Interested in learning more about security?

SANS Institute InfoSec Reading Room

A Practical Approach to Message Encryption

This paper provides a description of the mail encryption provided by ZixMail. and ZixMail.Net. from a security and business perspective by highlighting the advantages and disadvantages of these products.

A Practical Approach to Message Encryption

Edward Skerke
January 12, 2002
SANS Security Essentials GSEC Practical Assignment Version 1.2f
SANS Certification ADMINISTIVIA for All Assignments Version 2.0

Abstract

The intent of this paper is to provide a description of my journey of investigation for a practical mechanism of encrypting message content, emphasizing on the mail encryption provided by ZixMail™ and ZixMail.Net™ services offered by the Zixit™ Corporation. The content of this paper will explain the need these products fill from a security and business perspective by highlighting the advantages and disadvantages of these products. I will highlight and compare the features of Zixit™ 's service, offering my experiences with those of the popular email encryption product PGP™. I believe that after you read this document you will be convinced that the Zixit™ Corporation provides a practical service that fills a void in the secure messaging arena.

TABLE OF CONTENTS

I. Introduction

The desire to transmit messages without the content being known by anybody besides the intended recipient has existed for a long time. "In The Histories, Herodotus chronicled the conflicts of Greece and Persia in the fifth century BC…According to Herodotus, it was the art of secret writing that saved Greece from being conquered"[1]. It is arguable that this desire has existed and encryption was used since the beginning of any uniform form of communication.

Today, communicating across long distances at high speeds has been made very simple via the Internet and Email software. The majority of the Email products sending these messages utilize (by default) plaintext to transmit the messages. Plaintext is the default method of transmission because the technical evolution of email and cryptography ("the art and science of keeping messages secure"[2]) has not provided one uniformly accepted standard for encryption and decryption of email. "The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption."[3] The lack of security of any message sent via plaintext is only compounded by the fact that the majority of this email is transmitted via an insecure channel, the Internet.

The purpose of this Paper is to highlight the steps that I took to arrive at a solution which, when properly utilized, would help insure that sensitive information being sent via email would arrive with minimal chance of being viewed or modified by anybody other than the intended recipient. The emphasis of detail will be placed on the solution of choice: ZixMail. A secondary goal is to provide some real examples of different cryptography and some of the terminology used. I will make every effort to define terminology as it is introduced. This paper will not attempt to go into the mathematical details of any algorithms presented, references will be provided to other media that will provide those details that are beyond the scope of this paper.

II. The Journey Begins

I was chartered with the task of providing select individuals within my organization the ability to secure (encrypt) sensitive information being transmitted via email to internal and external clients.

This task was immensely complicated by the following criteria.

1. All email does not need to be encrypted, nor is it desired to have all email be encrypted. The majority of email transmissions will not require encryption since many recipients will not have the required tools to decrypt the message. The user must be able to select which emails are encrypted and which ones are sent plaintext.
2. The desire to choose an encryption tool that has the ability to send encrypted email to any receiver, and giving the receiver the ability to decrypt the message without having to load any new software on his machine.

[1] Singh, p.4
[2] Schneier-Applied Cryptography, p.1
[3] Schneier-Applied Cryptography, p.1

3. The encryption algorithm used should be computationally secure (strong).
4. The desire to easily decrypt any previously encrypted messages using a Corporate Wide recovery key (when passwords are lost or as people leave the organization).
5. Must be simple to use.
6. Associated costs to implement should be minimal.

Initially, I began looking at this task as impossible, especially with the ambiguity of several of the requirements. I made the following recommendations as solutions to this daunting task.

III. Proposed Solution 1- Symmetric Encryption with MicrosoftÔ Product

Prior to attending the SANS Great Lake Conference in Chicago (November 2001), I proposed this as a potential quick economical solution. Anybody sending sensitive information should utilize Microsoft Word™ or Microsoft Excel™ and use the built in encryption capabilities of these products to encrypt the information. "Access, Excel, and Word incorporate the symmetric encryption routine known as RC4. RC4 is stronger than the encryption routine used in previous versions of most Office applications, known as Office 4.*x* encryption. (Access has supported RC4 encryption since version 2.0.) Documents from previous versions of Office are not as secure as password-protected documents in Office 97 or 98 format."[4] I started working with several associates, providing detailed instruction on how to take advantage of the symmetric algorithm encryption capabilities of Microsoft Office products. "Symmetric algorithms sometimes called conventional algorithms are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same."[5] Symmetric algorithms have many inherent problems that are associated with tracking and communicating passwords to the person who will need to decrypt the file.

