Email Security Risks and How To Reduce Them

David Gibson
GSEC v1.4 Option 1
May 16, 2002

Abstract

Email is an often-overlooked exposure area when assessing or evaluating an organization's overall security risk. Firewalls may be implemented to protect traffic to or from a system connected to the Internet, along with strong password policies and enforcement. However, unless care is taken with information transmitted via email, or encryption used to protect the contents of email, organizations could be compromising their security by giving away key information about themselves. Email is sent and received as clear-text, and can be intercepted anywhere along it's transmission on the Internet. This paper will examine the exposures, their ramifications, and the possible defenses one can use to manage the risks.

This paper assumes the reader knows how to download and install programs on their computer, and are familiar with email software and the basics of configuration i.e. SMTP (Simple Mail Transfer Protocol) and POP3 (Post Office Protocol 3) servers, passwords, etc.

Introduction

When we think of the Internet and security exposures, we think of hackers using software tools to obtain confidential information from users and/or the systems they use. We use elaborate means to ensure our private information stays private. We are wary of entering our credit card numbers when ordering online for fear of someone stealing them. We make sure no one is looking over our shoulder when entering our passwords, and shred documents that may have confidential information in them. But because of the ease and convenience created by email communications these days, information we may include in an email could circumvent every safeguard we have in place.

Email Popularity and Exposures

Email usage has enjoyed phenomenal growth along with the Internet, because of the ease of communication it provides. Information can be sent to another person instantly, whether or not the other person is available (unlike the telephone), and can be sent virtually to anyone in the world in a split second. It allows us to carry on a conversation with someone on our own terms, at a time that is convenient for us.

It is this ease of communication that can cause problems. Particularly, in how quickly and easily we can communicate to someone. The communication could include information we would not consider saying in person; or we might have a tendency to include more information than we should. We key it in quickly and hit send, then wish we could retrieve it after thinking about it.

Before widespread use of the Internet when email systems were proprietary (i.e. online services such as CompuServe), if you wanted to send email to someone, they had to be a member of the same online service. Email sent and received stayed on the same secure system, but the chance of the intended recipient being on the same online service was slim. As online services began to implement gateways to the Internet, they enabled users on one service to send email to a user on a different service by using their Internet address. Now when email was sent, it left the secure environment of the online service's mainframe computer and was routed to the other user's online service via the Internet. The interface is still the same, and if we think in terms of the secure online systems we were used to, it is easy to think our communications are secure.

Email Insecurity

By design, the protocols that are responsible for the transfer of email on the Internet send everything clear-text (i.e. visible to any computer on the network) as stated in Request For Comments document #1939:

> Normally, each POP3 session starts with a USER/PASS exchange. This results in a server/user-id specific password being sent in the clear on the network. For intermittent use of POP3, this may not introduce a sizable risk. However, many POP3 client implementations connect to the POP3 server on a regular basis -- to check for new mail. Further the interval of session initiation may be on the order of five minutes. Hence, the risk of password capture is greatly enhanced[1] (Myers & Rose)

Each time our email client software communicates with the mail server, the mail sent and received is in clear text, including the password we use to access our mailbox. Depending on the distance to your mail server, your transmission could be routed via multiple servers on the Internet. Anyone with a mail server could configure it to save copies of all email for review later. A common analogy to the open nature of email is the comparison of it to a "postcard written in pencil", giving anyone along it's path the ability to either copy the data, or change it.[2]

How easy is it for someone to gain access to the Internet and monitor the millions of email messages that are sent each day? With tools readily available via the Internet, software such as mailsnarf (one component of Dug Song's dsniff package) can sniff (record network traffic as it passes without interrupting it) email related packets off the wire and re-assemble entire email messages into a format that any email client software can read. Dsniff has the ability to snag passwords from passing traffic.[3]

In spite of this exposure, the lack of news about it (in contrast to the amount of media coverage over the latest virus release) can create a false sense of security.

Problem? What Problem?

If it is so easy to monitor email, why don't we hear of this occurring more often? Fortunately the amount of traffic on the Internet to monitor and the number of messages that have no valuable or confidential content makes the work required to sift through all of the messages for useful data not worth the effort. However, as more people begin using email the amount of useful data increases (i.e. credit card numbers, bank account numbers, online shopping site passwords, etc.), making it advantageous for someone to monitor email traffic more closely.[4]

Why Me?

