saxophone performance minor. I have 10 years of experience as the Systems and Network Administrator at Regis High School in Manhattan. I also have 4.5 years as Systems Administrator and then Manager of Network Services for AO Fox Hospital in Oneonta, as well as, almost 2 years as the Systems Manager at Hartwick College.

How does Hartwick keep students and staff safe online?

This is, obviously, a challenge and a balancing act. On the one hand, we are an institution of learning with a commitment to keeping the internet free and open to everyone. On the other hand, we need to protect our systems and information. In most cases, the biggest risk is somebody inadvertently doing something they shouldn't and bringing some form of malware onto our network (of these, Ransomware seems to be getting the most news time). In the corporate world, there is generally a web filter in place which filters all traffic in and out of the building and only allows access to specific sites. Hartwick doesn't explicitly block traffic or web sites, so that increases our vulnerability. However, we do have a "next generation" firewall which actively scans traffic for malicious code and viruses. In addition to that, we control who has access to certain things, like ACLs and firewalled networks. The hope here is that if a machine is compromised, the damaged will be limited because access from that machine is

limited. For our institutional systems we have additional security in place and they are kept in a segregated network space behind, yet more firewalls.

In certain instances, such as Google Mail, D2L, and credit card processing, we have chosen to outsource both the services and the technology to secure them.

What type of cyber-attacks can't the Hartwick Wi-Fi system protect against?

Our Wi-Fi system really only controls who can access the network via Wi-Fi. Most attacks don't occur over Wi-Fi and by far, the biggest risk to any organization are social engineering attacks (i.e. tricking somebody into giving away their credentials or they click a bad link or execute malware) and or attacks that originate from a person already within the organization.

What are the advantages and disadvantages of using WPA2-Enterprise as the security protocol for the various access points around campus? How secure is WPA2-Enterprise?

As of now, WPA2-Enterprise is the industry standard/best practice for institutional wireless networks. At this point, it's been widely used for a decade and is sufficiently difficult to crack via brute force/vulnerabilities so that in doing so is not really worth the effort. As for disadvantages, it certainly requires a lot of supporting infrastructure to work and can get complicated quickly.

What are the advantages and disadvantages of 802.1x? How secure is 802.1x?

802.1x basically provides for authentication from a backend RADIUS server and handles the communication between the access device and the server doing the authentication. Using AES and 256-bit encryption certainly makes the traffic difficult to crack. The use of the 802.1x standard is also what distinguishes WPA2-Enterprise from WPA2-PSK.

Using an authentication server allows for far greater ease of management. For example, I can disable your user account to keep you off of Hartwick's Wi-Fi and this will have zero impact on the other Wi-Fi users. This would be a nightmare with PSK. Also, modern Wi-Fi systems can now make use of features in our user database to control who gets what access. For example, you can allow students, faculty and IT staff all to connect to the same SSID using their Hartwick account. Behind the scenes, the WiFi controller can then assign access based upon active directory groups or containers that pertain to the user such that a student might get limited access whereas the IT Director would be able to access everything.

Enterprise/802.1x also improves security over PSK because every WiFi session essentially uses a randomly generated, one-time use key. Even if somebody could brute force a wireless session, they would only get access to that one user's traffic and if the user logged off and back on again, the next session would have a new key. It's important to note that cracking the wireless session wouldn't reveal the user's password as that is only transmitted in the initial startup of the session. It would be far easier and more useful for an attacker to brute force a user's password than to break WPA2-ENT encryption. Easier still, is to trick them into giving up their password.

What are the disadvantages of other security protocols, such as WEP, WPA-PSK and WPA2 WPS?

WEP uses either a 64-bit or 128-bit key that was relatively easy to crack even 10-15 years ago. First, it's a shared key and the more people who know it, the more likely it is to fall into the wrong hands. But even still, you simply had to put your Wi-Fi adapter in promiscuous mode,

download a WEP cracker from google, and capture a couple of hours' worth of Wi-Fi traffic to break it.

