E-MAIL Security

(Is That An Oxymoron?)

By: Russ Licht
100 Lake Hart Dr.
Orlando, FL 32832
407-826-2825
russ.licht@ccci.org

February 22, 2002

TABLE of CONTENTS

TABLE of FIGURES

INTRODUCTION

The global Internet and worldwide use of e-mail has allowed people to experience immediate intimacy and anonymous intimacy via electronic messaging. Conversations that used to take place only when two people were together in private are now flowing at the speed of light across vast distances. Frequently the conversants have never even met. The contact feels very personal, but in the midst of that feeling we all tend to forget that our electronic conversations are no longer protected by doors, walls and windows.

The simple phrase "Electronic Mail (e-mail) Security" actually encompasses a multi-faceted group of issues for which there is no one solution. It will be helpful for this discussion if we think about the "life-cycle" of an e-mail message and review the paths it might travel. Toward that end, I'll define some terms, describe some diagrams and enlist you in the fun of trying to think like a thief!

Not covered in this discussion are issues of reliability. Lost or corrupted messages lessen one's trust in the system but are not directly related to having unwanted people viewing messages. Likewise, we will not deal directly with virus protection, though some viruses, or more correctly, Trojan horses and worms do pose an indirect security threat.

OBJECTIVES

After reading this document you will:

- ❑ Understand the 5 basic elements of an e-mail system
- ❑ Be able to diagram the path of an e-mail message
- ❑ Understand some basic security technologies
- ❑ Be able to separate the security issues in order to understand which group of technologies applies to which problem
- ❑ Understand a few basic hacker techniques used to steal information
- ❑ Understand some basic intelligence techniques used by those who want to uncover or track your activities in "Creative Access" (CA) countries

E-MAIL SYSTEM BASICS

The five basic parts of an e-mail system are: Client Software, Message Store, Message Transport, Management Systems and Gateways. We will dwell primarily on the first three.

Client Software

Users are most familiar with the Client Software that allows them to read, address and send messages. Client Software connects to the Message Store and displays the messages kept there. It may also connect to the Management System to display a centralized address book (a.k.a., directory). Most modern Clients keep a separate local address book for personal contacts.

Message Storage: Semi-permanent

The Message Store can exist in more than one place at the same time. In offices where workstation computers are all connected to file-server computers with a LAN (local area network) it is best to keep all e-mail in one main Message Store on the server. Client software at the workstation views messages from the server but does not make a separate local copy of it. This is the typical model for proprietary e-mail systems like Exchange, Groupwise and Notes.

Remote users with laptop computers or home computers will usually connect in a different mode that lets the Client make a local copy of some or all messages. If the remote user is connecting to a corporate e-mail server he typically keeps a synchronized secondary copy of his personal message store on the remote computer hard drive. If he is collecting his e-mail from a mailbox provided by his Internet Service Provider (ISP) he will normally copy his messages from the ISP and then delete the original from the ISP e-mail server.

Message Storage: Transient

Thus far, we have discussed semi-permanent message storage. There are also transient Message Stores that keep a copy of the message until it can be sent onto the next destination in its journey. This is commonly referred to as "Store-and-Forward."

Message Transport

Message Transport Agents (MTAs) are software systems that keep moving messages along to the intended destination. The first MTA exists in the Client Software that connects with its counterpart on the e-mail server.

MTAs always exist in pairs and must agree ahead of time on how they will communicate with each other. These pre-defined communication standards, or protocols, can be open-standards that are widely used by many products or proprietary and are used only between software packages from the same company. Some open-standards protocols are: SMTP (Simple Message Transfer Protocol) for sending and either POP3 (Post Office Protocol) or IMAP (Internet Message Access Protocol) for receiving.

Within a single MTA, a message will usually be moved more than once to different directories on the hard drive using file copy facilities built into the operating system of the host computer. These hard drive directories, dedicated to message traffic, are also known as queues because the messages are dispatched again according to the order in which they arrived.

Management Systems and Gateways

Management software is used to create user mailboxes, to maintain address lists and routing information, and to monitor message traffic. Gateways are needed only if a message must be translated in order to travel from a proprietary, private e-mail system to another, or to the public Internet mail system.

MESSAGE PATHS- From a Private LAN

The diagram in **Figure 1** gives a comprehensive, overview of a corporate e-mail system with connections to the global Internet e-mail system. For purposes of discussion, we will detail five typical message paths and note where temporary or permanent copies of a message were made during its passage.

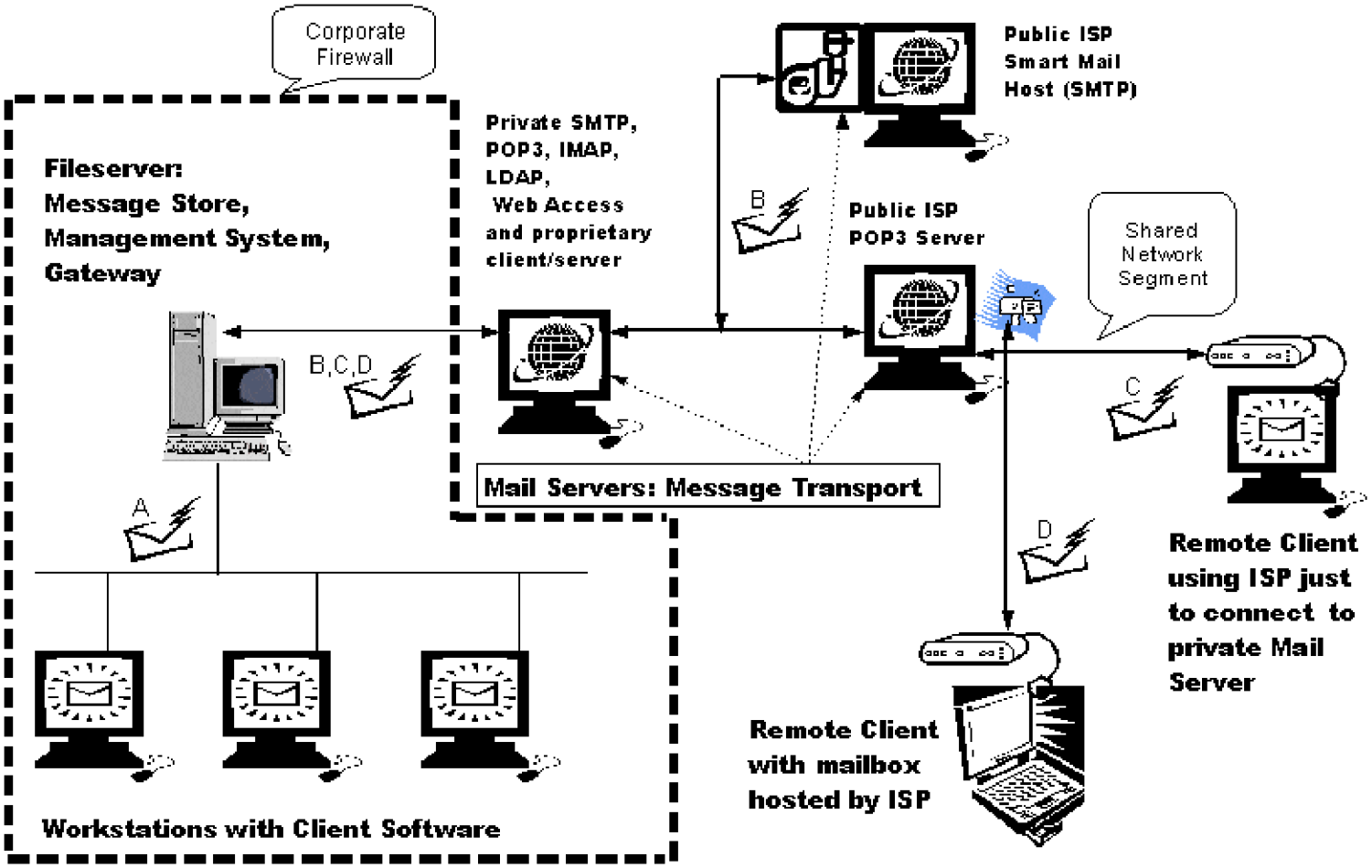

Figure 1 - Examples of 5 basic e-mail components in both private and publicly hosted e-mail systems.

Message A – An Internal or Intra-Office Message

This message never leaves the secure private LAN of the corporate offices. It gets written by one user, is stored on the file-server, gets read by another user at a different workstation, but is never copied or stored on the hard drive at either workstation. * The contents of the message may be viewed over the LAN many times without ever being copied.

