GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Encryption Solutions for Small Networks

GIAC (GSEC) Gold Certification

Author: David Reed, davidreed23@gmail.com

Advisor: Rick Wanner

Accepted: November 13, 2015

Abstract

Data breaches are becoming more and more common in commercial, corporate, and government systems. These breaches often result in massive amounts of sensitive data being exposed. These breaches are not exclusive to large networks. Small office and home office (SOHO) networks are potential targets as well. For the individual or small business, understanding the need for encryption and the proper way to implement it across the network can seem like a daunting task. This paper will provide background on the reasons encryption is important, examples of how it could have helped prevent real world breaches, and examples of its application in small networks.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

Data is being created faster than ever before. Every minute in 2014 users created 2.5 million pieces of Facebook content, 300,000 Tweets, and 220,000 Instagram photos (Gunelius, 2014). Each swipe of a credit card, scan of a loyalty card, and launch of a smartphone app creates even more data. This data has immense potential value. For corporations it can be used to target advertising in order to show goods and services are more likely to be purchased by the consumer. Government agencies use the data in building their case during a criminal investigation. As with anything of great value, this data is often the target of criminals.

Data breaches are increasing year over year. There were 27.5% more breaches reported in 2014 than 2013 (Identity Theft Resource Center, 2015). With the risks increasing it is more important than ever for networks to be secured with the tools and knowledge needed to protect the data. Any potential cost and effort in securing the network needs to be offset by the potential financial cost of a breach. The average cost of a breach in 2013 was $5.4 million (Weiss, 2014).

Large corporate networks are not the only networks that are vulnerable to data breaches. In small office and home office (SOHO) networks, the data is every bit as important as the data in the larger networks. Small networks are typically defined as networks with one to ten users (Mitchell, 2010). There are any number of reasons why the need for encryption in securing data can be overlooked; individuals and small businesses may assume that encryption is too costly or complicated to be justifiable on their networks; a false sense of security in other methods, like firewalls or intrusion detections systems, or simply not knowing the process for implementing encryption technology. Encryption is not a silver bullet or cure-all, but it should serve as critical part of a system of defense in depth.

The costs to purchase, implement, and maintain any defensive security tool must all be considered. No business or individual has an unlimited budget for network defense and as such, each decision must be thoroughly evaluated with a risk assessment and vetting by the required stakeholders. Encryption should be among the first considerations of any network security plan. When properly implemented strong encryption will provide a layer of security to the network that will make even the most determined adversary consider moving on to easier targets.

For small businesses and individuals the thought of using cryptography to protect their networks can be daunting, but it does not have to be. With some understanding of the need for

© 2015 The SANS Institute Author retains full rights.

encryption, the basics of encryption and ways to implement encryption on the network it is possible to begin confidently adding a cryptographic layer of security.

2. The Need for Encryption

Why do we need to protect data and who do we need to protect it from? Are small networks even at risk? Hackers thrive on arrogance and ignorance; the arrogance that existing defensive posture make networks immune to their efforts and ignorance in not knowing about other potentially appropriate defenses and how to use them effectively (Skoudis, 2015).

The vast amount of data generated each day is of value not only to businesses, but also criminal elements. Regardless of the type or source of the data, proprietary corporate data or customer data, it is a legitimate asset. Just as with any other assets, criminals will try to steal it if the value outweighs the cost of stealing it. Using encryption on each device that has the ability is among the best ways to prevent unauthorized access to data (Rose, 2013).

Before the Internet, corporate and personal data was manipulated and stored on machines located within local facilities. In those systems the needs of data security were often met simply by securing access to the facilities that housed these computer systems. That lack of connectivity beyond the local networks meant that securing the data could largely be done by physically securing the facility itself. With no physical access to the network, there could be no access to the data held within. The Internet has fundamentally changed not only the way that business is conducted, but the threats to the networks as well. Almost unlimited access to global networks meant that not only could businesses communicate with each other and their customers, but adversaries could potentially access the networks regardless of geographic location.

Advances in mobile technology have brought devices that have become a regular part of both personal and professional lives. Mobile devices are often either issued by companies to their employees or those employees taking advantage of a Bring Your Own Device (BYOD) policy. No matter how they are getting there, mobile devices are playing a larger role inside business networks. This potential new access vector has not gone unnoticed by criminals looking to exploit mobile (Barack, 2011). Every smartphone and tablet on the network is a target. Leaders in the mobile industry are taking the initiative and making encryption available natively on their devices. In 2014, Apple Inc. made headlines by announcing default encryption on all of their mobile devices (Poulsen, 2014).

© 2015 The SANS Institute Author retains full rights.

Beyond business practice of protecting customer data, or the personal need to protect individual data, corporations can actually be legally responsible for the loss of customer data (Sinrod, 2010). In 2009, an insurance provider settled for $1.5 million after they were found to be responsible for the loss of customer data when a pair of unencrypted laptops were stolen (Melnik, 2013). Simply applying an inexpensive encryption solution would likely have prevented these financial losses for the provider. More importantly it may have safeguarded the company's standing as a good manager of customer data.