What do I have on my computer or include in emails that anyone would be interested in? The answer depends on whether you think about the exposure before sending email. We would never intentionally include confidential information in an email, unless we forget and are not cautious. I have personally experienced these occurrences:

- At a class out of town, a classmate called his spouse and wanted to know the PIN code for their bank account. She sent it to him in an email.
- I placed an order for items on a secure website. They sent me a confirmation email, including my full credit card number and expiration date.
- A person in the accounting department emailed copies of confidential financial reports in text format as an attachment to their accountant.
- A network administrator emailed a Microsoft Visio document containing network configuration details.

Email exposure is both a social, as well as a technical problem. It becomes comfortable because of its convenience, and we often forget it's open nature. Consider emailing another about an upcoming trip out of town for the weekend, and without thinking, you ask them to come by the house and check on things,

and in case you forgot, the code is 4567 and the key is in the planter. Armed with this information and a reverse lookup of their email address, their home address can be accessed (or possibly sniffed from previous emails). Now an unknown party knows where they live, where the key is hidden, and how to disarm the burglar alarm.

If you think you have nothing private to say, the following illustration points out the pervasiveness of information that could be potentially damaging:

> Perhaps you think you have nothing to hide and don't need secure email. Would you ever find it embarrassing if your email is read by your sysadmin, your employer, your ISP, an unknown hacker, or government intelligence agencies? Do you ever use email to transmit confidential information like business plans, character references, credit card numbers, political strategies or love letters?[7] (Queen)

Identity Exposures

Another equally important aspect is if someone is capable of intercepting emails to or from you, they are also capable of capturing your email, modifying the contents, and re-sending it as though it were from you. The content of your message may not be confidential, but there may be instances where you want the recipient to be able to verify the message is from you. For example, authentication of the sender would be beneficial because of the current proliferation of viruses that automatically email everyone in a user's address book. If the identity of the sender could be verified, you could determine whether or not you want to open the email or discard it.[5]

What Can I Do To Limit My Exposure?

The most effective step in protecting yourself is to acknowledge the open nature of email and think before sending. Email should be treated as public i.e. any information you would not disclose to a caller (employee names, passwords, financial reports, server names, etc.) should not be emailed unless it can be secured.

Before sending, ask yourself if there is any information enclosed that I would not want posted on a bulletin board for everyone to see? If so, perhaps there is another way you can send the information. You could call the addressee and give it to them on the telephone. Faxing the information is another way to protect your information (a popular way with online purchases; many sites give the option of calling or faxing credit card information).

If you are an administrator in charge of a network, educate your users on the proper security state of mind. We all know not to divulge information about the company or it's employees unless the person asking has a need to know. Transfer this concept to email communication to make sure users are not disclosing too much information.

Another option is to use software to encrypt the contents of your emails so if they are intercepted, they will be unintelligible to anyone except yourself or the addressee. One example of a popular encryption software package is Pretty Good Privacy, or PGP, available free for personal use at the MIT Distribution Site for Free PGP.[6] PGP can be used to encrypt the contents of files on your hard drive as well, and has plug-ins for the most popular email programs, making it easy to use. PGP v6.5.8 is the latest freeware version for Windows 95/98/NT/2000.

How Does Encryption Work?