How did proposed solution #1 meet the established requirements?

Initial Requirements Satisfied (#1 and #6)

This solution would meet the primary objective of encrypting the data and would meet requirements #1 by allowing the user to decide what would be encrypted, and requirement #6 by having no associated cost, and just taking advantage of the products features.

Initial Requirements Not being Satisfied (#2,#3,#4,#5)

It did not meet requirement #2, because some clients do not have Microsoft Word or Excel on the receiving end. Requirement #3 is not satisfied, the algorithm used is strong but the entire procedure is flawed. A user can encrypt the message using whatever password they desire, and the length of the password chosen directly impacts the effort required to break the encryption. This is compounded by the fact that several easily acquired tools exist that will help you determine the password used by brute force. These tools can be easily obtained from the Internet, at sites like www.lostpasswords.com. " Password Recovery Modules: AccessData has a wide variety of individual password breaking modules that can help you recover lost passwords for almost every product in the industry. " [6], including Microsoft Excel and Word in the list of products that it can crack.

[4] Microsoft
[5] Schneier-Applied Cryptography, p.4
[6] Password Recovery ToolKit

Requirement #4 is not met because the encryption algorithm used by symmetric keys does not lend itself to this type of recovery unless the same password is used to encrypt all messages that leave the organization. This would not only be impossible to enforce, it would severely minimize the effectiveness of any encryption being done.
Requirement #5 is not met, because the user will be responsible for managing all the passwords being used and since the mechanism being used is a symmetric algorithm the user will be responsible for exchanging those passwords (ideally not via email, and hopefully not as plaintext with the encrypted message).

Proposed Solution #1 Summary
The solution of utilizing the encryption mechanisms built into the MS Office™ fell far from meeting the requirements. Some of the people I described the procedure to, found it to be cumbersome and challenging. If the lock is too difficult to operate it probably won't be used. I needed to provide a different solution.

IV. Proposed Solution 2 - Asymmetric Encryption with PGPÔ

Shortly after attending the Security Essentials track, at the SANS Great Lake conference (November 2001), I came back to the office and decided to take a thorough look at PGP™ and discover how it would fit with my set of requirements. I started by visiting the "MIT Distribution Center for Pretty Good Privacy"[7] and downloaded the PGP freeware. PGP utilizes Public Key encryption and functions within a PKI (Public key Infrastructure), which can be a little more difficult to understand, but was very well explained by Eric Cole during the SANS Security Essentials II: Network Security presentation. During this Seminar, I discovered that the plot surrounding private/public keys thickens quite quickly. I found that the following set of references explain the basics required for a better understanding

- What is PKI?
- A management structure for private/public
  - OK, we both have private/public keys now what?
  - There is more than meets the eye
- Public and Private encryption keys
- Digital Certificates
- Certificate Authorities
- Digital signatures
- Key management protocol[8]

Public and Private encryption keys
The following reference and diagram provides an excellent explanation.

> Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key

[7] MIT Distribution Center
[8] SANS Institute, p3-19

secret. Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met. It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information, but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.