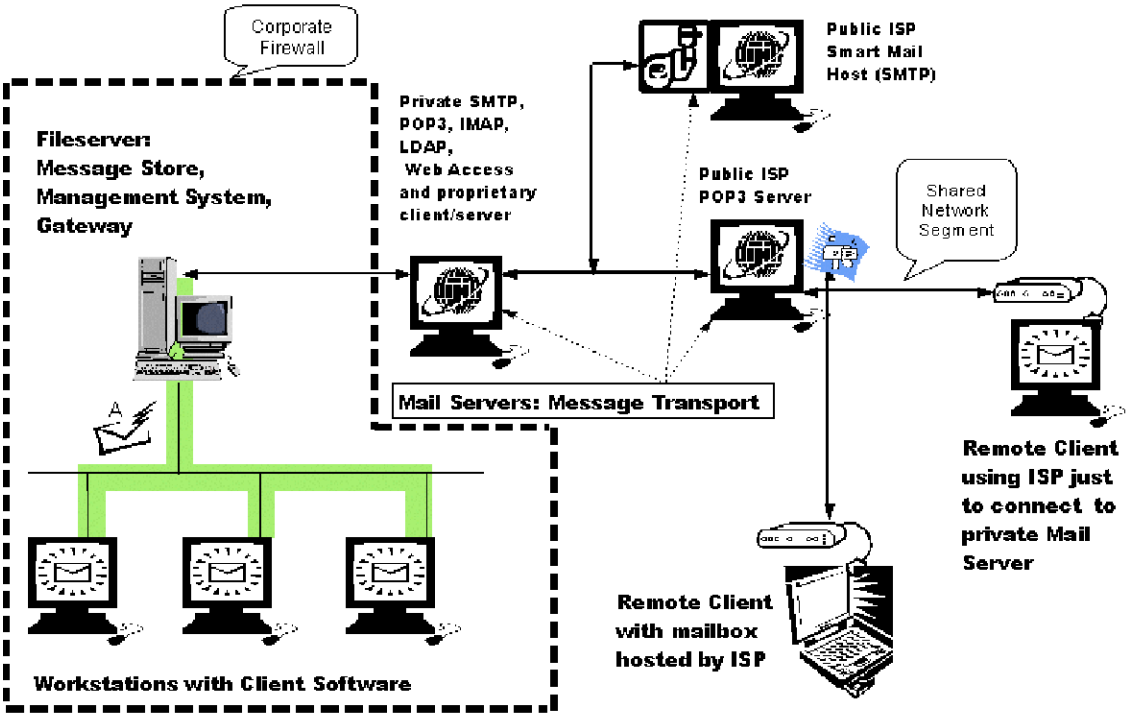

Figure 2 – Message A: Private internal e-mail messages

*

A little known foresenics factoid deserves mention here. If you view a message on the LAN message store but never make a copy to your local hard drive it is still possible that a ghost-like copy of it might be left on your hard drive. Most operating systems employ a swap file for making copies of RAM to allow other tasks to have access to that same RAM space. The swap file might get written and re-written many times over to various segments on your hard drive. It is possible that an IT foresenics expert could use special tools to read old swap file data from portions of the drive. Unless you are currently under indictment by a grand jury, or have been subpoened to turn over all your computer files I wouldn't worry too much about this possibility.

☺

Message B – To An External Office Outside the Corporate Network
This message is typed by a user inside the corporate LAN, but is destined for a recipient on some unknown e-mail system elsewhere in the world. Let us imagine, in this case, that the recipient is in a small office that gets connected to the Internet via a dialup account rather than an always-on service. Because the final destination does not have constant Internet connectivity it has directed an intermediary to act as a "Smart Mail Host" who holds the message until it is ready to receive it.

The reverse path is similar. The remote office dials out to its SMTP host who keeps a copy of the message until it can find the recipient e-mail system and forward the message on. This Store-and-Forward process is very common, and could even happen between two sites who normally have 24 hour Internet connections, because every SMTP mail host has at least one secondary mail server designated to receives its mail in case of a service outage or catastrophic failure.

Message B is first stored (and has a copy kept semi-permanently) on the private internal file-server, and is then forwarded to the MTA machine that has access to the public Internet. It is stored there temporarily and again for a longer period on the remote "Smart Mail Host." The first leg of its journey is over the private, protected LAN. The next two parts of its trip is made over public, unprotected Internet systems. The final leg may be another private LAN. Its final repository is on a hard drive in the remote office.

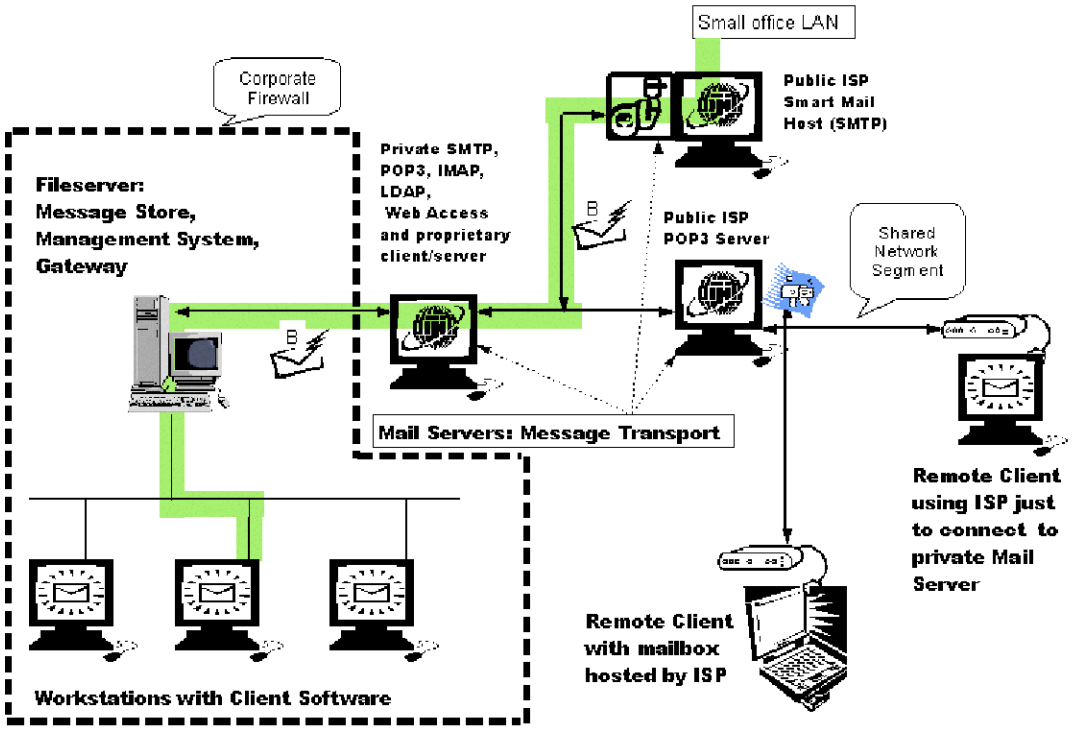

Figure 3 - Message B travels from large office LAN to small office LAN.

Message C – An Internal Message Accessed from Outside the Corporate LAN

This message has a dual life. It is first written and stored inside the private LAN just like Message A. The originator and/or the recipient also have computers that connect to the corporate LAN from outside the building. They use the public Internet just to establish a connection with the office. Using that temporary connection they make copies of their messages to work with later off-line.

