Aug 10th, 12:00 AM

VPN Usage in Higher Education: A Study to Mitigate Risk Related to Public Wi-Fi Usage

Deanna House
University of Nebraska at Omaha, deannahouse@unomaha.edu

Emil Radu
University of Tampa, eradu@ut.edu

VPN Usage in Higher Education: A Study to Mitigate Risk Related to Public Wi-Fi Usage

Emergent Research Forum (ERF)

Deanna House
University of Nebraska Omaha
deannahouse@unomaha.edu

Emil Radu
University of Tampa
eradu@ut.edu

Abstract

Higher education settings have unique security risks in that they traditionally do not have robust security programs. Higher education network infrastructure can be outdated and resources for information security limited. These challenges are met with frequent faculty and staff travel for conferences and recruiting events in other states and countries. Frequent travel can leave university and faculty information and assets at risk; particularly when faculty and staff use public Wi-Fi in areas such as hotels, conference venues, coffee shops, and airports. Data in higher education institutions can be leaked when sent over channels that are not secure. This emergent research explores virtual private network (VPN) usage in a university setting using employer-issued devices. Emphasis is placed on VPN usage when using public Wi-Fi. The research focuses on the importance of risk to the university and its researchers as an influence on VPN usage behavior.

Keywords

VPN, higher education, security, public Wi-Fi, proprietary research risks

Introduction

Universities have an open policy related to the sharing of knowledge between students, faculty, and among other universities (NCSC Warning, 2019). This is paired with the common knowledge that security controls at most schools and universities are not as rigorous and controlled as those in outside organizations (Foster, 2004; Leckrone, 2020). For example, a study by Aarthy, Mohan, & Sethumadhavan (2017) explored vulnerabilities in educational institutions due to lack of wireless security audits, which can increase the risk of data leakage and exfiltration. In addition, universities have a variety of data, including financial, health, proprietary, and research data, which can make them vulnerable (Bongiovanni, 2019).

The combination of open sharing, vast amounts of data, and unsecure environments can result in targeted attacks against universities. It is estimated the overall cost of spam to academia is $2.6 billion annually (Baker, 2020) which can put a strain on resources from both a budgetary and incident response cost perspective. In addition, many of the security requirements that are possible in public and private companies are not possible to adhere to in a university setting due to resource constraints and limitations related to academic freedom (Aberbach & Christensen, 2018). It is also troubling that according to the KnowBe4 Phishing by Industry 2020 Benchmarking Report, education is second most at risk industry across small organizations (KnowBe4, 2020).

Cyber-attacks on higher education institutions can be initiated by various threat agents such as hackers, hacktivists, foreign governments, or even students. The motivation can be for financial or notoriety reasons. But more seriously, the motivation can be for disruption of the activities of the institution or nation-state, for espionage, for stealing of research/findings, stealing of intellectual property, or for stealing student and faculty personal information. For example, nine Iranian nationals were indicted for coordinating a massive cyber-intrusion beginning in 2013 in 144 universities based in the United States and approximately 176 universities in other countries. They specifically targeted academic data and intellectual property and

obtained nearly 31.5 terabytes of data. (United States of America vs. Gholamreza Rafatnejad, Ehsan Mohammadi, Abdollah Karima, Mostafa Sadeghi, Seyed Ali Mirkarimi, Mohammed Reza Sabahi, Roozbeh Sabahi, Abuzar Gohari Moqadam, and Sajjad Tahmasebi, 2016). Nation-state attacks such as these are harmful not only to the universities and higher education, but also to the researchers. An important considerations for a successful security program is to create synthesis between behavior at work and behavioral at home which can shift the perspective to emphasize the benefits of robust cybersecurity hygiene (Rayome, 2017).

Challenges of Public Wi-Fi

Public Wi-Fi is a wireless network that is set-up by a public or private organization, a city, or even an airport that allows individuals to connect in order to receive Internet access. Many individuals travelling have a need to rely on public Wi-Fi (Sombatruang, Onwuzurike, Sasse, & Baddeley, 2019). Data can be leaked that is not encrypted through a Virtual Private Network (VPN) putting the university at risk (Consolvo, Jung, Greenstein, Powledge, Maganis, & Avrahami, 2010). This could include sensitive information such as sites visited and cookie information (Sombatruang, Onwuzurike, Sasse, & Baddeley, 2016).