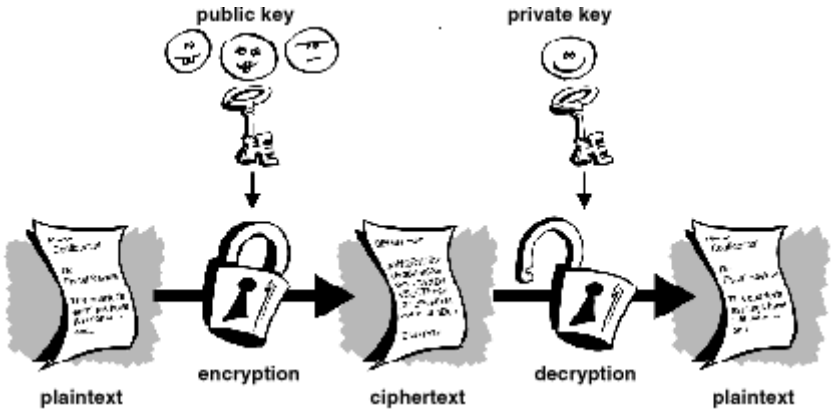

Figure 1-3. Public key encryption

The primary benefit of public key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. [9]

Digital Certificates

Once you generate a public and private key pair with the product, you will want to start sharing the public key with others, so they can use your public key to encrypt messages and send them to you. If somebody wants to send you an encrypted message, they will need to obtain a copy of your public key. That is where the TRUST factor becomes an issue. Where did that Public Key actually come from, and can I trust it? This is a very broad topic and I will leave it up to the reader to investigate this further, I recommend Chapter 15, "Certificates and Credentials "[10] of Bruce Schneier's book, *Secrets & Lies*.

Digital Signatures

The other important thing that came out of the discussion on PKI was Digital Signatures. This provides the ability to use your digital keys to attach a digital signature to a message, which accomplishes two things: 1) insures that the document was sent by someone with access to your private key, and 2) insures that the document content has not been modified in transit.

A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as to the identity of the signer.

[9] Intro to Cryptography, p 9
[10] Schneier - Secrets and Lies, Ch. 15

Some people tend to use signatures more than they use encryption. For example, you may not care if anyone knows that you just deposited $1000 in your account, but you do want to be darn sure it was the bank teller you were dealing with.
The basic manner in which digital signatures are created is illustrated in *Figure 1-6*. Instead of encrypting information using someone else's public key, you encrypt it with your private key. If the information can be decrypted with your public key, then it must have originated with you.

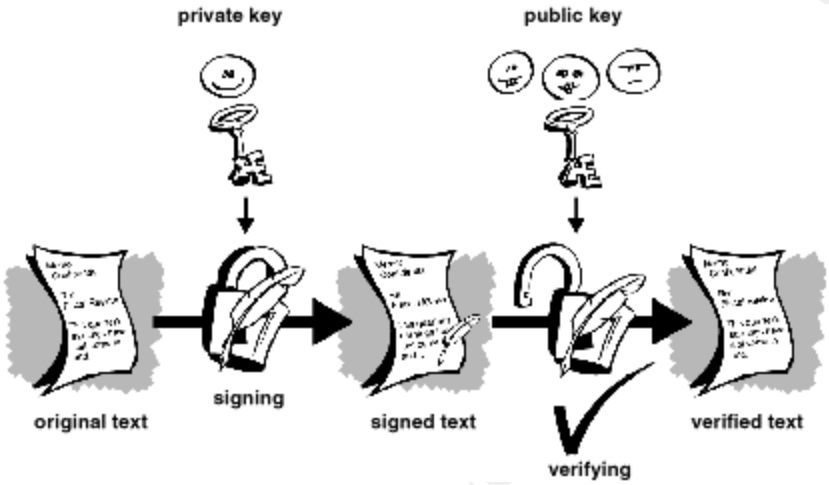

Figure 1-6. Simple digital signatures
[11]

I installed the freeware version of PGP™ at work and at home and set-up the necessary key pairs. PGP stores your keys on your local machine in a key ring, it is important to keep your private key secure,. The private keys are also kept confidential by establishing a passprhase to protect them. The longer the passphrase, the harder it will be to brute force into your private key. Then you need to connect to a key server and get the public keys for the users that you wish to send encrypted email messages to. This process started to become a little bit cumbersome and I believe would be considered challenging for most users. I then used this product to encrypt and decrypt messages, and digitally sign and verify messages. All the features worked as described above. I have come to the following conclusions regarding this product and its ability to meet the established requirements.