Recent disclosures have confirmed that governments see data as a tool; A tool to be leveraged in the prosecution of crime. Companies that provide data services, hardware, and software have been in conflict with the U.S. government recently regarding the move to encryption as a standard for consumers. As companies like Apple and Google have made encryption an automatic function, rather than an optional feature, certain portions of the U.S. government have advocated that these companies install backdoors to allow for warranted data collection. If allowed, the government could use back doors such as these to encrypted data. The problem is that there is no such thing as a backdoor that only the good guys can use. While it remains to be seen how this debate will play out in the future it is clear that not every department in the government is against encryption. The FTC Commissioner, Terrell McSweeny, has stated that, "In this environment, policy makers should carefully weigh the potential impact of any proposals that may weaken privacy and security protections for consumers." (Masnick, 2015)

Eric Holder, Attorney General of the United States, advocated that strong cryptography should not be accessible for civilians (Holder and FBI, 2014). Terrorism, child pornography, and organized crime are often cited by the government as situations that require a timely investigation. In these situations encryption could hamper the government's ability to conduct a thorough investigation. There has been no consistency in the courts when they have been asked to require defendants to unencrypt their data (Courts Rule For, 2012). If a legal need can be proven in court then the data can be decrypted. If there is no proven need, the data remains protected from all unauthorized exposure.

Telecommunication providers maintain immense infrastructure systems to provide service to their customers. These systems are also used to ensure precise billing for the services used. These huge stores of billing data are often sought by the government in the investigation of

© 2015 The SANS Institute Author retains full rights.

crimes (Wicker, 2011). Data like this is most often not encrypted, but is turned over to the government only in properly warranted cases.

3. Commercial Breaches

It is not difficult to find examples of corporate networks being breached. While no two breaches play out the same way, upon closer inspection there are often common traits. Lack of encryption, or poorly implemented encryption, are frequently found to be contributing factors of the breaches. By examining how these breaches occurred, it is possible to gain a better understanding of how to protect small networks.

3.1 Target Corporation

In December of 2013 news broke that there had been a data breach at one of the largest retailers in the country, Target Corporation. Target initially put the breach at 40 million debit and credit card numbers, but that number was later raised to 70 million (Clark, 2014). The hackers used a wide variety of tactics and techniques to make their way in to Target's network, potentially exploiting a third party vendor in the early stages (Kasner, 2015).

It is not that Target had been negligent in securing their networks; in fact they had spent hundreds of millions of dollars on network security (Clark, 2014). Ultimately the hackers used a sophisticated piece of malware that was able to scrape the system RAM. Despite their network security, the fact was that the card numbers were taken from unencrypted memory (Kasner, 2015).

There was a bright spot for Target in the aftermath of the hack. The point of sale (POS) systems provided end to end encryption of the customer's PINs (Robinson, 2014). From the time the customer entered their PIN in the POS device in the store, until the transaction hit the credit card providers network the PIN was encrypted. Even with the level of access the hackers had to the Target network, it is believed that they were not able to decrypt the PINs (Robinson, 2014). It is estimated that the breach cost Target $200 million, but those losses could have been much higher if the PINs associated with the credit/debit cards had been compromised as well (Clark, 2014).

© 2015 The SANS Institute Author retains full rights.

The gaps exploited in the Target network made it possible for large numbers of customer credit/debit numbers to be stolen, but a properly designed and implemented encryption system prevented the breach from being even more costly.

3.2 Ashley Madison

In August of 2015, a group of hackers followed through on a threat and released more than 9 gigabytes (GB) of data on Ashley Madison's customers (Victor, 2015). The breach had been known to Ashely Madison as early as June when the hackers made demands that they take down their site or risk the release of customer data.

Eventually even more data was released, as much as 100 GB (Goodin, 2015). As many as 32 million customer records were made public as a result of the breach. The impact of the breach was made worse when the hackers were able to crack 11 million passwords due to improperly implemented encryption (Ashford, 2015).

Even though the passwords were hashed using MD5, there was a significant flaw in the implementation. The Ashley Madison team used a system that converted both the usernames and passwords to a lowercase string of characters separated by two colons. This reduced the keyspace of possibilities, reducing the number of guesses needed to decrypt the passwords (Goodin, 2015). A variable called "$loginkey" was generated, presumably as a shortcut for users to login without having to input their password each time. The conversion of the username and password, combined with the $loginkey variable greatly reduced the amount of time needed to crack the passwords (Goodin, 2015).

It was not enough to simply employ encryption on their network. When not properly implemented even the most robust encryption systems do not provide much protection for data. If properly configured their encryption should have taken years to crack rather than days (CynoSure Prime, 2015).

4. Encryption Basics

"In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet." (Kessler, 2015).

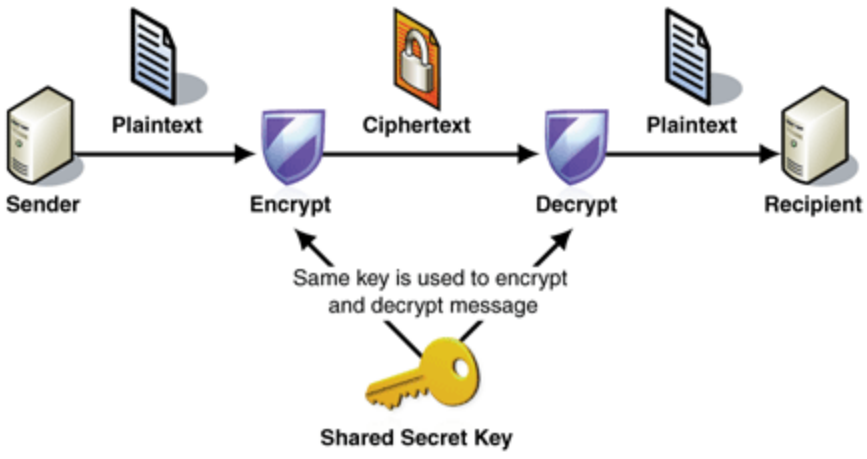
© 2015 The SANS Institute Author retains full rights.