WPA was a huge improvement as it used 256-bit encryption. However, it was deployed largely on older WEP devices which generally had other security flaws. Basically, they plugged the vulnerabilities as they found them and eventually created WPA2 as the new standard.

PSK: The 'shared' part of the pre-shared key is the biggest weakness here. Assuming you have a strong passphrase, the pre-shared key is likely safe from a brute force attack and is perfectly fine for home use. On a corporate level, the question becomes how do you distribute one key to everyone and control access to your network if somebody leaves. Also, in this environment, an attacker with the key can now see all wireless traffic and can get onto your network.

WPS isn't really a thing in corporate environments. It's entirely for consumer grade stuff to the best of my knowledge. I haven't really looked too far into it other than to know that it's recommended that you turn it off on your home router as it has security flaws that can be exploited.

Why does WPA2 use AES as the encryption protocol rather than TKIP? What are the advantages and disadvantages of AES and TKIP?

The short answer is that TKIP is an older protocol with known vulnerabilities and it has been replaced by AES. My understanding is that TKIP (and the original WPA) was basically created as an emergency stopgap that could be deployed by firmware upgrades to older WEP devices once it was learned how easily WEP could be cracked. The only "advantage" of TKIP

was that 10 years ago, it was compatible with more devices. As of 2006 or so, everything was required to support AES, so as far as I know, there is no legitimate reason to use TKIP now.

Conclusion

By utilizing the WPA2-Enterprise security protocol along with the 802.1x authentication the IT staff at Hartwick College has provided a secure network for its student body and faculty members. Although the technology provides safeguards, wireless networks are inherently insecure. For the students and staff at Hartwick College, routine searches and other uses of the network are safe. However, depending on the websites that people access and their password strength, there are always risks for security breaches. Just as the concepts of castle "technology" have evolved into wireless home security programs (e.g. ADT), network security will evolve as well. As technology and devices continue to develop, so too will the people that are developing the networks to keep their user-base secure for all those who use them.

Works Cited

Beal, Vangie.

"802.11x" *What is 802.11x? Webopedia Definition,* Webopedia, www.webopedia.com/TERM/8/802_11x.html.

"Password Cracking." *What is Password Cracking? Webopedia Definition*, Webopedia, www.webopedia.com/TERM/P/password_cracking.html.

"Network." *What is a Network? Webopedia Definition*, Webopedia, www.webopedia.com/TERM/N/network.html.

Burns, Jim.

"How 802.1x Authentication Works." *Computerworld*, Computerworld, 3 Apr. 2003, www.computerworld.com/article/2581074/mobile-wireless/how-802-1x-authentication-works.html.

Chauhan, Sudhanshu.

"Wi-Fi Security: The Rise and Fall of WPS." *InfoSec Resources WiFi Security The Rise and Fall of WPS*, InfoSec Institute, resources.infosecinstitute.com/wi-fi-security-wps/.

DeVries, Kelly Robert.

Medieval Military Technology. Peterborough, Ont., Broadview Press, 1992, pp. 172.

"Explained! Wireless Security".

director. JackkTutorials, 27 Nov. 2016, www.youtube.com/watch?v=mMdlD_fHzTg.

Furht, Borivoje, and Mohammad Ilyas.

Wireless Internet Handbook: Technologies, Standards, and Applications. Boca Raton, FL, CRC Press, 2003.

Kizza, Joseph Migga.

Computer Network Security and Cyber Ethics. Jefferson, NC, McFarland, 2002, pp. 73-74.

Miller, Lawrence C.

"*Wireless Security Protocols: WEP, WPA, and WPA2*." *Dummies*, www.dummies.com/computers/computer-networking/wireless/wireless-security-protocols-wep-wpa-and-wpa2/.

Winkelman, Roy.

"Chapter 2: Protocol." *Chapter 2: Protocol*, Florida Center for Instructional Technology College of Education, University of South Florida, fcit.usf.edu/network/chap2/chap2.htm.