How did proposed solution #2 meet the established requirements?
Requirements Met (#1, #3,#6) and minimally met (#2)
Requirement #1 is met because this solution provides the ability to differentiate what should be encrypted prior to sending. Many of the problems associated with choosing a password and sharing that password have been removed with the use of Public Keys, even if simple private key passphrases are chosen this method of encryption is much better at being a strong encryption mechanism. Requirement #2 is minimally met, because this freeware application is available on

[11] Introduction to Cryptography, p12

a large variety of Operating Systems and the retail product can be integrated with many of the major Email applications (Microsoft Outlook™, Netscape Navigator™, and Eudora™). Requirement # 6 is met, the PGP™product is available on many different operating systems as freeware and even the retail versions are very affordable.

Requirements Not being Satisfied (#4,#5)
Requirement #4 is not met. This product does not appear to have the ability to easily create a corporate recovery key.
Requirement #5 is not met. The installation and setup of this tool is definitely a large step past using a symmetric key to encrypt a Microsoft Word™ document. Once installed the product works well but still can be very cumbersome for an average user to use and understand.

Solution #2 Summary
Using PGP would definitely be a step in the right direction. Unfortunately, I think this solution would be very difficult to implement and understand for the average user. PGP lacks the necessary recovery functionality and requires that any user receiving a PGP encrypted message have the PGP software installed. The need to have PGP loaded on both the sender and receiver and the complexity of this tool will profoundly limit the ease at which individuals will be able to accept this tool and user it effectively to communicate privately. The concepts of Public key have added a great deal of complexity to the tasks, but digital signatures have added the important benefit of message integrity and non-repudiation to our secure messaging solution. This product is not a bad choice for technical people who are willing to spend additional time to understand all the details, but I feel this product would be overwhelming for the average person who just wants to ensure the security of his messages.

V. Proposed Solution 3 - ZixitÔ Mail in Detail

After returning home from the Great Lake SANS conference in Nov. 2001, I started to review PGP to discover what its potential as messaging encryption solution would be. During that same time, I started to research ideas for my Practical GSEC assignment. This is when I discovered a paper entitled "Secure Messaging" by Ron Hilton in the SANS reading room. After reading the following comment, " Of the three products surveyed, ZixMail is the closest to a standard PKI product. It offers public/private keys, certificate authorities, and digital signature capabilities."[12], I decided that I would investigate how ZixMail would meet my list of requirements. I contacted the company and started to learn about its product offerings and began to evaluate their products. Zixit has several mechanisms for sending/receiving email that are all interconnected. The following reference highlights the connection mechanisms available.

Within the ZixMail and ZixMail.net implementations, there are four basic send, deliver, and opening methodologies:

[12] Hilton, p2

Method

1. ZixMail Non-Certified delivery direct to ZixMail Recipient
2. ZixMail Certified Delivery direct to ZixMail Recipient
3. ZixMail to ZixMail.net to recipient
4. Browser to ZixMail.net to Recipient[13]

The following ZixMail Service Overview provides an excellent explanation of the services details.

ZixMail Services Overview

ZixMail is a service that enables the delivery of secure documents and private email to any email address in the world. ZixMail allows you to easily send encrypted and digitally signed communications to any recipient, even if the recipient is not equipped with ZixMail. The ZixMail client application features an intuitive, easy to use graphical user interface that looks like any other email application, but works with the users current email address. Available ZixMail plug-ins for Microsoft Outlook® and Lotus Notes® provide the same functionality as the ZixMail client application, but within the Outlook or Notes environment and using the existing Outlook or Notes user interface. ZixMail provides:

- The ability to send secure messages to anyone with an email address
- Certified delivery receipts verifying the message "send" and "open" times
- Fast transmission of large documents through compression of attachments
- A minimum 1024-bit Asymmetric Public Key and Triple-DES Symmetric Key encryption technology
- Key management and distribution that is transparent and seamless to user

ZixMail senders have two options for message delivery: **ZixMail** direct to a ZixMail recipient or **ZixMail** to **ZixMail.net**, which enables various secure delivery methods, including secure browser-based (SSL) message pickup.