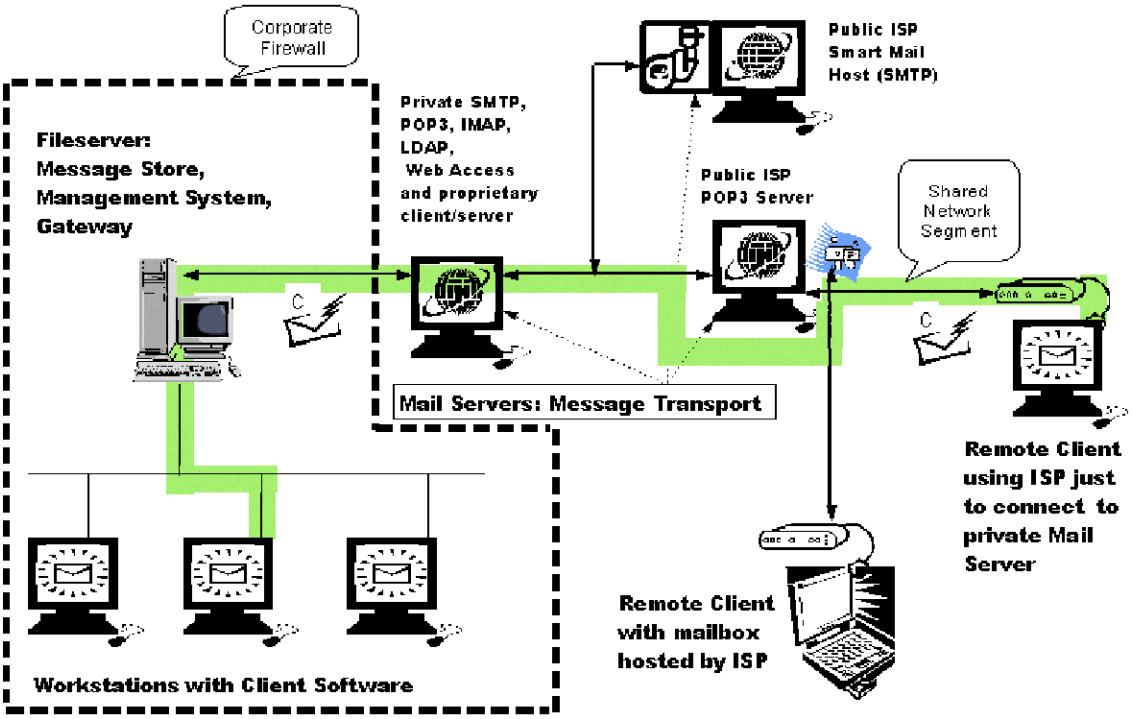

Figure 4 - Remote access to the private LAN to make copy of Message C for offline work.

Message C gets stored in two or three places: on the file-server, and on one or both remote user's hard drives. It transits the public Internet; possibly via the open-standards protocols of POP3, IMAP or SMTP. It does not, however, get stored temporarily anywhere along the way.

Message D – To An Individual Outside the Corporate Network

Message D is very similar to Message B. The difference is that it sits in a POP3 server rather than an SMTP server while waiting for the recipient to dial in and pick up the mail. Usually the recipient is an individual at home or on the road, rather than in a small office. It is possible for an office to receive e-mail for several individuals via a single POP3 mailbox; this is referred to as multi-drop POP. It is also possible for an office e-mail server to collect mail from several POP3 mailboxes to redistribute to people inside the LAN; this is called multi-POP.

Whatever the case, a POP3 receiver has the option to immediately delete mail from the POP3 server after reading or to wait and delete it later. So a copy of Message D may exist in several locations: on the originating e-mail server, on the POP3 server and on the recipients hard drive. A temporary copy was also made on the originating and possibly an intermediary SMTP server during transit. Just like Message B, the first leg of its journey is over the private, protected LAN. The next two parts of its trip are made over public, unprotected Internet systems.

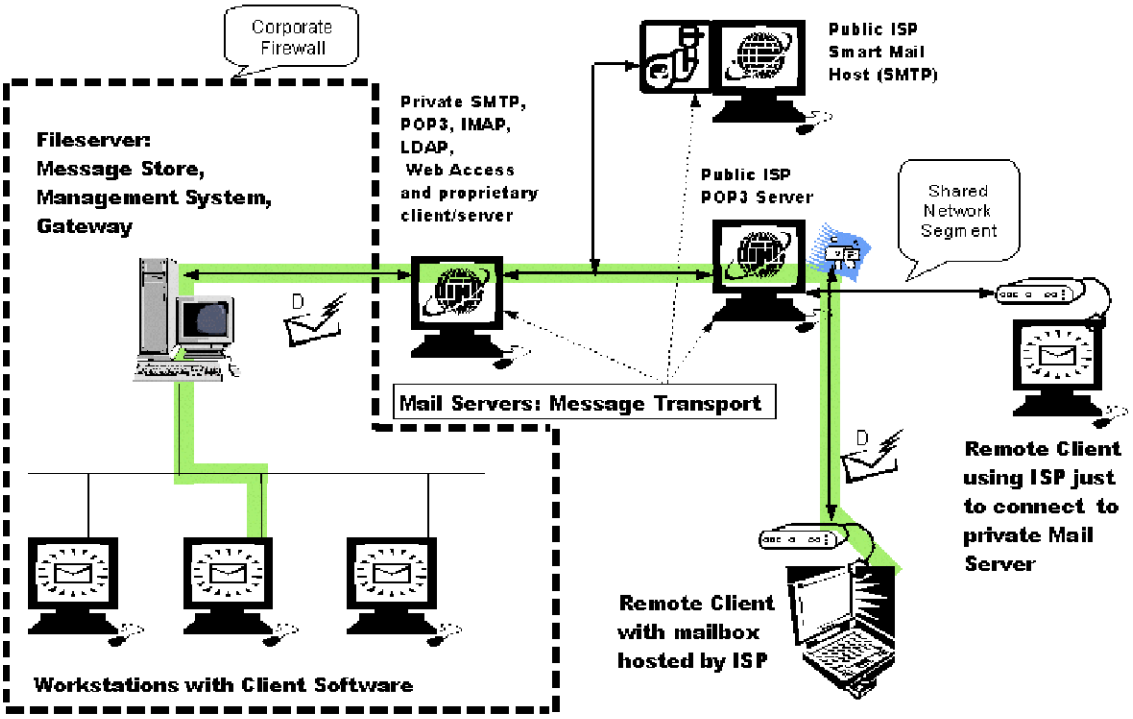

Figure 5 - Message D to a client with a POP3 mailbox hosted by a public ISP

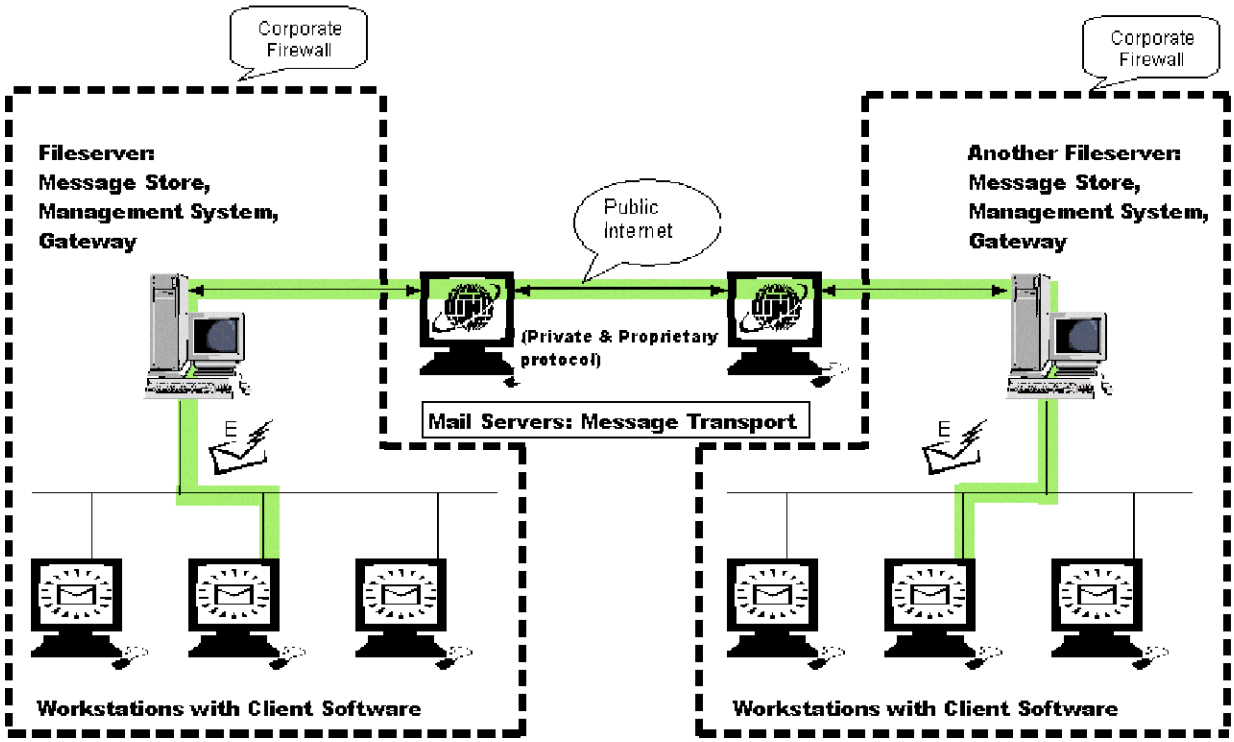

Figure 6 - Message E from private LAN to another private LAN.

