Encryption Lecture

By Marilyn Washington

Cybercrime Techniques and Response – CIS 552

Dr. JodineBurchell

April 20, 2015

Strayer University

Introduction

Cryptography is the art of protecting data that is transmitted from system to system. It provides users the ability to protect personal information. There are two types of cryptography symmetric or asymmetric (So you think the Government Can’t Regulate Internet Gambling…(n.d.). Symmetric Systemuses a secret key, such as the DES and AES algorithms. They are s both used by the sender and receiver to encrypt and decrypt the information. Symmetric is the faster of the two options, however getting the secret key to the recipient sometimes can be a problem(Koved, Nadalin, Nagaratnam, & Pistoia, 2004). Asymmetric System is the second methodthat uses a two key process, the first key is the public key open for all to view, and the second key is the private key available for only the message recipient. The keys are used to encrypt and decrypt information transferred from one person to the next (CARD\_RSA\_DECRYPT\_INFO Structure (Windows) (n.d.)). Encryption can be in the form of files, directories, disk drive or emails (Koved, Nadalin, Nagaratnam, & Pistoia, 2004).

Encryption Lecture

# Explain, in your own words, the purpose of cryptography and take a position on whether or not you believe encryption is sufficiently utilized in organizations today. Provide a rationale with your response.

Cryptography is the science of securing data; it transmits data in a secure manner by using one of the preferred methods symmetric or asymmetric(InfoSec Baselines - All.Net. (n.d.)). Each method it enables organizationsto have ability to storesensitive information, and transferring the information across unsecured networks. The process converts readable information to an unreadable form to anyone except the intended receiver(Koved, Nadalin, Nagaratnam, & Pistoia, 2004).

When the data is in its standard form, it is called plaintext, and its unreadable form is called ciphertext. The data is only readable by a person with the decoding keythat is provided by the sender. The key converts the ciphertext message back into its original form(Koved, Nadalin, Nagaratnam, & Pistoia, 2004). In order for this process to be successful the originator of a coded message provides the decoding key to the intended receiver(s) of the message. However, if the key is intercepted by unauthorized personnel, the security is then compromisedbecause the message can now be converted by an unknown recipient(Koved, Nadalin, Nagaratnam, & Pistoia, 2004).

Today's' organization are not taking full advantage of utilizing encryption of the information that should be protected. By recalling the multiple incidents that have occurred just within the this year pertaining to personal information being stolen from organizations like; OPM, Home Depot, Target, Neiman Marcus, Michaels Storesor other organization that have not reported their incident, or are yet to discover it has occurred. There is no system is 100% secure, however by adding encryption protection to the all data files adds an extra layer of security if at any time attackers attempt to compromise the organization(GoLocalProv News Team, 2014).

# Describe the differences between symmetric and asymmetric encryption.

Encryption can come in two different forms symmetric and asymmetric. When unitizing symmetric encryption system or algorithms, one encryption key is used to encrypt and decrypt the traffic and shared between both parties involved. The key is to be kept secret to provide privacy, which means that each user will own a copy of the symmetric secret key. If the key(s) are not protected and somehow compromised the information is no longer be considered protected(Garloff, 2000).

Symmetric encryption is considered to be extremely fast and provides relatively little complexity that allows for smooth implementation. However, symmetric requires that the systems involved with encryption process have already been configured with the secret key. Another advantage of symmetric encryption is that it does not consume a lot of computing power. An example of symmetric algorithms include DES, Triple-DES (3DES), IDEA, CAST5, BLOWFISH, and TWOFISH(Garloff, 2000).

Asymmetric encryption or algorithms require the use of a pair of keys. As it can be imagined one key is used for encryption and the other for decryption. The decryption key is kept secret, called private key or secret key. The encryption key is then shared with anyone who might need to send encrypted messages, called public key. Whoever has the public key can send encrypted messages to the owner of the secret key(Garloff, 2000). The secret key cannot be reconstructed from the public key. Asymmetric algorithms are said to be ideally suited for real-world use, mainly because the secret key does not need to be shared, which reduces the risk of being compromised, and each user is only required to protect one secret key. Examples of asymmetric algorithms areRSA, DSA, and ELGAMAL(Garloff, 2000).