ZixMail

ZixMail direct to ZixMail recipient is ZixIt's premier secure email system and is used when both the sender and recipient are set up with the ZixMail client application (also available as a plug-in to Microsoft Outlook or Lotus Notes). ZixMail provides email messaging that is comprised of digitally signed, encrypted, and time-stamped messages sent over the Internet. At no time does ZixIt require your email, encrypted or unencrypted, to be delivered to ZixIt, or to be stored on or passed through ZixIt servers. Private keys are created on the ZixMail user's desktop PC and stay there.

[13] Zixit Corporation,p3

ZixMail.net
For instances when secure email recipients do not have the ZixMail client, they can still receive secure messages through the ZixMail.net delivery portal which:

- Provides, at a minimum, a browser-based solution for recipients to view secure messages over a secure (SSL) connection.
- Allows incoming encrypted messages (secure) from many sources, including the ZixMail clients, Entrust Express™, and Yahoo!® Mail. The incoming messages are decrypted and then standardized to a format that allows browser-based delivery, or direct email delivery using interoperability between different encryption methodologies, such as S/MIME and ZixMail.[14]

I initially started my review of this product by decrypting and reviewing a few encrypted messages that I received from the Sales and technical representatives via ZixitMail.Net. I did not load the client on my machine and had not yet established a public key with the service. The mail message I received from Zixit contained a pointer to an SSL encrypted web page that stepped me through the process of developing a key pair to retrieve the encrypted mail from ZixitMial.Net. After submitting the request for the key on the initial SSL encrypted web browser page, I received a message in my email with a link that would allow me to acknowledge the setup of this key. This prevents just anybody from creating a temporary set of keys and viewing your online email.

After acknowledging this key, I was taken to an SSL encrypted site that allowed me to view my decrypted email messages and reply to those messages, extract attachments, and compose a new message and send it encrypted as a reply. I was impressed, I was able to view an encrypted message securely without loading any additional software.

I then decided that this entire process was so easy that I would send a couple encrypted email messages to my peers and family members. I went to the web site and downloaded an evaluation copy of the software. Here is a summary of the screens I encountered during the installation process.

- The typical "Close all other applications before continuing " message.
- Typical License Confirmation Screen.
- Type of Install (Minimal or Typical)
  I chose Typical
- Prompt for Installation location.
- A Dialog offering you registration options
  - I have not used Zixit. help me register
  - I am a ZixMail user, my email already works with ZixMail
  - I am a ZixMail user. I want to register another email address to work with ZixMail

  I chose the first option - I have not used Zixit - help me register
- Prompt for Email Address that I would be registering, twice for confirmation.

[14] Zixit Corporation, p6

- Prompt for passphrase that I wished to use.
- The Zixit client then sent this information to their server, I know this because I had to enable the application to talk to the internet in Zone Alarm
- It then stated that a confirmation message would be sent to my email account, the email message would contain a link that needed to be connected to acknowledge and complete the registration process.
- The last step in the process prompted me for the creation of a recovery file. This file can be used to recreate your account. If your signature becomes corrupt, or you forget your signature passphrase you can use this recovery disk to reestablish your signature.
- **VERY IMPORTANT (if you choose this option) SECURE THE DISK**, the content of this disk can be used to impersonate your signature and used to open any encrypted mail that you receive.

The software installation process went smooth. The difference between typical and minimal installation depends on how you wish to view the decrypted messages. A typical install adds the integrated outlook client (which allows you to view the decrypted message right in outlook), if you choose a minimal install, the Zixit Client will be used to view encrypted messages. During later conversations with Zixit technical support, I discovered that this installation could be customized for corporate accounts. The passphrase validity parameters can be modified to demand that a minimal length, case change, or special character be included in the passphrase. The user will not be able to continue with the registration until he meets these passphrase requirements. The corporate account installation can also require that a recovery disk be created or NOT allow the creation of this disk. These customized installation options allows a great deal of flexibility in what you would like to accomplish while insuring that simple passphrase (and therefore stronger authentication) is maintained.