Message E – From One Private LAN to Another Private LAN

Note that **Figure 6** has been altered from the original in **Figure 1** to show two private LAN systems connected together. The connection could be a private, leased line, but that would be the same as having the two systems on the same LAN. For discussion purposes, we will suppose that they use the public Internet for a connection.

Message E gets written by one user and is stored on the first file-server. The first and second file-servers connect to each other via mail servers who serve as intermediaries. The message is finally copied to the second file-server from which it gets read by another user at a different workstation, but is never copied or stored on the hard drive at either workstation. The contents of the message may be viewed over either LAN many times without ever being copied.

Temporary copies of the message were made on the hard drive of each of the two mail servers. These servers are controlled and maintained by the private corporation. The message transits both private LANs and the public Internet.

MESSAGE PATHS- Life in the Public Eye

For completeness, let's include three more example message paths. These messages never see the inside of a LAN. They originate and end with people who use e-mail services provided for them by public Internet Service Providers (ISPs).

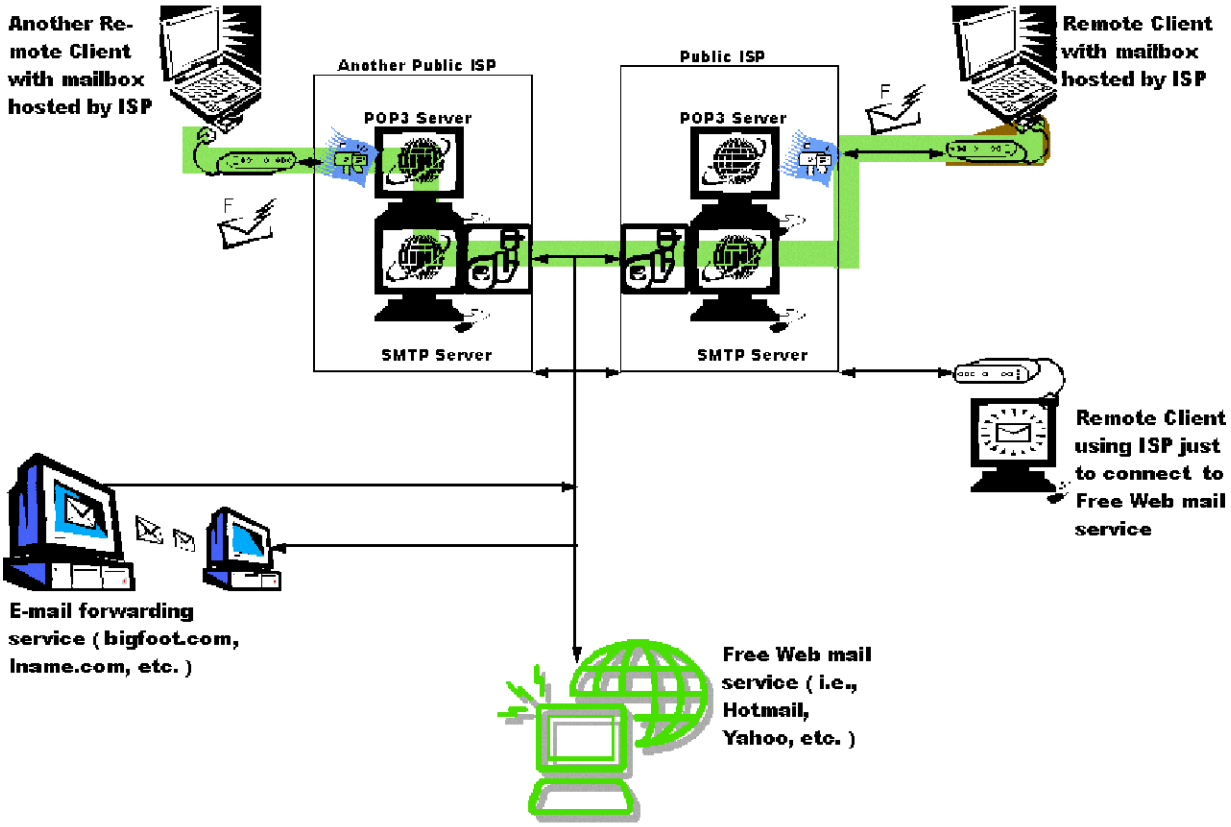

Figure 7 – Message F between two public Internet POP3 e-mail accounts.

Message F – From One Public Internet User to Another

This message is typed by a user with a mailbox on a public ISP and is destined for a recipient mailbox on another ISP elsewhere in the world. First the message is typed and queued on the local hard drive of the client machine. A copy of it will remain there. It is then sent on to the SMTP mail server of the ISP. From there it gets forwarded to the mail server of another ISP. Finally, it gets copied into the POP3 mailbox of the recipient.

The recipient eventually dials his ISP and retrieves a copy of the message and probably also deletes the copy kept in the POP3 mailbox. A semi-permanent copy of the message resides on both the originating and receiving client computer's hard drives. It has also been stored temporarily on two or more SMTP servers along the way and the POP3 server. All transmissions of this message are made over public, unprotected Internet systems.

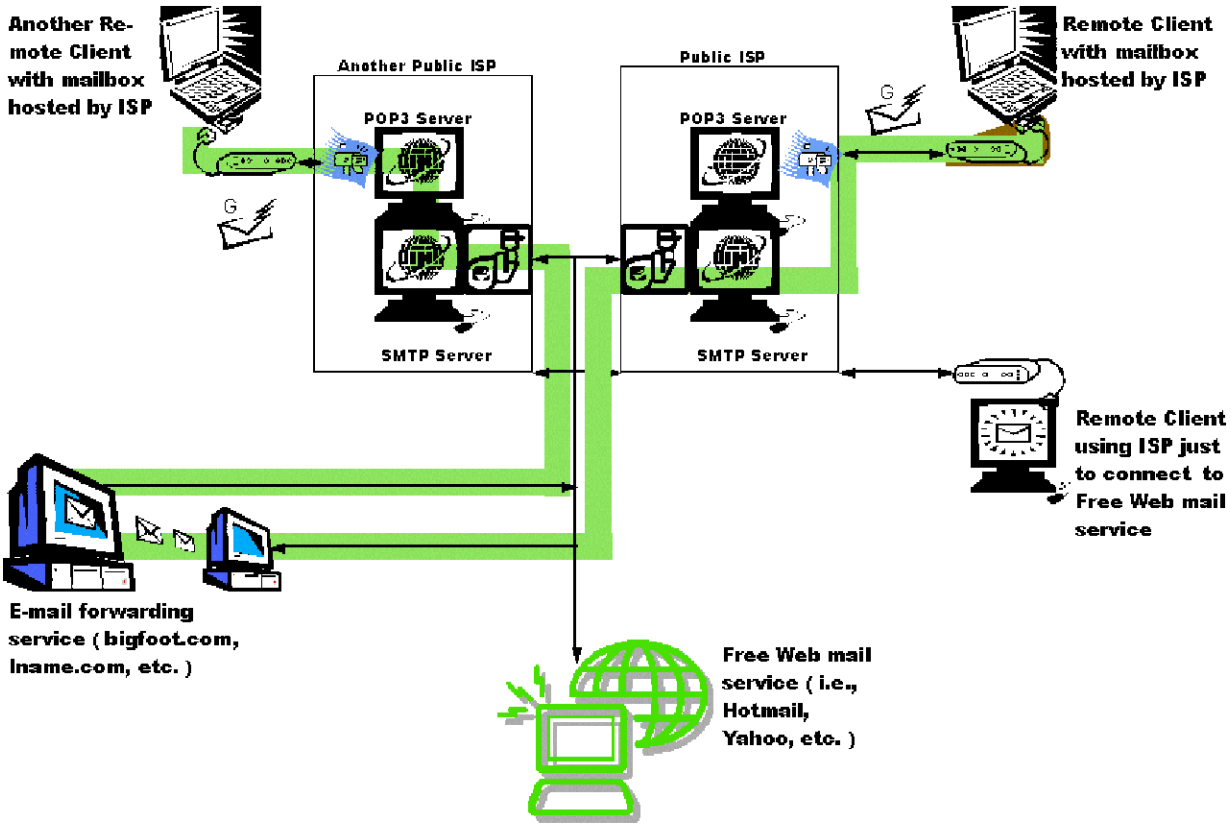

Figure 8 – Message G using an E-mail forwarding service

Message G – Via an E-mail Forwarding Service

Message G is very similar to Message F except that it is originally addressed to an "e-mail forwarding address"(e.g., mymail@bigfoot.com). The forwarding service changes the destination address to whatever has been provided by the recipient (e.g., mymail@ccci.org). Forwarding services are provided to customers who don't know how long they may keep an account with a specific ISP and don't want to have to keep informing people about a new e-mail address every time they change service providers. It also works well for people who want to use different e-mail service providers when traveling.