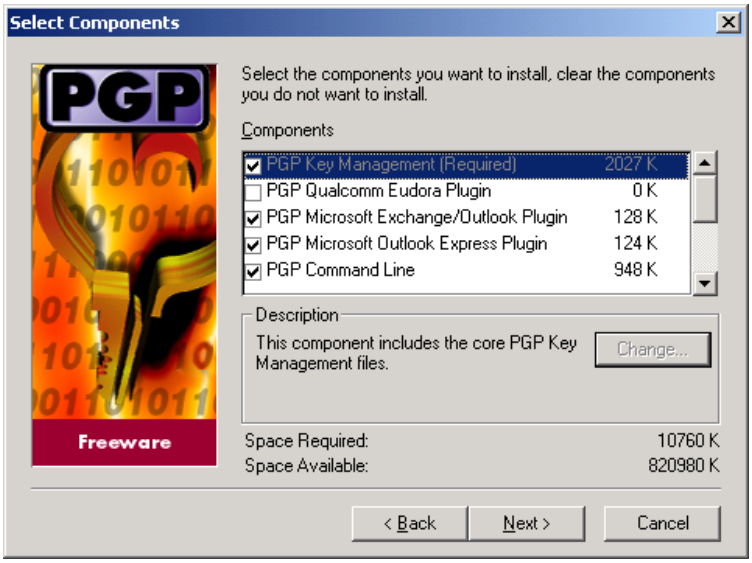
Encryption is the process of scrambling the contents of a message by using a key (pre-defined data used to determine what bits are moved where, and changed to what) so that only those persons who possess the key can decrypt the message. The disadvantage of single key encryption is that both parties must know the key, which requires an exchange prior to sending the message. Exchanging the key in a non-secure manner negates the process, and if a secure means of transmission were available, you might as well send the message itself.[7]

Public-key cryptography eliminates this problem by using two keys, a public and a private key to encrypt messages. These keys are based on what mathematicians call one way functions, or a relation between two objects, A and B, such that B can be readily calculated from A, while there is no computationally feasible way of determining A from a knowledge of B[7], i.e. it would take multiple computers many years to crunch the numbers necessary to determine the value of A. When you install PGP, it creates these keys; the public key is distributed to other individuals you intend to exchange secure email with, and the private key is kept secret. To encrypt with public-key cryptography, you use the addressee's public key and your private key to perform the encryption. The addressee then uses their private key and your public key to decrypt the message.

A good overview of encryption and security, which compares the process to a postman carrying the mail, can be found in a paper written by Alan Bleasby.[8]

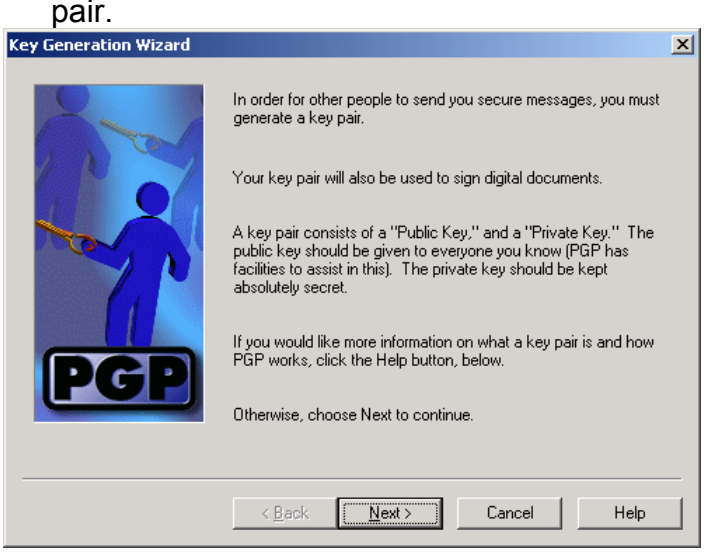
Steps to Install PGP

1. Download PGP at the MIT Distribution Site for Free PGP[6], unzip the program files, and run setup.exe.
2. After the initial information windows and licensing agreement, you will be prompted for your Name, Company, and installation location. Use the default location unless you have a need to install elsewhere.
3. On the select components screen, PGP Key Management is required. Choose the plug-ins for any email programs you use. Also install the PGP documentation, which contains helpful information regarding program usage. PGP Command Line is optional if you only plan to use the GUI interface.



4. After pressing Next to proceed and the files are installed, check the box marked Launch PGPkeys and press Finish to complete setup.