In its simplest form, encryption is transforming a message from readable plaintext to an unreadable ciphertext. From the earliest forms of simple substitution ciphers, to the Enigma machine of WWII, to the modern day computer algorithms, encryption has played a pivotal role in history. Encryption algorithms are a set of rules based on mathematics that are used to encrypt plaintext data. Keys are "a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text or to decrypt encrypted text" (Rouse, 2005). Since most algorithms are public it is keeping the key secure that makes the encryption secure. Key security, complexity, and length are absolutely essential to a secure encryption system.

There are many cryptographic methods, but we will cover three of the most widely used; private key, public key, and hashing functions. Each has its own strengths and weakness. No one encryption method is appropriate for all situations. Each encryption method should be evaluated and applied in a manner that is most appropriate for the given use case.

4.1 Symmetric Key Encryption

Symmetric key, or shared secret key, encryption is the process of encrypting and decrypting data with the same key. Assuming the symmetric key stays safe, this type of encryption is very secure. The encrypted data can be transmitted or stored without fear of unapproved disclosure. Once encrypted, anyone viewing it would only see the unintelligible data and would have no way of determining the true contents of the data ("Public Key and Private Keys", 2015).



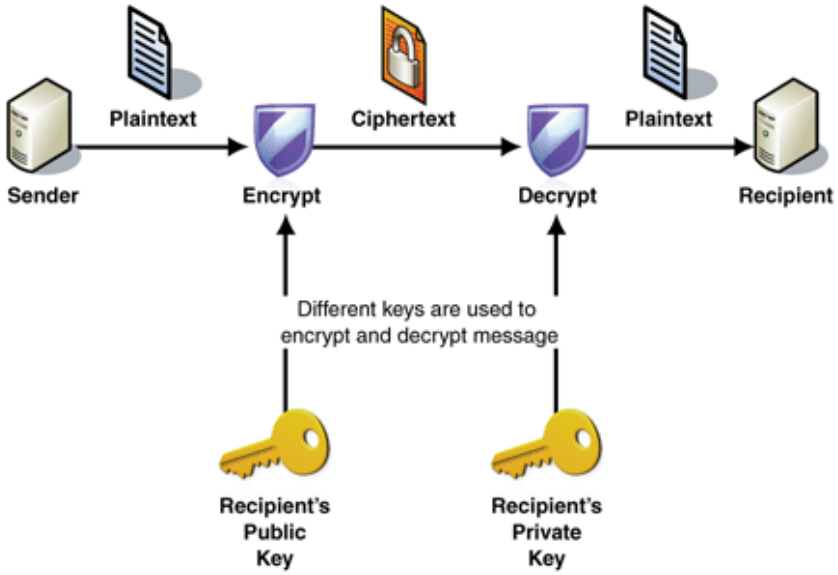
Symmetric key data encryption and decryption (Microsoft, 2005)

© 2015 The SANS Institute Author retains full rights.

This method of encryption is very secure, but it has one major drawback. Each step of the encryption and decryption process requires the same symmetric key. It is essential to ensure that all approved users have access to the correct key prior to viewing the data. There are many ways to pass this key, such as printing a hard copy of the key or using a thumb drive to pass a soft copy. A serious consideration for symmetric keys are that the larger the number of people that have access to the key, the more likely it is that there will be a breach. Due to this limitation, "symmetric key encryption is particularly useful when encrypting your own information as opposed to when sharing encrypted information" (Poretsky, 2013).

4.2 Asymmetric Key Encryption

Asymmetric key, or public key, encryption is a system that uses multiple keys in the encryption and decryption process. It is very similar to private key encryption, however the data is encrypted with a private key and is then decrypted with a corresponding public key. The process can be reversed as well. For example, Bill can send Sally a message encrypted with his private key. Then Sally, or anyone with Bill's public key, can decrypt the message. When Sally wants to respond to Bill, she can use his public key to encrypt the message and Bill can use his private key to decrypt that message. Only Bill's private key can be used to decrypt messages encrypted with his public key.



Asymmetric key data encryption and decryption (Microsoft, 2005)

© 2015 The SANS Institute Author retains full rights.

A limitation of asymmetric encryption is speed. The computational resources required for asymmetric encryption are much higher than those of symmetric encryption (Lander, 2013). Looking only at this for one transaction at a time does not seem like much, but extrapolating these differences across an enterprise sized system and these computational resource cost become much more impactful. Additionally, for distributing the public key often times a certificate authority is required. Certificate authorities are third party entities that are used to verify the identities of parties on the Internet (Rouse, 2007). Assuming the certificate provided by the involved parties is not compromised, the validity of the public keys can be trusted. As with symmetric key encryption, keeping the private key secure is crucial to the security of the overall system.

Non-repudiation, is an added benefit of this public/private key association. The data encrypted by the private key can only be decrypted by the equivalent public key. This relationship results in the clear-cut knowledge that, as long as the private key has not been breached, the data that can be decrypted with the public key can only have been encrypted by the corresponding private key. This ensures that the data is not only secure, but that the sender is verified (Wuest, 2015).

4.3 Cryptographic Hash Functions

A third method for encryption is cryptographic hash functions, or one-way hash functions. Hashing works by passing data, of almost any size, through the algorithm and outputting a hash of a fixed size. Cryptographic hashes provide a method for encrypting data to such a degree that it would be impossible to reconstruct the input using only the hashed output (Northcutt, 2008).

Hashing functions are very useful in proving data integrity due to the very low likelihood that two plaintext messages will result in the same hash value (Northcutt, 2008). A hashing algorithm's data integrity properties are used not only to ensure data integrity in messaging, but also in proving the integrity of data during an incident response or criminal investigation. Once the data has been hashed, changing any of the data will result in a completely different hash. In this manner it is possible to prove that data presented in a report or court case is in fact the same data that was recovered initially.