Like Message F, a semi-permanent copy of the message resides on both the originating and receiving client computer's hard drives. It has also been stored temporarily on three or more SMTP servers along the way. All transmissions of this message are made over public, unprotected Internet systems.

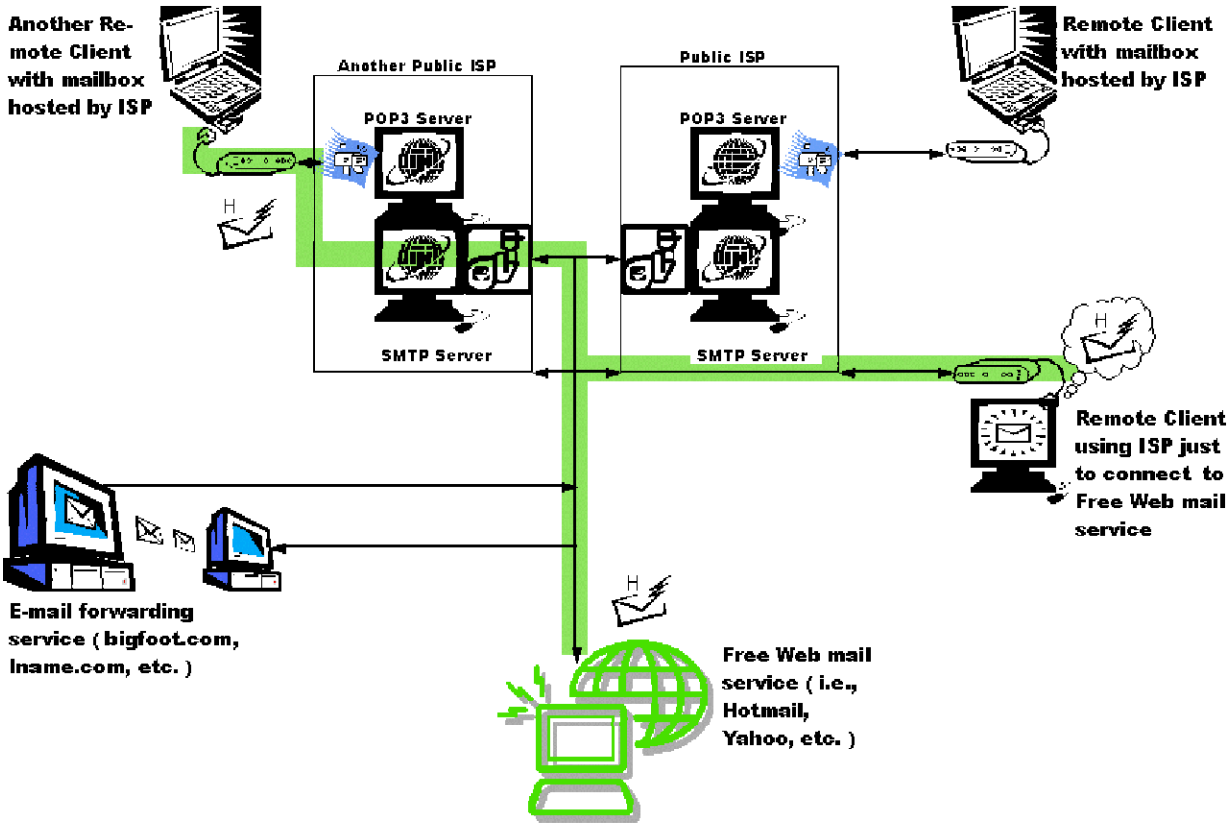

Figure 9 - Web-mail services like Yahoo or Hotmail

Message H – Web-Mail

This is a variation of Message F. The final destination of Message H, however, is the public service provider. It is kept there semi-permanently for viewing via web browser. The recipient has no e-mail client software, and probably does not intentionally make local hard drive copies of the message. Unintentionally, however, the recipient leaves copies of his messages in the "Temporary Internet Files" (i.e., cache) directory of every computer he uses for viewing the messages.

This type of service makes the most sense for people who will be reading their e-mail from many different computers, but seldom from the same computer. This type of service provides some anonymity because its users are from all over the globe and not from one specific geographic region or Internet domain.

VULNERABILITIES

Storage

Individual messages stored as text files in directories are not usually encrypted or compressed. This plain-text format is easily read by anyone who has access to the computer where the message is stored. The messages may be protected by file system security provided by the operating system, but are otherwise vulnerable to viewing.

Database storage of messages is typical of proprietary, LAN-based e-mail systems like Exchange, Groupwise and Notes. The main advantage of database storage is its efficiency and its ability to provide another layer of security protection. This, however, still does not protect you from a rogue system administrator who has access to all the software and security clearances necessary to tap into that database.

In general, server computers implement much better file system security than workstation computers. This means that only people with the proper clearance may view files in any given directory. Likewise, server computers are more likely to be protected by backup systems, Internet firewalls, and physical protection from fire, theft, and third-party viewers. If the server is kept on your own organization's property and is maintained by trusted, and qualified technicians, you can have a much higher level of confidence in the security of your message store.

If you keep a copy of e-mail messages on a local hard drive, a wise, but poor data thief who wants to read your e-mail needs simply to break into your home or office and steal your computer. This beats spending time and money on sophisticated hacking techniques and is easily disguised as simple burglary of expensive electronics. I have just recently learned of a real case of this in a CA country. The couple, fortunately, was warned of the theft while they were out of the country and that the security police were looking for them. Their only option was to never return and to have friends help pack up and ship out their remaining household goods. This, of course, exposed their friends to guilt by association.

Transport

While messages are being moved between different computers there is a chance of those messages being viewed by someone else on that same network segment. This practice is commonly referred to as "packet sniffing." Your next-door neighbor could run a "sniffer" program and watch your e-mail traffic if you both connect to the Internet via a cable modem. Sniffer programs are readily available, but must be used by someone with good computer skills, and who most likely has physical access to the same network segment as your computer. It is possible to plant sniffer software on someone else's network, but that takes much more advanced computer skills or special permission.

Carnivore (a.k.a. DCS1000) is a sniffer program deployed by the FBI in the U.S.A. for the e-mail equivalent of wire-tapping. Echelon is another very sophisticated espionage tool used by governments. One aspect of Echelon uses satellites to record wireless communications, including wireless Internet traffic. (The system includes stations run by Britain, Canada, Australia and New Zealand, in addition to those operated by the United States.[1])

Sniffing network traffic is not the only way to observe e-mail messages in transit. After the transmission from one computer to another, the message is copied to a queue on a hard drive. At this point, a clever system administrator could easily make copies for later review. Note that trying to view someone's messages while in transit takes time, skill, and access to network and computer resources.

General Principles Regarding Theft or Inappropriate Viewing

- Messages are more secure from prying eyes when stored in a database on a properly secured file server on private corporate property.
- Messages are somewhat vulnerable to theft when stored on an individual workstation, but are better off there than being left stored with a third-party service provider.
- Messages are somewhat vulnerable to viewing while in transit between computers connected to the public Internet.
- Messages are vulnerable to viewing while in temporary storage during transit.
- Messages are most vulnerable to viewing if left stored on a public e-mail service.

Guilt By Association

When working in CA (Creative Access) countries it is important to guard your privacy carefully. You may not want to be observed in public with certain people. Likewise, if there are several of you doing similar work you would be wise not to all gather in one place. Telephone calls to each other could be taped, but more likely the pattern of whom you call will be observed to see who your associates are.

Similar risks are associated with your computer communications. A private Internet domain name is associated with an organization or an individual. It is not hard to look up the owner of a domain name and find out where they reside or what organization they work for. Public ISPs serve many different types of people, but if many people or organizations of the same type all use the same ISP it becomes an indication that they may all be working together or have similar values. Therefore your e-mail address may give away whom you work for, and the pattern of e-mail addresses you send to will likely reveal your associates.