5. You are now presented with a screen to generate your public/private key pair.

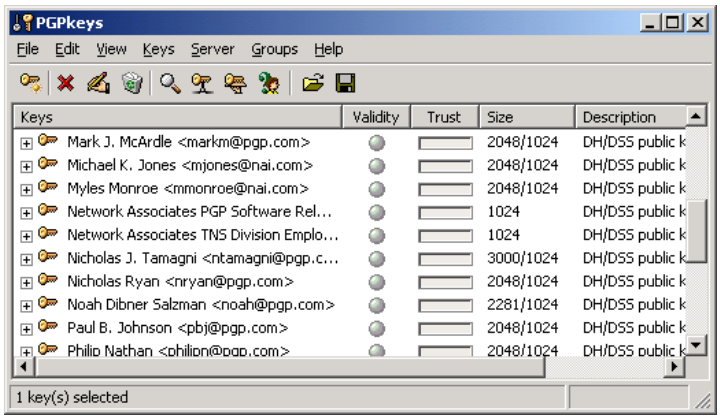


6. Enter your name and the email address you plan to send encrypted email with. Caution – if you change email addresses later, you will have to generate another public/private key for it.

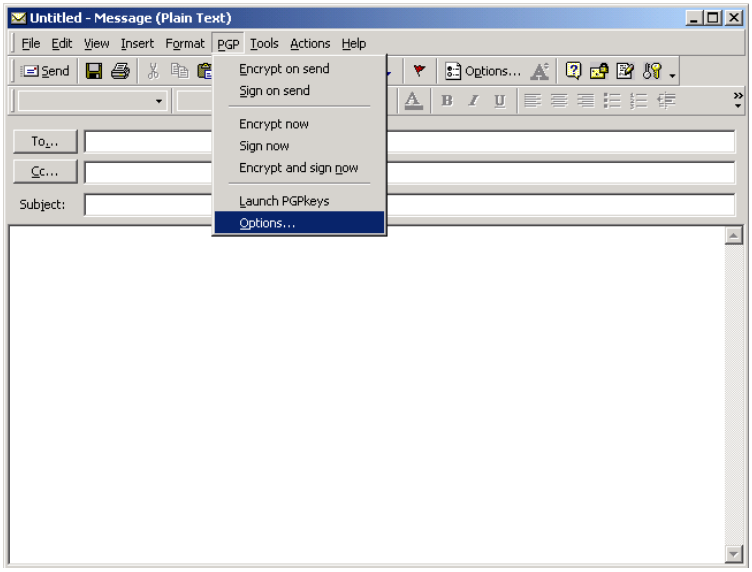
7. You will be prompted for the type of key to generate. Typically you will want to choose the default (Diffie-Hellman) with a key size of 2048 bits.

8. When prompted to set an expiration date, keep the default key pair never expires. Next you will create your passphrase. The passphrase protects your private key, and is hashed (a hash is a one-way operation that transforms a string of data of any length into a shorter fixed-length value) to encrypt your private key. As you key in your passphrase, the passphrase quality bar will increase in length corresponding to its level of security. Use a passphrase that is easy to remember, yet long enough to provide adequate security. NEVER WRITE YOUR PASSPHRASE ANYWHERE. Anyone that knows your passphrase can encrypt and sign email for you. If you forget your passphrase, you can no longer decrypt emails and files encrypted with it.

9. After generating the passphrase, you will be prompted to send your key to a public key server, which is optional. Storing your key on a server makes it easier for others to find your public key and send you encrypted email. You can also export your key to a file in the PGPkeys program, and give this to someone else via email (less secure) or in person (more secure). PGPkeys already contains keys for users at PGP (which you can delete) plus the one you created for yourself. For each key, you can assign a level of trust, lower for keys you receive via email, highest for keys traded in person.



10. When PGP installs it's plug-in for Outlook, it creates a new menu item called PGP and creates additional buttons with locks and keys on them to select either signing, encrypting, or both. In PGPKeys, you can set options to always encrypt new messages, always sign new messages, or both, eliminating the need to select these manually.



Why Isn't the Use of Encryption More Widespread?

Use of encryption for email has not been widely adopted, mainly due to a lack of knowledge about the subject, and users not being aware of the need for it. For some, the concept is only as good as the software they can use to implement it, and getting up to speed with Internet browsing and email are difficult enough without introducing another concept, more software to install, things to remember, etc.