© 2015 The SANS Institute Author retains full rights.

There are numerous forms of modern hash functions; Message Digest (MD2, MD4, and MD5) and Secure Hash Algorithms (SHA1, SHA256, and SHA512) are some of the more well-known versions. The Secure Hash Algorithms are notable because they are a group of cryptologic hash functions published and maintained by the National Institute of Standards and Technology (NIST).

There are many differences between the various types of hashing functions, but of significant concern are collisions (Konheim, 2010). Collisions are the result of two separate inputs generating the same hashed output. While rare, these collisions can create doubt in the integrity of data and result in the hashing function that generated them falling out of use. By lengthening the size of the output string the likelihood of a collision is greatly reduced.

Algorithm	Length of Hashed String
MD5	22-characters (128 bit)
SHA1	27-characters (160 bit)
SHA256	43-characters (256 bit)
SHA512	86-characters (512 bit)

Hash functions and output length (IBM, 2013)

4.4 Key/Password Management

Encryption does not provide any security if the key (password) is not strong and secure. The same guidelines used for selecting a strong password can be used for selecting a strong key (Hoffman, 2015):

- 12 Characters, Minimum – Key length can vary based on the type of encryption being used, but longer is generally better
- Includes Numbers, Symbols, Uppercase Letters, and Lowercase Letters
- No Dictionary Words
- No Common Substitutions - Replacing 'a' with '@' and 's' with '$' will not make the password more secure. These common substitutions often show up in Rainbow Tables used by password cracking software (Warner, 2010).

© 2015 The SANS Institute Author retains full rights.

Additionally, having a strong key will not provide security if adversaries can readily access the key. Some best practices for keeping keys secure include (Leichter, 2013):

- Restrict access to the keys to as few users as possible
- Store encrypted data and keys on physically separate systems
- Change keys periodically
- Encrypt the key when possible
- Never share keys in plaintext

5. Encryption in Small Networks

Encryption makes data virtually unreadable to anyone but authorized users. It is useful for protecting data at rest on networks, data in motion between networks, and can even be used to protect data being transported on physical media. While some encryption systems can be quite expensive, there are many low or no cost options available. Some of these options may already exist on the network.

5.1 Data at Rest

Data at rest is a term used to describe data that is stored on the network (Lee, 2009). Think of this in terms of data that is stored or archived, rather than data that is sent outside of the networks.

5.1.1 Whole Disk Encryption

The first step in implementing encryption on the network is to decide what data needs to be encrypted. This can be a time consuming and difficult task to accomplish. It often requires a well written and enforced policy document that lays out the criteria for determining which files will be encrypted as well as the process to actually implement the encryption. Each and every piece of data on the network, as well as each new file created or brought in to the network, will need to be reviewed and assessed. Each user on the network will need to be trained on how to properly encrypt the data and there will be work associated with ensuring that the encryption policy is being followed. Whole disk encryption eliminates the need for this initial review process as well as the ongoing policy enforcement.

© 2015 The SANS Institute Author retains full rights.

© 2015 SANS Institute, Author retains full rights.

Whole disk encryption starts by modifying the boot sequence, the instructions that the machine uses to start up. Depending on the implementation, pre-boot is the point where the user will be required to authenticate with a strong password, USB, one-time use password from a token, or even a biometric means (Ruebens, 2012). Once the user is authenticated there is no further action required on their part. The encryption happens in user transparent processes.

From a user perspective, whole disk encryption does not have a significant impact on the use of, or performance of, the encrypted machine. Once the user has authenticated themselves, the data is encrypted/decrypted as it passes through the input and output level of the system. For the average user performing normal office operations such as email and document creation, the processing impact will be minimal (Rubens, 2012). One significant point to remember is that once the user is authenticated they have access to all the data on the machine. If the user walks away from their machine without locking it, anybody can sit at that machine and access the data. Additionally, if the network has already been compromised with malware, or some other vulnerability, the data could be at risk.

After whole disk encryption is properly configured, all the data on the drive, including the OS, is automatically converted from plaintext to ciphertext. This ciphertext makes the data unreadable to any unauthorized users. The encryption protects the data even if the drive is physically relocated to another machine (Rouse, 2014). This is of particular importance for portable media such as laptops and external storage devices. Laptops can be configured in the same manner as desktop machines, but external storage devices such as thumb drives and external disk drives might need to be configured separately. Depending on the whole disk encryption solution that is selected, there are options to automatically encrypt any external storage devices when they are plugged into the encrypted machine.

There are many commercial options for whole disk encryption depending on the operating system and hardware configuration (Paul, 2014). If the systems are running certain versions of Windows, Elite and Pro versions since Vista, then BitLocker is already available on the system (Waggoner, 2010). There are a number of free alternatives to BitLocker. TrueCrypt was popular because of its features and ease of use, but as of May 2014 it is no longer considered secure (Goodin, 2014). There are a number of other free whole disk encryption options that serve as replacements for TrueCrypt; such as VeraCrypt, CipherShed, and DiskCryptor. VeraCrypt is

© 2015 The SANS Institute Author retains full rights.

based on the same source code as TrueCrypt, but has made improvements to security by raising the number of iterations per encryption (Krishna, 2015). Each whole disk encryption offering, commercial or free, has its own pros and cons including cost, features, and ease of use.