The asymmetric algorithm process is much slower than the symmetric process, and many of the system applications use a combination of both symmetric and asymmetric. The asymmetric key(s) are used for the authentication, once completed, one or a combination of symmetric keys are generated and exchanged using the asymmetric encryption process, using both algorithms. Examples of this procedure areRSA/IDEA, a combination of PGP2 or the DSA/BLOWFISH used by GnuPG(Garloff, 2000).

# Select the encryption method you believe is typically more reliable of the two and explain why. Determine if there are any situations where the typically less reliable method could be the better option.

The asymmetric encryption, the process is considered a more reliable option than Symmetric encryption. Asymmetric ciphers are used when transferring session keys for symmetric ciphers. When a little amount of information is transferred, cryptographers send encrypted data with a symmetric cipher andsend the decrypt key with an asymmetric cipher. Asymmetric encryption can also be used for digital signatures, even thought symmetric encryption can be used for message authenticity it cannot provide non-reputable signatures(Garloff, 2000).

The downside of asymmetric algorithms; it requires at least a 3,000-bit key for the same level of security provided by a symmetric 128-bit key. Asymmetric algorithms are slow and may not be the best suited to encrypt large amounts of data. Because of this reason they are often used together, the public-key algorithm preferred to encrypt a randomly generated encryption key, and the random key is preferred to encrypt the message using a symmetric algorithm. This process is called hybrid encryption(Hirsh, 2013).

Select one (1) of the common cryptographic systems and justify why you believe it to be the best encryption technology to date.

The one common used cryptography system is Pretty Good Privacy (PGP). PGP is a computer program that provides cryptographic privacy and authentication, as well as data encryption and decryption for data communication. PGP is a hybrid cryptosystem; it combines features from both conventional and public key cryptography(pgpi.org, 2014). PGP provides the benefit of public key cryptography that allows people with no security training to secure messages. It allows them to encrypt and decrypt files, directories, and disk partitions, along with signing, encrypting, and decrypting texts, e-mails, for the security of e-mail communications(pgpi.org, 2014).

PGP encryptions work by compressing plaintext data, the compressed data reduces transmission time, disk space and strengthens cryptographic security. By compressing the data, it reduces the chances of plaintext of exploitation techniques used by cryptanalysis(pgpi.org, 2014). PGP creates a one-time-only secret session key, which is randomly generated with the use of the mouse and keyboard. The session key is used with a secure encryption algorithm to encrypt the plaintext; the result is ciphertext. After encrypted, the session key is encrypted with the recipient's public key. The key is transmitted to the recipient along with the ciphertext. The decryption process will work in reverse(pgpi.org, 2014).

PGP is the best encryption to date because it provides a means for users to send messages confidentially, supports message authentication and integrity checking, and secures files, directories, and hard drives. PGP compatibility allows it to work with other cryptography systems. There had been no known method produced that has allowed a person or group to break PGP encryption by cryptographic or computational means(pgpi.org, 2014).

Describe the common uses of the aforementioned selected cryptographic system and provide a real-world example of how it is used in securing networks, files, and / or communications in the present day.

The National Security Agency (NSA) has pointed out that more and people have the means of securing e-mail transition but are not using the tool. Society has chosen convenience, usability and user-friendly tools for communications over their cryptographically secure competitors with features that would be difficult to implement in an NSA-proof fashion. In most cases, modern online services do us some encryption method commonlySSL. SSL only protects the data moving between the devices and servers operated by Google, Apple, and Microsoft, which have access to unencrypted copies of user's data(Lee, 2013).