After the installation integrated the Zixit Client with Outlook 2000 on my machine, I was ready to continue the evaluation. To use the product, I typed a message and instead of hitting send, I chose the Z icon (Zixit Icon) from the Outlook 2000 toolbar. I chose to have these messages sent with a certified receipt of delivery, to see if they actually opened the messages. The content of the message included the following - "Congratulations - the message you just received was sent to you encrypted via Zixit, and you are the only one who has seen the content of this message decrypted. The steps you just took to view this encrypted message provide you with a sample of the steps that will be required when you encrypt and send sensitive information to a client that may not have the Zixit Client. Please write me back and tell me what you think." The majority of the people I sent this message to where able to follow the process of generating a temporary key, and view the message and responded that they had no problems. Many of the responses were returned to me as an encrypted ZixMail.Net response. This proved to me that the process was simple. I was sending encrypted email messages to people who have never received an encrypted message in their lives and they were able to view this message without loading additional software. They viewed the message by completing the few extra steps required to connect securely to ZixMail.Net.

These messages will remain in ZixMail.Net until the encrypting senders' expiration setting, of 21 days or less. I recommend that you send items that you wish the user to keep as attachments to the messages, when you are sending encrypted messages to non-ZixMail client users. Zixit

Corporation has this limit because they are in the business of providing encryption, not storing mail. If a message receiver does not open a message that you sent to them with ZixMail.Net, you will receive a message indicating that the message you sent to user@domain was never opened and has expired.

After experimenting with the product for a day or two, I inquired about the key recovery aspects of the product. I was informed that I could purchase an option to have a corporate recovery key. This recovery key would allow me to recover the content of any user in the domain I specified. I completed the forms to test this option. A representative of the Zixit Corporation made contact with the registered domain owner and obtained permission for this to happen, and set me up with a test corporate key. I had a member of the evaluation team forward me an encrypted message that was sent to him. I used the account that I set up with the corporate key to decrypt his message. The ability to recover corporate messages was satisfied.

ZixMail includes a Signature Manager that can be used to manage the following aspects of your digital signatures. This tool is used to create, edit, or delete your signature. This tool becomes important when you have to deal with multiple email addresses, because each signature is connected to one email address. You will also need to use this tool when copying a signature between machines.

How did proposed solution #3 meet the established requirements?

Requirements Met (#1,#2,#3,#4,#5,#6)
Requirement # 1 has been satisfied. ZixMail will allow the user to decide to whom he will send encrypted messages.
Requirement # 2 has been satisfied. ZixMail will allow you to send encrypted email to any user that has the ability to receive email messages and has an Internet browser. The browser will be used to view the email via an SSL encrypted web page.
Requirement #3 has been satisfied. the Rabin Algorithm and 3DES utilized are well known industry standards. The security is greatly enhanced by the corporate ability to demand certain passphrase characteristics such as minimum length, case change, and Alpha Numeric.
Requirement #4 is doubly satisfied, complete recovery files can be created on installation (KEEP THESE FILES SECURE) and a corporate recovery key option is available.
Requirement # 5 has been met. The software installed easily and lacked much of the confusion that I encountered with PGP. Shortly after installation, I was sending encrypted email messages to users and a large majority of them followed the simple steps required to view the decrypted messages, without loading software on their machine.
Requirement #6 was met. The product is licensed on a fixed dollar amount for each user over a one-year period and was less then purchasing retail PGP/user.

Requirements Not being Satisfied (None - All are met)
This product met all the requirements that I set out to meet.

Solution #3 Summary
This product has satisfied all my initial requirements. I purchased a 25 user corporate license with the corporate recovery key. I am currently in the process of extending the initial evaluation

group of users to include many more users that require the ability to send encrypted email messages. The technical support group at Zixit Corporation has been very easy to work with, and the product has been solid. They also offer a product called ZixVPM™ [15] that is a hardware solution that will automatically filter all email and based on sender name, recipient name, or subject content and automatically apply encryption to those messages based on a centrally maintained set of rules. This product is just being introduced, to find out more about the product read the press release referenced.