5.1.2 Folder/File Encryption

Whole disk encryption may not be right for the network, especially if a large majority of the files are not sensitive. Encrypting individual files and folders is a more granular way to secure data (Pinola, 2012). Even in cases where whole disk encryption is in place, applying further encryption to specific files is a way to add another layer of security to the network. This added security comes at a higher time cost to the individual user in the form of multiple levels of authentication. Unless the system has been configured for automation, such as EFS, file encryption is not automatic. Users will have to be trained and trusted to follow the policy on encrypting sensitive data.

As with whole disk encryption, there are many different commercial options for encrypting files. Some of the whole disk encryption solutions also offer file encryption possibilities. Many of the modern operating systems provide a way to apply whole disk and file encryption natively (Microsoft, 2015a). Microsoft began offering their Encryption File System (EFS) on certain versions of Windows 2000 (Bragg, 2015). EFS was supplemented with BitLocker in later versions of Windows. Apple offered file and disk encryption with FileVault beginning with Mac OS 10.3 Panther (Apple, 2015). Linux offered dm-crypt with the release of the Linux kernel version 2.6 (Broz, 2015).

Some applications, like Microsoft Office (Microsoft, 2015b) and Adobe Acrobat (Adobe, 2015), offer the ability to encrypt the files created within the application. While whole disk encryption provides a level of completely automatic data encryption, an additional file encryption policy can be used to augment security for particularly sensitive files (Condon, 2010).

5.1.3 Mobile Devices

There is no denying the prevalence of mobile device in the modern workspace. These devices are often used to view, manipulate, and store the same sorts of sensitive data that is guarded so closely on traditional network devices. In many ways these devices are no different than a laptop when considering security.

© 2015 The SANS Institute Author retains full rights.

For phones, simply having a lock screen with a passcode is not enough. Hackers routinely find ways around these screens (Brandom, 2015). Once they are beyond the lock screen the data on an unencrypted phone is freely accessible. Both of the top mobile operating systems, Android and iOS, offer the native ability to encrypt portions of the data on mobile devices (Pinola, 2013). iOS devices do not require much from the user to enable the encryption. The data is automatically encrypted and simply adding a passcode to the lock screen protects the data (EFF, 2014). Many manufacturers of devices using the Android OS apply their own changes to the base OS. This fragmentation results in each device having a different set of encryption options. Generally speaking encryption is available on versions of Android since Lollipop, but each manufacturer has the option to make it automatic (Seppala, 2015). Each specific device and OS combination will have its own particular options, but a strong passcode combined with encryption goes a long way towards making mobile devices much more secure.

5.1.4 Cloud Storage

Cloud storage solutions are an attractive option for providing large amounts of relatively cheap and easily accessible storage. Almost all of the cloud storage solution providers offer encryption as automatic feature (Henry, 2013). While this encryption is generally okay, the problem is that these same providers have the keys to decrypt the data as well (Castle, 2013). The solution to this problem is to encrypt the files before sending them to the cloud storage provider or to set up an encrypted volume in the cloud that only authorized users in the organization have the keys for (Castle, 2013).

There are dozens of providers of cloud storage, but Microsoft OneDrive, Dropbox, and Google Drive are among the most widely used (Moran, 2015). In the case of Microsoft's OneDrive the data is protected with encryption while at rest and while in motion. The data at rest can be protected with BitLocker for whole disk level encryption and also with file level encryption as well. Both options use AES encryption with a key size of 256-bits. When moving data from the local network to the cloud, or between data centers for redundant storage, SSL/TLS with a 2048-bit key is used (Microsoft, 2015c).

5.2 Data in Motion

Data in motion typically refers to communication (Schneier, 2010). Data that is being sent from one location to another. Examples include web traffic and email.

© 2015 The SANS Institute Author retains full rights.

5.2.1 TLS

Transport Layer Security, or TLS, is a protocol that provides data security when communicating between two systems (Tyson, 2001). TLS is often used in Internet based communications. Websites, webmail providers, voice over IP, and instant messaging are all examples that can use TLS for secure communication.

Traffic sent using TLS is initiated with a handshake protocol that results in the exchange of keys for encrypting and decrypting traffic (Honorof, 2013). Once this exchange is successfully completed there is very little chance of the communication being decrypted by unauthorized viewers. For web browsing this process involves digital certificates and results in unencrypted HTTP web traffic being sent encrypted via HTTPS (Kangas, 2009).

5.2.2 VPN

In addition to securing the data located within local networks, it is necessary to consider options to protect the data that is sent outside the network. One of the simplest solutions for this is the Virtual Private Network (VPN). A VPN creates a tunnel, secured with encryption that allows data to be sent securely over the Internet or other untrusted network (Andres, 2010).

A VPN can be set up as a third party web service, installed on router/servers, or installed on the network as a hardware appliance (Vaughan-Nichols, 2011). No matter which version or implementation of VPN is selected, the end result is the same; the Internet traffic will be secured against prying eyes, even if that traffic is intercepted.

There are many options for commercial VPN services at varying price points and feature sets. Private Internet Access, TorGuard, IPVanish, and CyberGhost are very popular possibilities (Henry, 2014). In addition it is possible to setup and run a VPN on the local network. For example, Windows comes with a VPN client already installed. Another free option is to install and run OpenVPN as either a hardware or software implementation (Geier, 2013).

5.2.3 Email

© 2015 The SANS Institute Author retains full rights.

Email may be the single biggest source of new data day to day in the network. By necessity, email must travel across networks beyond the control of internal network security measures. End to end email encryption is so important to have, but since the data moves off the local network it can be potentially difficult to implement. There are more methods for securing email data with encryption than ever before. Many of the web and desktop mail service providers offer options for enabling encryption (Howell, 2014). Some providers, such as Google's Gmail, automatically encrypt all email. Google is even taking it a step further by releasing the source code for an end-to-end email encryption solution using Pretty Good Privacy (PGP) (Forrest, 2014). Options such as Google's tool, End to End, and PGP begin to give choices to apply encryption to networks in manageable and reliable ways (Lardinois, 2014).

