Levi Seibert

00086809

lseiber1@my.athens.edu

ITE 523

Securing Cyberspace

Cyberspace refers to the great unknown. No, not the final frontier. Rather, the hidden world that nearly everyone uses on a consistent basis, but very few truly understand. Cyberspace is the interconnected world that nearly everyone has access to with their fingertips. It is the network-connected, Internet-worked world. The space that connects your smartphone to a web server in Bangkok, a digital library in Ontario, and an online forum of computer scientists in California.

Different authors and researchers have different ideas of what cyberspace actually is. This maybe because the Internet rapidly grew out of obscurity and few people fully understand what it is. In a period of 60 years, this perplexing network grew from a military and university research tool into a necessary part of the public's life. The World Wide Web is incredibly complex, and many people just don't comprehend the reality of what cyberspace is. In addition, many researchers have different points of view when considering cyberspace. A fry cook at McDonald's will more than likely have a different understanding of the Internet-world than a Computer Scientist at Michigan Institute of Technology.

Regardless of how it is defined by the user, cyberspace has evolved to become a necessary part of our lives. Who could imagine a world without social media, without electronic mail, or without access to the world of information known as the World Wide Web? With all the billions of Internet communications that occur every day across the globe, a plethora of information is shared across the wires. Without any forms of protection, this data is freely available to the curious observer, as well as the malicious hacker.

Thankfully, cryptography has been developed to keep our cyber data private and secure. Cryptography is a method of "hiding" information from observers. It is a method of obfuscating data by manipulating it in some fashion to make it hard (preferably impossible) to decipher. Cryptography is not solely a cyberspace concept, rather it has its origins thousands of years before the idea of cyberspace was on anyone's mind. In fact, Julius Caesar is well-known for his Caesar Cipher, a method of "encryption" that just shifted letters in a message by a predetermined number of places. For example, if a 3-shift was implemented (as was common in Caesar's days), the letter 'A' becomes 'D', 'B' becomes 'E', and so on. Today, algorithms like this are naïve, and pointless, as anyone can decrypt the cipher text (a message that has been encrypted with little to no effort).

As the years have progressed and cyberspace has become a standard resource, the need for "real" encryption algorithms has become a necessity. Cryptography is used in other ways, such as protecting files on computers and securing passwords, yet cyber-cryptography may

present itself as its most important application. Data travelling across the Internet has great potential of causing major issues. Now, rather than just shifting around letters, true obfuscating takes place. In its basic sense, cryptography starts with a plaintext message, which is just the message that is awaiting encryption. To that plaintext, an initialization vector is applied, which randomizes the beginning of the process to a certain extent. Next, an encryption algorithm is applied with a secret key. After this mathematical algorithm is applied to the plaintext, the message is encrypted, and the plaintext has now been transformed to the ciphertext.

Cryptography does not rely cyberspace, as it is a concept that is larger than the cyber world. It can be used to encrypt messages that never go near a network wire. However, in today's cyberspace relies on cryptography in order to be most effective. An unprotected network is a privacy-free network.

There are two main methods of cryptography, symmetric and asymmetric. Symmetric is considerably simpler, but does have its downsides. In symmetric cryptography, both the sender and receiver have the same key. The sender encrypts the plaintext using the shared key, and the receiver decrypts the message using the same key. The biggest problem with this method is that for every unique entity that a sender communicates with, he needs a separate key, known only to that receiver. Exchanging keys must also be done out-of-bounds, that is, it can not take place over a unsecured network (if it does, then an attacker could access the key and then decrypt any future messages). Symmetric encryption is also not scalable. Examples of symmetric cryptography include AES and 3DES.

Asymmetric encryption is a bit more complicated, but it does handle the issues that exist within symmetric encryption. In asymmetric encryption, every entity has a private and a public key. The public key is just that, public. It is well-known what someone's public key is. This may sound concerning and dangerous, but it is completely safe and is the backbone of what makes asymmetric encryption actually work. The private key must be kept 100% private, not even the other party in a communication can know what it is. The public and private keys are mathematically related so that something encrypted by one of the keys can only be decrypted by the other. In its normal form, a sender will encrypt the message using the receiver's public key (remember that this key is well-known). Because the receiver's public and private keys are related, only his private key can decrypt the ciphertext that was created by the sender. Because there is no key exchange taking place, the algorithm is scalable and does not have the same issues that symmetric encryption does. In addition, asymmetric cryptography can provide for authentication, integrity, and non-repudiation, if executed properly.

Regardless of the method and algorithm selected, encryption has become a necessary part of cyberspace. It is simply not smart to use the Web without having some form of cryptography protecting your data. This is why HTTPS (HyperText Transfer Protocol Secure) has become so common, it is an improvement upon the antiquated HTTP protocol in that it adds a level of cryptographic security that keeps users safe as their browse the Web and perform their online activities. In addition, email messages can be encrypted in order to protect the privacy (and provide authentication) for users. Both email encryption and HTTP are examples of how

cryptography better protects the cyberspace, making the “great unknown” at least a little bit safer.