SECURITY TECHNOLOGIES

Rather than starting out with a plethora of acronyms and a deluge of techno-babble, I'd rather describe different types of security technology. For our purposes we will define five types: Connection Protection, Message Protection, Storage Protection, Physical Protection and Association Protection. Basic to all of the above is encryption.

Connection Protection

As mentioned in the Message Transport section, when two computers connect to each other they must agree on a protocol for transmitting messages between each other. The protocols mentioned (SMTP, POP3 and IMAP) are all "clear text" transmission methods. Anyone who can observe (i.e. sniff) the network segment being used could easily read the messages as they fly by on the wire. This is especially easy to do on wireless networks (e.g. Echelon). Since we use the public Internet for connections, we can't be sure that our messages are not being observed during transmission.

If, however, we encrypted the connections, we might be reasonably assured that a packet sniffer could not understand the traffic he is observing. This encryption must begin with password protection. Clever algorithms have been created to make sure that passwords used to authenticate the user are not observed, but these are not always required. Password protection is also known as "Secure Authentication." It would do no good to protect the connection but reveal the password so that on a later connection someone could pretend to be you and get your messages.

Examples of Connection Protection Technology are:

- SSL – Secure Sockets Layer
- VPN – Virtual Private Networking
- SSH – Secure Shell

If we protect the connection, our message may still be stored in a readable format while in temporary storage during transit, which leads us the next type of protection.

Message Protection

When the message itself is encrypted and there is a way to make sure that only the intended recipient can decrypt the message, then we have protected the message from both sniffers and rogue system administrators who might try to capture copies of the message from temporary storage queues.

Examples of Message Protection Technologies are:

- PGP – Pretty Good Privacy
- Stenography – Hiding messages inside picture or music files

However, if before encryption and after decryption the original and final copies of the message are stored in clear text, then the storage computer may be vulnerable to physical intruders. Likewise, message encryption will not keep the ISP from observing who the correspondents are.

Physical Protection

At the risk of overstating the obvious, I have to mention plain, old-fashioned things like locked doors. Personal computers and private LANs must be protected from burglary, by physically baring unknown people from accessing your buildings. Locked doors, security badges and vigilant receptionists are important. Likewise, burglar alarms, steel gates, and security guards will greatly improve your chances of keeping out thieves.

If your computers are stolen or accessed by intruders they can read whatever they like from your hard drive unless you implement the next type of protection.

Storage Protection

The data stored on hard drives, even networked file-servers, is usually stored in clear-text or un-encrypted format. A UserID & Password might be required to convince the operating system to let you use your files, but the files themselves are not encrypted. Once someone has physical access to the computer the operating system is easy to defeat. Disk encryption is the only real solution for this situation.

Some important pointers for disk encryption:

- Don't trust the disk encryption supplied by the operating system (OS) unless you understand how to use it securely. (Most OS solutions are notoriously insecure unless you take special steps to improve on the standard setup)
- Don't keep the encryption key on the same hard drive that is being encrypted. (This is analogous to putting a key under the doormat.)
- If you must keep the encryption key with the data, make sure your password
    - has multiple lines (i.e. not just one word)
    - is at least 8 characters or longer
    - uses no words found in a dictionary
    - uses at least three of the following:
        - lower-case letters
        - capital letters (upper-case)
        - numbers
        - special characters (e.g. !@#$%&*)
- Consider encryption schemes that keep the key on a smartcard or other device and which also require you to supply a password.

Some good encryption algorithms for hard drives are:

Blowfish – best and fast
Twofish – faster, but new
GOST – older, slower Russian standard
3DES – slower than GOST, but of U.S. origin [2]

(Many products will allow you to choose which encryption algorithms you want to use.)

Now, let's assume that you are protecting your connections, messages, computers and hard drives. Consider the following: Does using encryption make you look guilty of something? If so, read the next section. This is where the real fun stuff begins for you 007 types.

Association Protection

I already breached this subject in the **Vulnerabilities** section, but it deserves further attention. "Guilt by Association" was something our mothers told us to be worried about when we hung out with the wrong crowd. But, what if you are hanging with the "right" crowd in the "wrong" place? I've intentionally used the euphemism of "Creative Access (CA) Countries" to describe places where you want or need to do work, but aren't too sure the locals will appreciate your presence if they really knew what you were up to. Catch my drift?

In the late 1980s and early1990s people began using PGP encryption to protect their e-mail messages. This raised a red flag in many countries that either outlawed the use of encryption or sent the security police to find out what was really going on. Fortunately, large multi-national companies have convinced most governments that they will not invest in a country if they cannot use VPN technology to protect themselves from industrial espionage. The emergence of on-line shopping has also forced the acceptance of SSL encryption in most countries. However, make sure you know what encryption technologies are commonly accepted in a country before using them.

As a foreigner, you can be certain people are watching what you do and who you associate with. The government could certainly keep track of whom you phone and whom you e-mail unless you take precautions to disguise your contacts. (In another document I've gone into more detail about general security precautions for CA countries, so contact me if you need that as well as the following.)

Keeping your own e-mail address a secret doesn't work very well because you need to give it out to other people so they can contact you. You can, however, keep your address very generic by using an e-mail forwarding service that is also used by millions of others. Lets assume you are working in a country that hates American soft drink companies, so rather than using johndoe@cocacola.com, use johndoe@iname.com.

Keeping your e-mail contacts anonymous is the next challenge. You need to abide by the following rules:

- If necessary, use a local ISP account for Internet connectivity, but don't use the e-mail address they give you.
- Likewise, don't use the SMTP mailer they instruct you to use for sending messages.
- Make arrangements to use a protected e-mail service with someone you can trust. This service must require connection protection (SSL or a VPN) for sending and receiving.
- Give people your generic e-mail address, but have the forwarding service send your messages to the protected e-mail service.
- If too many people from your organization are using the same protected e-mail service, then consider using an "anonymiser" service to keep sniffers from seeing what e-mail service you attach to. Anonymiser.com is a good web site to explore if you need this type of service. Another alternative is to get a VPN connection to some site outside your country from which you can then make further e-mail or Internet connections.

An appropriate Level Of Paranoia

What level of protection do you need? After all, security costs money, but a loss of integrity, confidentiality or intellectual property can cost even more. A paranoid person spends way too much energy protecting something of little value, but as the old saying goes, "just because you're not paranoid doesn't mean they're not out to get you." I offer the following guidelines, but each reader must do a detailed analysis of his situation to properly evaluate what level of paranoia he can or must afford.

Intra-Office Communications

People on a corporate LAN presume a certain level of confidentiality when e-mailing each other within the walls of their building (see **Message A** for example). Make sure that confidentiality is maintained for them if they use remote connections to access their e-mail. Require the use of either a VPN to connect to the corporate LAN, as if they were at the office, or SSL for SMTP, POP3, IMAP or Web-mail connections (this pertains to the **Message C** scenario described earlier).

Something which cannot be required, but should be explained to people who connect to the corporate LAN from outside the building, is that they should use the private SMTP mail server provided by the company rather than pointing their e-mail client to the SMTP server recommended by their ISP. One caveat to this recommendation is that some ISPs block access to any SMTP server except their own (although, I don't think this applies to SMTP over SSL).

Inter-Office Communications

Messages B & E are examples of inter-office communications. Unless an e-mail system allows the administrator to designate that connections to certain offices be encrypted (or use proprietary Message Transport Agents) there is no way to guarantee connection protection of e-mail after it leaves the corporate LAN enroute to another company's LAN. Therefore, inter-office communications without special arrangements are the same as communicating with any other user of Public Internet services. It doesn't matter that the recipient is using e-mail in a nice safe corporate environment if the message gets transmitted in clear-text over the Public Internet. See the next section for suggestions on protecting messages sent over the Internet.