If a non-web based email option is needed, there are several desktop email clients that offer encryption options. Microsoft Outlook offers the ability to encrypt individual messages or all outgoing email traffic (Microsoft, 2015d). Similar to Google, Mozilla's open source desktop email client, Thunderbird, also provides PGP based encryption (Mozilla, 2014).

6. Conclusion

Ultimately networks of all sizes need protection. This requires a proactive approach to examining how data lives on the network and travels outside of the network. This paper has provided a look at some low cost, easy to use encryption options that are suitable for use in even the smallest network. It is not meant to be an exhaustive source of all things encryption, but to serve as a starting point for looking at encryption options available to small networks.

For anyone trusted to administer a network it is imperative to apply the appropriate defenses to the network to ensure the confidentiality, integrity, and availability of the data. An understanding of the added security that encryption can bring to the network and how to properly implement it is a great step towards a more secure network. Encryption provides a great advantage that should be used in all suitable areas of the network. With the information set out above, a network will be well on its way on the path of data security. The use of encryption can provide data protection from all types of undesirable access. Encryption is a tool that deserves strong consideration in a system of defense in depth.

David Reed, davidreed23@gmail.com

© 2015 The SANS Institute Author retains full rights.

7. References

Adobe. (2015). Adobe Acrobat X Standard * Securing documents with passwords. Retrieved from http://help.adobe.com/en_US/acrobat/X/standard/using/WSD012A4E1-51D1-4bcd-BA9F-EF03C6F20BB6.html

Andres, S. (2010, June 3). How to Set Up a Secure Web Tunnel | PCWorld. Retrieved from http://www.pcworld.com/article/197725/how_to_set_up_a_secure_web_tunnel.html

Apple. (2015, September 4). Use FileVault to encrypt the startup disk on your Mac - Apple Support. Retrieved from https://support.apple.com/en-us/HT204837

Ashford, W. (2015, September 11). Ashley Madison data breach escalates with password encryption failure. Retrieved from http://www.computerweekly.com/news/4500253313/Ashley-Madison-data-breach-escalates-with-password-encryption-failure

Barack, L. (2011). Cyber Hackers are Faster and Better Equipped Than You. Registered Rep, 35(6), 47-50

Bragg, R. (2015). The Encrypting File System. Retrieved from https://technet.microsoft.com/en-us/library/cc700811.aspx

Brandom, R. (2015, September 30). Apple has fixed the latest iPhone lock screen bug | The Verge. Retrieved from http://www.theverge.com/2015/9/30/9426403/lock-screen-bug-fixed-iphone-ios9-apple

Broz, M. (2015, March). Dmcrypt | Wiki | cryptsetup / cryptsetup | GitLab. Retrieved October 27, 2015, from https://gitlab.com/cryptsetup/cryptsetup/wikis/DMCrypt

Castle, A. (2013, January 18). How to encrypt (almost) anything | PCWorld. Retrieved from http://www.pcworld.com/article/2025462/how-to-encrypt-almost-anything.html

Clark, M. (2014, May 5). Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer. Retrieved from http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056

David Reed, davidreed23@gmail.com

© 2015 The SANS Institute, Author retains full rights.

Condon, R. (2010, February 8). Full disk encryption: Safer and easier than file and folder encryption. Retrieved from http://www.computerweekly.com/news/1381003/Full-disk-encryption-Safer-and-easier-than-file-and-folder-encryption

Courts Rule For, Against Hard Drive Decryption. (2012). Information Management Journal, 46(3), 17

CynoSure Prime. (2015, September 10). CynoSure Prime: How we cracked millions of Ashley Madison bcrypt hashes efficiently. Retrieved from http://cynosureprime.blogspot.co.uk/2015/09/how-we-cracked-millions-of-ashley.html

EFF. (2014, November 18). How to: Encrypt Your iPhone | Surveillance Self-Defense. Retrieved from https://ssd.eff.org/en/module/how-encrypt-your-iphone

Forrest, C. (2014, June 5). Google's end-to-end Gmail encryption: An excellent development for the enterprise - TechRepublic. Retrieved from http://www.techrepublic.com/article/googles-end-to-end-gmail-encryption-an-excellent-development-for-the-enterprise/

Geier, E. (2013, March 19). How (and why) to set up a VPN today | PCWorld. Retrieved from http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html

Goodarzi, K., Karimi, A. (2014). Cloud Computing Security by Integrating Classical Encryption. Procedia Computer Science, 42320. doi:10.1016/j.procs.2014.11.069

Goodin, D. (2014, May 28). "TrueCrypt is not secure," official SourceForge page abruptly warns | Ars Technica. Retrieved from http://arstechnica.com/security/2014/05/truecrypt-is-not-secure-official-sourceforge-page-abruptly-warns/

Goodin, D. (2015, September 10). Once seen as bulletproof, 11 million+ Ashley Madison passwords already cracked | Ars Technica. Retrieved from http://arstechnica.com/security/2015/09/once-seen-as-bulletproof-11-million-ashley-madison-passwords-already-cracked/

David Reed, davidreed23@gmail.com

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Gunelius, S. (2014, July 12). The Data Explosion in 2014 Minute by Minute – Infographic | ACI. Retrieved from http://aci.info/2014/07/12/the-data-explosion-in-2014-minute-by-minute-infographic/