In addition, public Wi-Fi networks are not always trusted networks (Molina, Gambino, & Sundar, 2019; Sombatruang et al., 2019). When unencrypted information is transmitted, is it possible for others on the network to potentially view those transmissions (Klasnja, Consolvo, Jung, Greensten, LeGrand, Powledge, & Wetherall, 2009). It is very easy to set up a rogue access point or conduct a man-in-the-middle attack to intercept communications between the endpoint of the user and the wireless access point. Even if the user is accessing a browser using a secure communication (https), information related to pages browsed can easily be intercepted by someone with malicious intent.

Prevention Mechanisms Related to VPN

A secure way to protect users from data leakage is to utilize a VPN. A VPN ensures a secure/encrypted communication that provides security through an encrypted tunnel. A VPN works by routing your device's internet connection through your chosen VPN's private server rather than your internet service provider (ISP) so that when your data is transmitted to the internet, it comes from the VPN rather than your computer. The VPN acts as an intermediary of sorts as you connect to the internet, thereby hiding your IP address – the string of numbers your ISP assigns your device – and protecting your identity. Furthermore, if your data is somehow intercepted, it will be unreadable until it reaches its final destination.

Encryption hides information in such a way (basically transforming it to gibberish) that it cannot be read without a very strong password, which is known as a key. This key essentially breaks the complicated code that your data has been turned into. Only your computer and the VPN server know this key. The process of decoding your data is known as decryption, which is the process of making encrypted information readable again through the application of the key.

Using VPN is a necessity when connecting to public Wi-Fi. This mitigation strategy provides an organization with a working solution, provided that its users utilize it. It is important for organizations, including universities to enforce the use of VPN while also communicating the risks to the organization when a device is connected on public Wi-Fi (Sombatruang et al., 2016). It is also necessary to use an approved VPN service, as research by Ikram, Vallina-Rodriguez, Seneviratne, Kaafar, & Paxson (2016) found that several VPN apps were exposing users to serious vulnerabilities such as data leakage and traffic redirection. The use of a VPN can be perceived by users as difficult without the proper training (Molina et al., 2019). We seek to address these challenges by emphasizing the benefits of VPN and the risks of not using VPN for university faculty and staff while utilizing public Wi-Fi.

Methodology

The research study is conducted in a university setting to determine if the communication and emphasis of risks to the university have an influence on behavior related to VPN usage. Data was collected on the use of VPN prior to the beginning of the study. The high risk subjects such as those that transmit financial data were selected first. The study is set up so that participants sit through a training session that discusses how and when to use VPN. Emphasis is placed on the usage of VPN while away from the office and while using public Wi-Fi. Additionally risks related to information and privacy leakage are presented in the context of the university and at the individual level. A longitudinal survey is conducted to determine the pre and post intended use of VPN while using public Wi-Fi. Tracking is conducted on the VPN software side to determine if actual usage increases as a result of the training campaign.

It should be noted that initial data was collected for a baseline, prior to beginning the training and prior to the onset of COVID-19, which will be discussed below. Baseline data indicates that on average, only 30 users were on VPN a day, with the majority of users in the Information Technology and Security department.

Limitations

This research was conducted in a private university in the southern United States. It is possible that policies in private university higher education settings differ from those of public universities. In addition, the research was initiated to gain baseline data prior to the onset of the COVID-19 pandemic. The research was conducted during the pandemic, when remote access policies and communications were being emphasized in all fields and industries.

While the higher education institution in the study provided limited communications related to secure practices, the emphasis of VPN use was not highlighted outside of this study. The researchers were fortunate that they were able to maintain a study that was free of bias that could have been introduced by such communications. Also, it should be noted that there was a change in VPN software at the beginning of the study. This provided a more robust VPN platform to gather usage information from but did not change the functionality on the user side.

Conclusion

Research related to information security management and information security culture in higher education have gaps that should be addressed (Bongiovanni, 2019). This research provides a contribution to the field by exploring VPN usage as a mitigation to risk in higher education. A study by Sombatruang et al. (2019) found that perceived risks related to using unsecured Wi-Fi networks did not deter users from utilizing them. However, a university is a unique setting that has both a frequency of the need to use public Wi-Fi paired with an environment of many researchers that have proprietary data.

This study focuses on providing faculty and staff with the mechanisms to secure their connections when using public Wi-Fi. This risk mitigation strategy is easily implemented using existing VPN software. Universities need to secure one of the most important assets, the research. While there have not been numerous incidents involving university data breaches, when compared to other industries, it is important to proactively work to set up secure practices while connecting to public Wi-Fi. Evolving threats are continuing to present institutions with new challenges while they still struggle to solve old ones. Research such as this can help provide insights related to measures that can be implemented to maintain the intellectual property of our higher education institutions.

REFERENCES

Aarthy, D.A., Mohan, A.K. & Sethumadhavan, M. 2017. "Wireless Security Auditing: Attack Vectors and Mitigation Strategies", *7th International Conference on Advances in Computing & Communications, ICACC,* August 22 – 24, Cochin, India.

Aberbach, J.D. & Christensen, T. (2018). "Academic Autonomy and Freedom Under Pressure: Severely Limited, or Alive and Kicking?" *Public Organization Review,* 18:4, pp. 487-506.

Baker, S. 2020. "Dealing with Spam Emails Costs Academia More Than Peer Review", *Times Higher Education*. Retrieved April 20, 2020 from https://www.timeshighereducation.com/news/dealing-spam-emails-costs-academia-more-peer-review.

Bongiovanni, I. 2019. "The Least Secure Places in the Universe? A Systematic Literature Review on Information Security Management in Higher Education", 86, pp. 350 – 357.

Consolvo, S., Jung, J., Greenstein, B., Powledge, P., Maganis, G., & Avrahami, D. 2010. "The Wi-Fi Privacy Ticker: Improving Awareness & Control of Personal Information Exposure on Wi-Fi", *UbiComp '10,* September 26 – 29, Copenhagen, Denmark.

Foster, A.L. 2004. "Insecure and Unaware: An Analysis of Campus Networks Reveals Gaps in Security", *The Chronicle of Higher Education*. Retrieved April 20, 2020 from https://www.chronicle.com/article/InsecureUnaware/11671.

Ikram, M., Vallina-Rodriguez, N., Seneviratne, S., Kaafar, M.A., & Paxson, V. 2016. "AN Analysis of the Privacy and Security Risks of Android VPN Permission-Enabled Apps", *IMC 2016,* November 14 – 16, 2016, Santa Monica, CA.

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B.M., LeGrand, L., Powledge, P., & Wetherall, D. 2009. "When I Am On Wi-Fi, I Am Fearless: Privacy Concerns & Practices in Everyday Wi-Fi Use", CHI 2009, April 4-9, Boston, MA.

KnowBe4. 2020. "KnowBe4 Phishing by Industry 2020 Benchmarking Report". Retrieved April 20, 2020 from https://www.knowbe4.com/hubfs/2020PhishingByIndustryBenchmarkingReport.pdf.

Leckrone, B. 2020. "Why Colleges Are Ripe Targets for Cyberattacks – and How They Can Protect Themselves", The *Chronicle of Higher Education*. Retrieved April 20, 2020 from https://www.chronicle.com/article/Why-Colleges-Are-Ripe-Targets/248012.

Molina, M.D., Gambino, A., & Sundar, S.S. 2019. "Online Privacy in Public Places: How Do Location, Terms and Conditions, and VPN Influence Disclosure?", *in CHI 2019, May 4 – 9, Glasgow, Scotland UK.*

NCSC Warns UK Universities of Cyberthreats. 2019. *Network Security Newsletter,* 10, pp. 1-2.

Rayome, A.D. 2017. "How to Make Your Employees Care About Cybersecurity: 10 Tips", *Tech Republic*. Retrieved April 20, 2020 from https://www.techrepublic.com/article/how-to-make-your-employees-care-about-cybersecurity-10-tips/.

Sombatruang, N., Onwuzurike, L., Sasse, M.A., & Baddeley, M. 2016. "Why Do People Use Unsecure Public Wi-Fi? An Investigation of Behaviour and Factors Driving Decisions", *STAST '16,* December 5-6, Los Angeles, CA.

Sombatruang, N., Onwuzurike, L., Sasse, M.A., & Baddeley, M. 2019. "Factors Influencing Users to Use Unsecured Wi-Fi Networks: Evidence in the Wild", in *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19),* May 15 – 17, Miami, FL.

United States of America vs. Gholamreza Rafatnejad, Ehsan Mohammadi, Abdollah Karima, Mostafa Sadeghi, Seyed Ali Mirkarimi, Mohammed Reza Sabahi, Roozbeh Sabahi, Abuzar Gohari Moqadam, and Sajjad Tahmasebi. 18 CRIM 94. (2016). Retrieved April 20, 2020 from https://www.justice.gov/usao-sdny/press-release/file/1045781/download.