Public Internet E-mail Communications

Encrypting messages before they get sent is the only way to stop sniffers and snoopers from seeing your messages as they fly by on the wires or stopover at store-and-forward servers along their way to the recipient. PGP is the most widely known solution for message encryption. Microsoft Outlook also has a message encryption option. Both rely on Public Key Infrastructure (PKI), which is a topic for other publications. [3, 4] The bottom line is that a PKI implementation must be engineered and maintained. It is not as simple as telling users to check a box in their e-mail client software setup. Without a high level of infrastructure support and trust management, PKI simply creates a false sense of security.[5]

Some banks and financial services companies have implemented a creative solution for securing only messages that need to be secure on their corporate web pages. If you need to e-mail someone at that company with confidential data, they encourage you to type the message on a secure web page (SSL) provided specifically for that purpose. This pre-supposes that they then store the message in a privately protected server, which only trusted employees can access. If

they simply turn around and forward the message via a less secure channel to someone at another site, they have defeated the purpose of the SSL web connection.[6]

Creative Access Country Communications

If you live in a CA country then the precautions described under the sections on **Storage Protection** and **Association Protection** in the previous chapter are essential. If you are corresponding with someone in a CA country just remember that unless you are using message encryption your message is still being routed in clear-text format until it gets to the secure, private e-mail service that your recipient is hopefully using. Check it out before you begin corresponding about delicate topics! Are they using a secure, private e-mail service? If not, would an encrypted (or cryptic, i.e. use of obvious code words) message from you expose them? Likewise, always remember that, message encryption alone will not protect the sender and receiver addresses. It will only encrypt the contents of the message.

Appendix A contains a diagram of a secure e-mail service. It details what message traffic is sent in clear-text and what traffic is secured if message protection/encryption is not used. My admonition is that message encryption is a good thing to use if the user has a firm understanding of the "chain-of-trust" issues[3]. It is also imperative that the client software makes it very easy to use message encryption, and very hard to accidentally send an un-encrypted message when, in reality, it should have been encrypted.

CONCLUSION

If you understand the 5 basic elements of an e-mail system you can diagram the path of an e-mail message and distinguish between the different security issues. Then you will be able to understand which combination of technologies applies to each situation. Once you have selected a security technology, make sure you understand its strengths, weaknesses and proper usage. It is helpful to read about a few basic hacker techniques used to try and break whatever solution you have settled on. Then evaluate the risks and make sure you have "an appropriate level of paranoia" before beginning your deployment.

Carefully research a CA country before deploying any security solution there. Make contact with expatriates who have worked in the country and learn from them. Travel there personally, if necessary, to learn from the people you are trying to protect, and to see their circumstances first hand.

1 – "Inside Echelon" by Duncan Cambell (http://www.heise.de/tp/english/inhalt/te/6929/1.html)
2 – "Frequently Asked Questions about BestCrypt Software" section 2.1 (http://www.bestcrypt.com/)
3 – "PGP: Pretty Good Privacy" by Simson Garfinkel, O'Reilly & Assoc., Inc.
4 – "Public Key Infrastructure – The VeriSign Difference", VeriSign Strategy White Paper #98-01
5 – "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure " by Carl Ellison and Bruce Schneier (http://www.counterpane.com/pki-risks-ft.txt)
6 – "PKI – Breaking the Yellow Lock" by Richard Forno, (http://www.securityfocus.com/columnists/60)

APPENDIX – A : VARIATIONS ON A THEME

If you've succeeded in wading through the previous 17 pages you will have concluded by now that securing e-mail correspondence is a very complex subject. This appendix will diagram several combinations of security technologies applied to the task of protecting the connections, people associations and message contents from prying eyes for a person working in a CA (Creative Access) country.

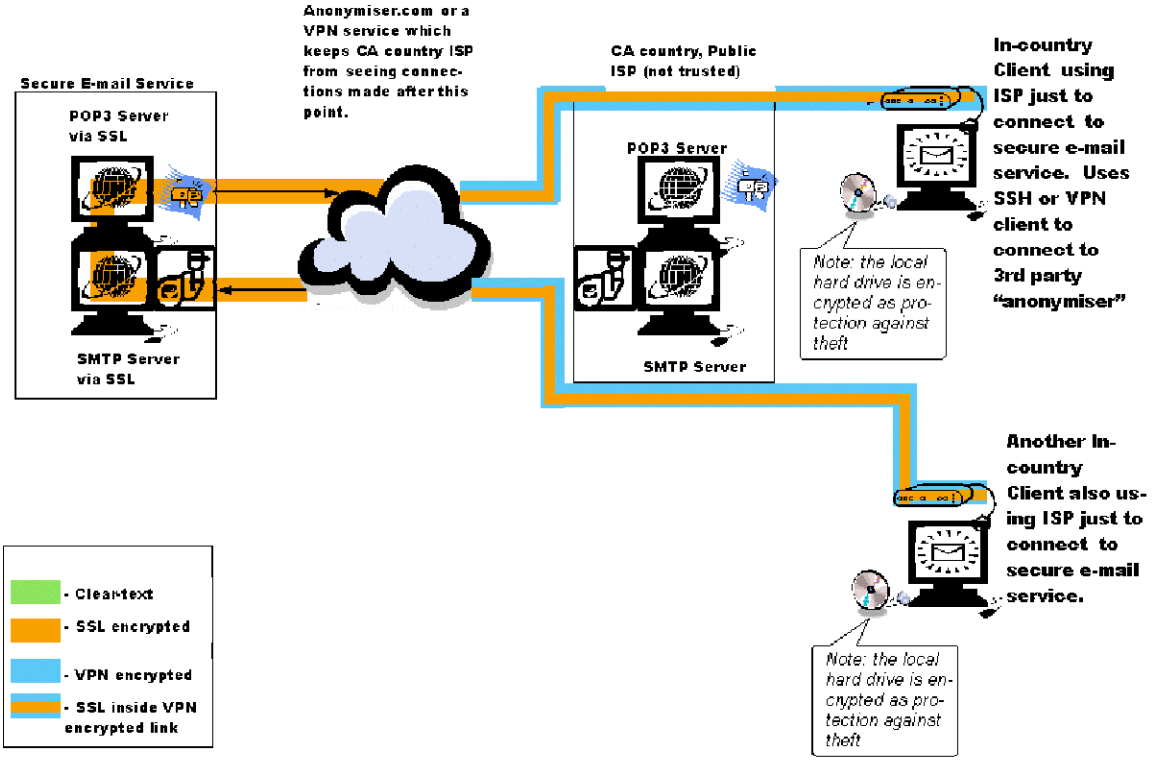

Figure 10 – SMTP and POP3 over SSL via VPN-type connection

Two Correspondents Both Working in the Same CA Country

Figure 10 shows two people, supposedly unaffiliated, who want to correspond without the Host country observing their contact with each other. They each keep the messages on their local hard drives stored in an encrypted format. Each uses a VPN service or Anonymiser.com to blind the Host country ISP from recording where they connect for sending and receiving e-mail. The local ISP can observe that both connect to such a service, but can't see past the encryption cloud to find where they go from there. Ideally, it would be best if they don't both use the same VPN service, but there are only so many such services available and it would be very difficult to try and coordinate so that everyone uses a different one.

The SSL layer of encryption protects the message traffic over public Internet connections between the secure e-mail service and the VPN/Anonymiser service. Again, it is critical in this scenario that both people and the secure e-mail server keep their message store and address books encrypted to prevent physical theft of a computer from exposing their messages and contacts.