Henry, A. (2013, July 10). The Best Cloud Storage Services that Protect Your Privacy. Retrieved from http://lifehacker.com/the-best-cloud-storage-services-that-protect-your-priva-729639300

Henry, A. (2014, March 23). Five Best VPN Service Providers. Retrieved from http://lifehacker.com/5935863/five-best-vpn-service-providers

Hoffman, C. (2015, May 29). How to Create a Strong Password (and Remember It). Retrieved from http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

Holder And FBI Looking To Stop Civilian Use Of Strong Crypto | FDL News Desk. (n.d.). Retrieved from http://news.firedoglake.com/2014/10/10/holder-and-fbi-looking-to-stop-civilian-use-of-strong-crypto/

Honorof, M. (2013, September 6). SSL vs. TLS: The Future of Data Encryption. Retrieved from http://www.tomsguide.com/us/ssl-vs-tls,news-17508.html

Howell, D. (2014, June 7). How to Use Encryption in a Small Business | Lifehacker UK. Retrieved from http://www.lifehacker.co.uk/2014/06/07/use-encryption-small-business

IBM. (2013, April 18). IBM Support for passwords greater than 8 characters - United States. Retrieved from http://www-01.ibm.com/support/docview.wss?uid=isg3T1010741

Identity Theft Resource Center. (2015, January 12). Retrieved from www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

Kangas, E. (2009, March 17). How Does Secure Socket Layer (SSL or TLS) Work?. Retrieved from https://luxsci.com/blog/how-does-secure-socket-layer-ssl-or-tls-work.html

© 2015 The SANS Institute Author retains full rights.

Kassner, M. (2015, February 2). Anatomy of the Target data breach: Missed opportunities and lessons learned | ZDNet. Retrieved from http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Kerner, S. M. (2013). Google Encrypts to Evade NSA Surveillance: Should You?. Eweek, 3.

Kessler, G. (2015, January 21). An Overview of Cryptography. Retrieved from http://www.garykessler.net/library/crypto.html#intro

Konheim, A. G. (2010). *Hashing in computer science: Fifty years of slicing and dicing*. Hoboken, NJ: Wiley

Krishna, V. (2015, August 18). 5 Best TrueCrypt Alternatives to Safeguard Your Data. Retrieved from https://www.maketecheasier.com/truecrypt-alternatives/

Lander, S. (2013, June 4). Disadvantages of Public Key Encryption | Chron.com. Retrieved from http://smallbusiness.chron.com/disadvantages-public-key-encryption-68149.html

Lardinois, F. (2014, December 17). Google's End-To-End Email Encryption Tool Gets Closer To Launch | TechCrunch. Retrieved from http://techcrunch.com/2014/12/17/googles-end-to-end-email-encryption-tool-gets-closer-to-launch/

Lee, S. (2009, March 13). What Is Data At Rest Encryption? (Updated) - AlertBoot Endpoint Security. Retrieved from http://www.alertboot.com/blog/blogs/endpoint_security/archive/2009/03/13/what-is-data-at-rest-encryption.aspx

Leichter, W. (2013, November 19). Best Practices for Encryption Key Management. Retrieved from http://www.ciphercloud.com/blog/encryption-key-management-comply-pci-dss-3-0/

Manes, C. (2015, June 12). The top 24 free tools for data encryption. Retrieved October 1, 2015

© 2015 The SANS Institute Author retains full rights.

Masnick, M. (2015, September 4). FTC Commissioner Says The Public Needs Strong Encryption, Not Backdoors | Techdirt. Retrieved from https://www.techdirt.com/articles/20150903/17322932164/ftc-commissioner-says-public-needs-strong-encryption-not-backdoors.shtml

Melnik, T. (2013). Court Decision on a Class Action and an Office for Civil Rights Action Highlight the Importance of Mobile Device Encryption. Journal Of Health Care Compliance, 15(1), 43-57

Microsoft. (2005, December). *Private key data encryption and decryption*. Retrieved from https://i-msdn.sec.s-msft.com/dynimg/IC168364.gif

Microsoft. (2005, December). *Public key data encryption and decryption*. Retrieved from https://i-msdn.sec.s-msft.com/dynimg/IC155063.gif

Microsoft. (2015a). Encrypt or decrypt a folder or file - Windows Help. Retrieved from http://windows.microsoft.com/en-us/windows/encrypt-decrypt-folder-file#1TC=windows-7

Microsoft. (2015b, October 14). Add or remove protection in your document, workbook, or presentation - Office Support. Retrieved from https://support.office.com/en-us/article/Add-or-remove-protection-in-your-document-workbook-or-presentation-05084cc3-300d-4c1a-8416-38d3e37d6826

Microsoft. (2015c, February 3). Data Encryption in OneDrive for Business and SharePoint Online. Retrieved from https://technet.microsoft.com/en-us/library/dn905447.aspx

Microsoft. (2015d, November 9). Encrypt e-mail messages - Outlook. Retrieved from https://support.office.com/en-us/article/Encrypt-e-mail-messages-84d7e382-5f76-4d71-8705-324489b710a2

Mitchell, B. (2010, November 13). What Is a SOHO Router (and Network)?. Retrieved from http://compnetworking.about.com/b/2010/11/13/what-is-a-soho-router.htm

© 2015 The SANS Institute Author retains full rights.