To summarize the advantages and disadvantages:

The advantages of PGP are:

- The program is free for personal use.
- Of all encryption software in use today, PGP is the most popular, with multiple key servers available for key storage and retrieval.
- Plug-ins for popular email programs makes it easy to use.
- It can be used to encrypt files on your hard drive to hide sensitive information in spreadsheets, documents, etc.
- It can securely delete files (called wiping), which overwrites files multiple times before erasing them so that no trace of the original file is still on your hard drive.
- If you make it a habit of signing your email before sending it, and then were infected with a virus that sends email to everyone in your address book, the recipients would know to discard your message and it's attachment if it were not signed by you.

The disadvantages of PGP are:

- The majority of email users today do not use PGP, or any method of encryption, giving little opportunity for using it on a regular basis to stay familiar with it.
- Cryptography is a foreign concept for most people, and keeping up with keys, passphrases, and trust can be overwhelming for the casual user.
- Bad press relating to how encryption technology has been used in plotting terrorist attacks (a major point of contention, the debate of which is on-going).
- If the particular email software you use does not have a PGP plug-in available, it can be a challenge to use.

It is important to note the majority of PGP's disadvantages can be eliminated with the first step below.

To increase the reliability of PGP:

- Install it and practice using it. If a need arises and you do not have the program available or know how to use it, it's easy to just go ahead and send the email plain text instead of going through the installation, key generation and transfer. As it is used, it becomes second nature and easier to utilize.
- The passphrase is the weakest link of PGP. The creation of the passphrase is a balance of choosing one secure enough it cannot be

guessed, yet not overly complex to ensure it can be remembered without writing it down.

- To ensure optimal trust, the best method of key exchange is to have the persons you correspond with give you their key in person so you can verify the key is in fact from them. A key attached to an email can be intercepted, and the interceptor can use the key to impersonate you. In your key ring, you can specify the amount of trust you have in the validity of a person's key.

Summary

In determining an overall security strategy, all factors must be investigated because the best defense is only as good as it's weakest component. While we use firewalls with hard and fast rules to determine what comes in or goes out of our network connection, the content of email is a variable that is difficult to control.

Email presents more of a social, rather than technical challenge that requires special attention to reduce exposures. Education is key since the variable in the equation is the person sending the email. Knowledge of the open nature of email and the weakness it creates are crucial to maintaining security.

Not knowing about an exposure or not hearing of a weakness being exploited offers no protection; it's often not if, but when someone will choose to exploit the weakness.

The exposures are not limited to intrusions into our privacy, but also theft of our identity or using information gleaned from those intrusions to send message and make commitments on our behalf.

Knowledge of these factors, in addition to the use of software and technology to protect our private information, ultimately provide the best defense.

---

[1] Myers & Rose "Network Working Group Request for Comments: #1939 – Post Office Protocol Version 3" May 1996
URL: http://www.ietf.org/rfc/rfc1939.txt (14 May 2002)
[2] Rogers, Larry "Email – A Postcard Written in Pencil" 28 February 2002
URL: http://www.cert.org/homeusers/email_postcard.html (14 May 2002)
[3] Edwards, Mark Joseph "Think You're Safe from Sniffing?" 1 June 2000
URL: http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=8878 (14 May 2002)
[4] ONE/Northwest (Online Networking for the Environment) "Encrypting your email with PGP"
URL: http://www.onenw.org/bin/page.cfm?pageid=37 (16 May 2002)
[5] DigitalGhost "PGP and Your Email" 2001
URL: http://www.spectrenet.org/privacy_article01.htm (15 May 2002)
[6] MIT Distribution Site for Free PGP

URL: http://web.mit.edu/network/pgp.html (15 May 2002)
[7] Queen, Nat "PGP for secure email" February 2000
URL: http://www.senseofsecurity.com/yPGP.asp (15 May 2002)
[8] Bleasby, Alan "Email Security"
URL: http://www.hgmp.mrc.ac.uk/embnet.news/vol5_4/body_email_security.html (15 May 2002)
McCune, Tom "Tom McCune's PGP Questions and Answers"
URL: http://www.mccune.cc/PGPpage2.htm (15 May 2002)
Garfinkel, Simson PGP: Pretty Good Privacy
O'Reilly & Associates, Inc.: 1996
"How PGP Works"
URL: http://www.pgpi.org/doc/pgpintro/ (16 May 2002)