This problem can be avoided with end-to-end encryption, the messages sent from the user through Google or Microsoft will only see the encrypted version. PGP is one of the software tools that enable e-mail encryption and secure instant messaging. Installing PGP can be a hassle that causes people to resist using it(Lee, 2013). Remember Edward Snowden the person who leaked NSA PRISM program, his fist contact was Glenn Greenwald, according to the Washington Post, Snowden asked the journalist to install PGP on his computer in order for them to communicate securely. Snowden provided Greenwald with step-by-step directions for setting up the software(Lee, 2013).

However, Greenwald did not know the significance of Snowden's leaks and did not install PGP until late March when Laura Poitras, who Snowden had also contacted, informed him of the importance of the information. PGP is strong cryptographic software that whistleblowers, dissidents, criminals and governments use it every day(Lee, 2013).

# Create a network diagram of a network and / or in a data flow where your real-world example would exist using a diagramming application such as Visio or Dia.

# 

# Analyze current cryptographic attacks that are used in the present day and determine how they can be a detriment to the security where encryption is implemented.

Hackers today use various types of attacks that are the result of organized groups, many of which are professional. Most of the cyber attacks are designed to weaken the security of any network (Grimes, 2012). Some of the attacks include but limited to:

* **Cyber crime syndicates -** mostly organized cyber crime syndicates are businesses that lead large affiliate conglomerate groups.
* **Hacktivists - p**olitically motivated hackers is the new form of political activism.
* **Intellectual property theft and corporate espionage -** method of breaking into a company's IT assets, dump all the passwords, and over time, steal gigabytes of confidential information.
* **Botnets as a service - a**malware program that creates the bot, today's owners will either use the botnet for themselves or rent it to others by the hour or another metric.
* **All-in-one malware -** malware programs that will not only infect the end-user but also break into websites and modify them to help affect more victims.
* **The increasingly compromised Web -** the attacker finds a weakness or vulnerability in a website that allows them to bypass admin authentication and write malicious scripts.

With each of the above attacks, encryption should be in place throughout the network. The attackers will attempt to access the network in many different ways, applying an encryption system to combat these types of attacks, requires a team of IT security professionals monitoring, scanning and analyzing network traffic 24/7 (Grimes, 2012).

# References

CARD\_RSA\_DECRYPT\_INFO Structure (Windows). (n.d.). Retrieved from <https://msdn.microsoft.com/en-us/library/dd627634(v=vs.85).aspx>

Garloff, K. (2000, Aug 28). *Symmetric vs. asymmetric algorithms*. Retrieved from http://users.suse.com/~garloff/Writings/mutt\_gpg/node3.html.

GoLocalProv News Team. (2014, Feb 06). *10 Big Companies with Recent Major Security Breaches*. Retrieved from http://m.golocalprov.com/news/10-big-companies-with-recent- major-security-breaches/.

Grimes, R. (2012, Aug 27). *IT's 9 biggest security threats*. Retrieved from http://www.infoworld.com/article/2614957/security/.

Hirsh, A. (2013, Sept 18). *Cloud Encryption: Differentiating Between Symmetric, Asymmetric & Hashing*. Retrieved from http://technologyadvice.com/cloud-backup-and- storage/blog/differentiating-between-symmetric-asymmetric-hashing-encrpytion/.

InfoSec Baselines - All.Net. (n.d.). Retrieved from http://all.net/books/document/secman/Part6.html

Koved, L., Nadalin, A., Nagaratnam, N., & Pistoia, M. (2004, June 4). *The Theory of Cryptography*. Retrieved from http://www.informit.com/articles/article.aspx?p=170808.

Lee, T. B. (2013, Jun 14). *NSA-proof encryption exists. Why doesn’t anyone use it?* Retrieved from http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa- proof-encryption-exists-why-doesn't-anyone-use-it/.

pgpi.org. (2014, Oct 26). *How PGP works*. Retrieved from http://www.pgpi.org/doc/pgpintro/.

So You Think the Government Can't Regulate Internet Gambling ... (n.d.). Retrieved from http://cyber.law.harvard.edu/fallsem98/final\_papers/Glassberg.html