Moran, J. (2015, June 9). 10 Top Cloud Storage Services for SMBs. Retrieved from http://www.smallbusinesscomputing.com/slideshows/10-top-cloud-storage-services-for-smbs.html

Mozilla. (2014, February 20). Digitally Signing and Encrypting Messages | Thunderbird Help. Retrieved from https://support.mozilla.org/en-US/kb/digitally-signing-and-encrypting-messages

Northcutt, S. (2008, January 10). Hash Functions. Retrieved from https://www.sans.edu/research/security-laboratory/article/hash-functions

Paul, I. (2014, May 30). So long, TrueCrypt: 5 alternative encryption tools that can lock down your data | PCWorld. Retrieved from http://www.pcworld.com/article/2304851/so-long-truecrypt-5-encryption-alternatives-that-can-lock-down-your-data.html

Patterson, N. J. (2010). The Key Theory: Authenticating Decrypted Information in Litigation While Protecting Sensitive Sources and Methods. Texas Law Review, 88(7), 1767-1794

Pinola, M. (2012, April 26). Do I Really Need To Encrypt Every File on My Computer?. Retrieved from http://lifehacker.com/5905374/do-i-really-need-to-encrypt-every-file-on-my-computer

Pinola, M. (2013, August 13). How to Encrypt Android and iPhone Cell Phone Data. Retrieved from http://mobileoffice.about.com/od/mobile-devices/a/How-To-Encrypt-The-Data-On-Your-Android-Phone-Or-Iphone.htm

Poretsky, S. (2013, January 12). Advantages & Disadvantages of Symmetric Key Encryption | Science - Opposing Views. Retrieved from http://science.opposingviews.com/advantages-disadvantages-symmetric-key-encryption-2609.html

Poulsen, K. (2014, October 8). Apple's iPhone Encryption Is a Godsend, Even if Cops Hate It | WIRED. Retrieved from http://www.wired.com/2014/10/golden-key/

Public Key and Private Keys. (2015, January 1). Retrieved from https://www.comodo.com/resources/small-business/digital-certificates2.php

David Reed, davidreed23@gmail.com

© 2015 The SANS Institute Author retains full rights.

Robinson, R. (2014, January 9). Three Lessons from the Target Hack of Encrypted PIN Data. Retrieved from https://securityintelligence.com/target-hack-encrypted-pin-data-three-lessons/

Rose, A. D. (2013). Mobile Devices: Know the Risks, Know the Safer Practices. Journal Of Health Care Compliance, 15(1), 47-58

Rouse, M. (2005, September). What is key? - Definition from WhatIs.com. Retrieved from http://searchsecurity.techtarget.com/definition/key

Rouse, M. (2007, June). What is certificate authority (CA)? - Definition from WhatIs.com. Retrieved from http://searchsecurity.techtarget.com/definition/certificate-authority

Rouse, M. (2014, December). What is full-disk encryption (FDE)? - Definition from WhatIs.com. Retrieved from http://whatis.techtarget.com/definition/full-disk-encryption-FDE

Rubens, P. (2012, May 9). Buyer's Guide to Full Disk Encryption - eSecurity Planet. Retrieved from http://www.esecurityplanet.com/mobile-security/buyers-guide-to-full-disk-encryption.html

Schneier, B. (2010, June 30). Retrieved from https://www.schneier.com/blog/archives/2010/06/data_at_rest_vs.html

Seppala, T. (2015, March 2). Google won't force Android encryption by default (update). Retrieved from http://www.engadget.com/2015/03/02/android-lollipop-automatic-encryption/

Sinrod, E. (2010, February 2). Data Security Breaches Cost Real Money - Technologist. Retrieved from http://blogs.findlaw.com/technologist/2010/02/data-security-breaches-cost-real-money.html

Skoudis, E. (2015). *Hacker Tools, Techniques, Exploits, and Incident Handling*. The SANS Institute.

Smartphones and the 4th Amendment. (2014, April 27). Retrieved from http://www.nytimes.com/2014/04/28/opinion/smartphones-and-the-4th-mendment.html

David Reed, davidreed23@gmail.com

© 2015 The SANS Institute Author retains full rights.

Talbot, D. (2010). Security in the Ether. Technology Review, 113(1), 36-42

Tyson, J. (2001, June 4). SSL and TLS - HowStuffWorks. Retrieved from http://computer.howstuffworks.com/encryption4.htm

Vaughan-Nichols, S. (2011, March 24). Get Started With a VPN: For Beginners, Power Users, and IT Pros | PCWorld. Retrieved from http://www.pcworld.com/article/223044/vpns_for_beginners_to_experts.html

Victor, D. (2015, August 19). The Ashley Madison Data Dump, Explained - The New York Times. Retrieved from http://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html

Waggoner, R. (2010, March 17). What is BitLocker? What does it do? What does it not do? - Welcome to the US SMB&D TS2 Team Blog - Site Home - TechNet Blogs. Retrieved from http://blogs.technet.com/b/uspartner_ts2team/archive/2010/03/17/what-is-bitlocker-what-does-it-do-what-does-it-not-do.aspx

Warner, C. (2010, December 20). Access denied | optimwise.com used CloudFlare to restrict access. Retrieved from http://optimwise.com/passwords-with-simple-character-substitution-are-weak/

Weiss, R. (2014, May 21). Cyber Liability Insurance - A Definition | Insurance Protection Blog. Retrieved from http://www.weissins.com/blog/entryid/5304/cyber-liability-insurance-defination

Wicker, S. B. (2011). Cellular Telephony and the Question of Privacy. Communications Of The ACM, 54(7), 88-98. doi:10.1145/1965724.1965745

Wlasuk, A. (2012). THE PERFECT SECURITY STORM. American School & University, 84(6), 38-41

Wuest, A. (2015, March 21). Introduction to Public-Key Cryptography. Retrieved from https://developer.mozilla.org/en-US/docs/Introduction_to_Public-Key_Cryptography

© 2015 The SANS Institute Author retains full rights.