VI. Conclusion

As I started down my research path, I encountered a very important aspect of encryption that is made possible with a PKI, Digital Signatures . Digital Signatures are important because they 1) insure the integrity and 2) provide non-repudiation (validating the message was sent from the person digitally signing the document) of messages. I did not include these in my initial requirements, in hindsight I should have. Fortunately, the two viable solutions proposed (1) PGP and (2) ZixMail have this functionality and when tested in each product this function worked properly. ZixMail takes this functionality to the next level by providing Digitally Signed receipt messages when communicating with another subscribed ZixMail client. If SANS was using this tool, I would be able to receive an automatically generated digital receipt once the email containing my practical assignment was received. PGP is more standalone in this regard and can not deliver receipt messages.

It should be apparent from reading this document that I chose to implement ZixMail as our corporate solution. I would like to point out that this does not mean that it is the correct solution for everybody. Some of this increased functionality comes at a cost, there is no such thing as a free lunch. ZixMail requires a connection to the Zixit Corporations public key servers in order to work properly, PGP allows you to build a locally stored public key ring on your computer .PGP is therefore less reliant on that additional server link. I am also very confident that the Zixit Corporation places an enormous importance on their service being available all the time and doubt that this will be an issue. ZixMail also lacks a feature that is inherient to PGP. PGP can be used to encrypt files on the local machine. PGP stores the public keys locally and does not lack the dependency of having to check a server for the public keys, this has its distinct disadvantage when it comes to insuring that you have the latest Public key.

My journey to discover a satisfactory message encryption system has been very educational and rewarding. This paper provides the steps that I took to evaluate several products and ultimately reach my goal of meeting my requirements. Each of the proposed solutions listed may apply in different situations depending on the requirements. ZixMail best met the requirements that I set out to accomplish. I hope that after reading this paper you learned about the differences between symmetric and asymmetric encryption algorithms and have a better understanding of how public keys are used. It would have been more efficient to initially start by locating ZixMail, but then I would not have had the experience of learning the details (Pro's and Con's) of several technologies. I am certain that you will agree that I have adequately described the differences between the various solutions and that after reading this paper you are also convinced that ZixMail has best met the business requirements that I initially set. It is also very important to

[15] Zixit Corporation – Press Relase

remember that the weakest link in the security chain is not utilizing the tools made available. If the tools we provide as security professionals are difficult to use, they will most likely not be used regardless of the stated procedures and policies, it is very important to provide the tools that make it simple (almost second nature) to lock the door.

References

Singh, Simon. The Code Book: the evolution of secrecy from Mary Queen of Scotts to quantum cryptography.New York: DoubleDay,1999. 4

Schneier, Bruce. Applied Cryptography Second Edition: protocols, algorithms and source code in C. New York:John Wiley& Sons, Inc, 1996.

Schneier, Bruce. Secrets and Lies: digital security in a networked world. New York: John Wiley & Sons, Inc, 2000.

Microsoft."Security Features in Office." Microsoft Office 97 Resource Kit. January 1998 http://msdn.microsoft.com/library/default.asp?url=/library/en-us/office97/html/ORKht/034.asp

Password Recovery ToolKit. http://www.lostpasswords.com/Product00_Overview.htm?ProductNum=00 (27 Dec 2001)

MIT Distribution Center for PGP (Pretty Good Privacy http://web.mit.edu/network/pgp.html (Nov 2000)

SANS Institute. SANS Security Essentials IV: Encryption and Exploits. p3-19

"An Introduction to Cryptography." p9. http://www.pgpi.org/doc/pgpintro/#p9 (Jan 2002)

"An Introduction to Cryptography." p12http://www.pgpi.org/doc/pgpintro/#p12 (Jan 2002)

Hilton, Ron. "Secure Messaging" (7 Nov 2000) http://rr.sans.org/email/messaging.php (Nov 2001)

Zixit Corporation. ZixMail and ZixMail.Net Basic Encryption and Delivery Processes http://www.zixit.com/products/ZixMail_Technical_Paper.pdf (Dec 2000)

Zixit Corporation. “Press Release: Zixit Expands Family of Secure Messaging Solutions with ZixBlast and ZixVPM.” 11 Sep 2001. http://www.corporate-ir.net/ireye/ir_site.zhtml?ticker=ZIXI&script=410&layout=-6&item_id=205897

Last Updated: August 17th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Adelaide 2017	OnlineAU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced