**Unit 9 Encryption and Security Overview**

Corey Crooks

Purdue University Global

IT331-01

Ahmed Banafa

January 18, 2023

There are many threats that plague the various cybersecurity platforms in today’s market. Namely, these threats are organized into the categories of internal and external. Although there are countless different kinds of threats to be aware of—and new ones being developed every hour of every day—this system seems to classify the applicable threats fairly well (Dungan, 2019). Internal threats are as they sound; these are threats that originate inside your local network. These could be anything from a lack of information and education for your employees that causes a system failure, or even an employee that trades confidential information about your systems to a competitor, or malicious party. External threats are those that make their way into your network while originating from the outside. Common examples of this may include things like a ransomware attack, SQL injection, or even an exploit of a Zero Day vulnerability. Although neither of these threat classifications have “solutions” to them that will prevent all risks for all time, there are steps a business could take in order to mitigate the risks associated with each. Insider threats tend to be the most straight-forward and simpler approach to mitigating risks. The world of external threats is ever expanding with different disciplines, opportunities, and attack patterns. While complicated management systems like Honey Pots have been made to try and distract attackers, internal threats are much easier to diagnose (Cybersecurity and Infrastructure Security Agency, n.d.). Simply put, what it comes down to is the discipline of each of your employees. Should an employee grow disgruntled, and have major issues with your business, the risk of an internal threat grows more and more. Additionally, should an employee feel valued, respected, and educated on the cybersecurity risks they may interact with, the employee will be significantly less likely to sell trade secrets, or accidently download a keylogger. For this reason and more, it is especially important to have a written security policy. With a written policy, employees can reference it at any point in their daily work to be able to modify their approach to their work and research to conform with the policy. Additionally, should a security failure occur, your business is less likely to be the basis of legal action due to improper security placements, or more likely to be able to hold the individual responsible to account.

Many tools exist to help individuals of various dependencies to operate discretely and with a high degree of security. These tools operate using different forms of encryption. One of these tools is a highly popular messaging platform called Pretty Good Privacy (PGP). Using a Public, a user is able to send encrypted files to a destination. The destination then has a private key that will turn the encrypted file into something the destination will use, such as a scramble of ASCII values to readable text (Raicea, 2017). This is a relatively optimal solution to this problem, as the redundancies in this transaction are eliminated, thus reducing vulnerability. For example, the sending client does not need to un-scramble the data being sent after the package is transmitted, and the receiving file does not need to re-scramble the data being received after de-coding. By eliminating these redundancies, should a key-breach occur the malicious force does not have access to the other’s job and will need to steal both keys in order to have a complete transcription for the entire message stream. This differs from Kerberos Cryptography in that Kerberos only uses conventional cryptography with no public keys.

All this being said, the wireless communications market is quite a volatile platform. Malicious actors are everywhere while novice users are vulnerable. For this reason, it is important to look at the two main ways to secure your data. Firstly, Data encryption is a technical implementation to secure your data in the event of an interception to ensure that the intercepted package is as useless as possible to the malicious actor (Wong, 2023). Using various techniques, encryption will scramble the data in a message or file, and then un-scramble it upon arriving at the intended destination. This way, should the data be intercepted in the process, the thief will only have the scrambled data, and must work to un-scramble it if that is at all possible. User authentication takes a different approach to this problem (Wong, 2023). Most commonly, a user will have a series of credentials like a username and password that ideally only they would know. They would then give those credentials at an authentication page, and be allowed access to their account or information. Although this approach is theoretically less secure than something like encryption algorithms, it also is evolving overtime and has been more user-friendly to novice online individuals that do not have the technical background to set up PGP or understand what encryption algorithms are. This goes a step further with Wi-Fi algorithms (Wong, 2023). In 1997, WEP protocols were introduced in wireless transmissions. Although this was marginally better than no security at all, it gave rise to WPA in 2003. This sought to address weaknesses in WEP by adding an encryption layer by the name of Temporal Key Integrity Protocol. This was optimized further in 2004 with the introduction of WPA2 by addressing TKIP’s protocol with weak passwords. WPA2 is today’s standard on wireless networks, and is widely adopted due to its backwards compatibility to WPA. That is not to say that your data is completely safe on a Wi-Fi hotspot. Due to Wi-Fi security operating on OSI Model Layer 2 and above, they cannot protect against any type of attack on the physical layer (Arana, 2006). This is the primary vulnerability for any Wi-Fi security standard, as they all share this weakness.

# **References**

Arana, P. (2006). *Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)*. Retrieved from INFS 612-Fall 2006: https://cs.gmu.edu/~yhwang1/INFS612/Sample\_Projects/Fall\_06\_GPN\_6\_Final\_Report.pdf

Cybersecurity and Infrastructure Security Agency. (n.d.). *Insider Threat Mitigation Resources*. Retrieved from cisa.gov: https://www.cisa.gov/insider-threat-mitigation-resources

Dungan, L. (2019, August 20). *Organizational Cybersecurity Threats - External vs Internal*. Retrieved from captechu.edu: https://www.captechu.edu/blog/organizational-cybersecurity-threats-external-vs-internal

Raicea, R. (2017, October 8). *How Pretty Good Privacy Works, and how you can use it for Secure Communication*. Retrieved from freecodecamp.org: https://www.freecodecamp.org/news/how-does-pretty-good-privacy-work-3f5f75ecea97/

Wong, C. (2023). *Protecting your Wireless Communication*. Retrieved from cityu.edu.hk: https://www.cityu.edu.hk/csc/netcomp/dec2009-2.htm#:~:text=Data%20encryption%20and%20user%20authentication,access%20to%20the%20wireless%20network.