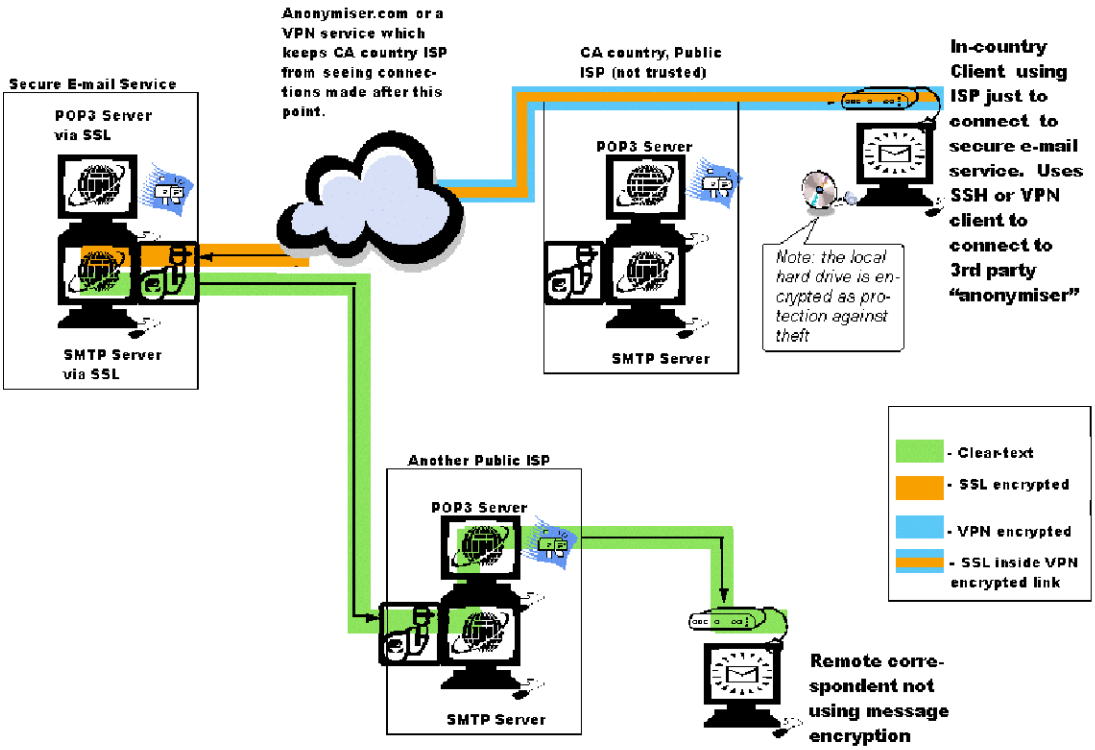

Figure 11 – Sending with SMTP over SSL via VPN to non-secured correspondent

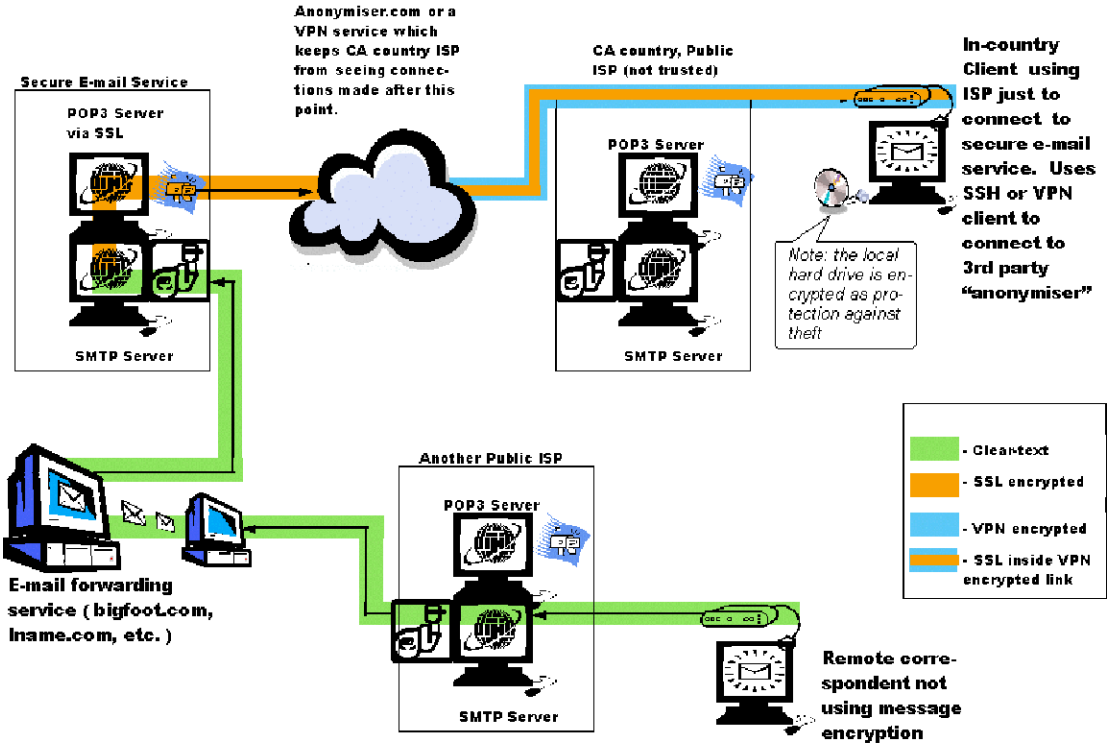

Figure 12 – Receiving from POP3 server over SSL via VPN from non-secured correspondent

Person in CA Country Corresponds With Someone Who is Not Using a Secure E-mail service

The person in a CA country needs to send and receive e-mail from friends and family members outside the country. They are not particularly concerned about the privacy of their messages in their home countries and don't use any message encryption software. For instance, dear, sweet Aunt Suzy might ask, "how many people have you convinced to drink Coca-Cola this week?" She knows no one in North America would be concerned if she asked such a question and can't really grasp the sensitivity of the situation. The question would, obviously, reveal to the authorities in the CA country what that person was really up to. The double encryption of SSL and VPN for sending and receiving those messages protects the person in-country but contents of the messages could be observed over public Internet connection elsewhere. (See **Figures 11 & 12**)

Communicating Sensitive Data Via E-mail

In this scenario the correspondent outside the CA country needs to exchange sensitive data with the person in-country, but is not subscribed to the same secure e-mail service. Since the number of such correspondents is small and limited to a controlled sub-set of people, it is not unreasonable to expect everyone in the group to understand and use message encryption software. One reason for this concern is that the CA country may have loyal countrymen working outside their homeland in key positions with large, international ISPs (a.k.a., "spies") who are looking for sensitive data to report back to their home country.

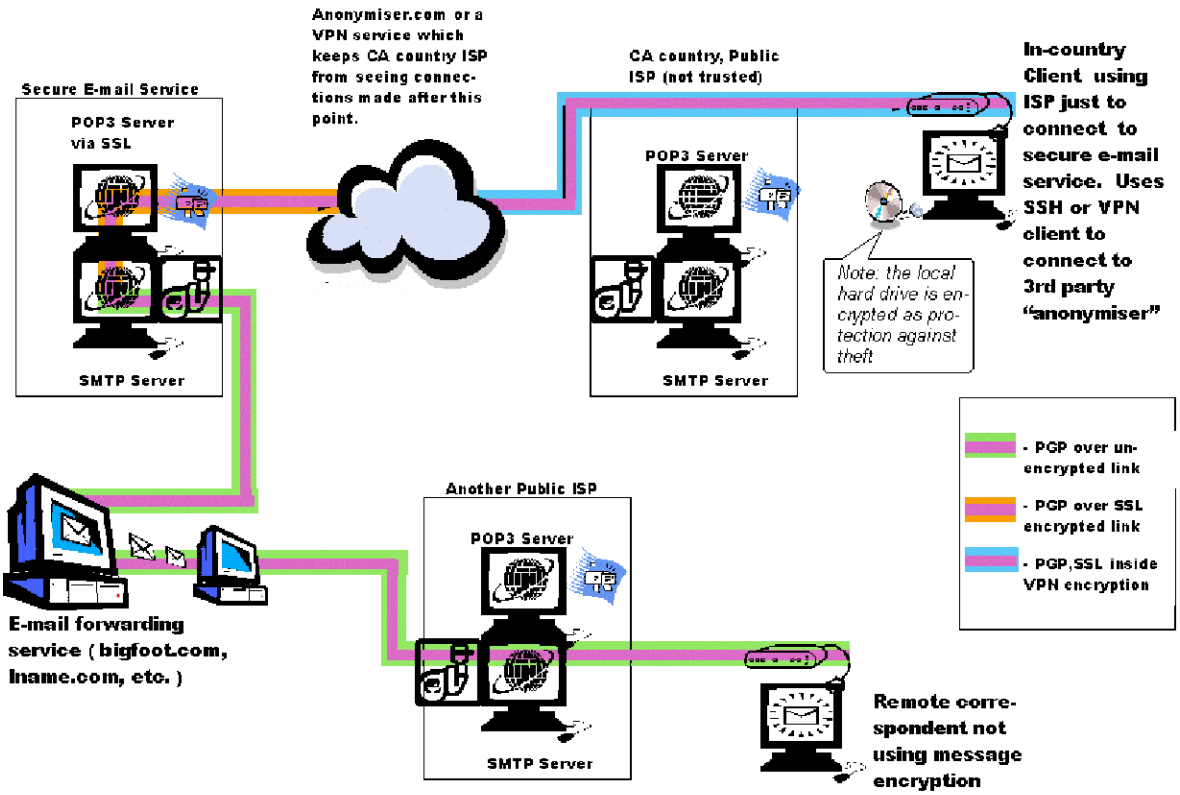

Figure 13 – Using PGP message encryption with secure e-mail service

In **Figure 13** it would be difficult to show the third layer of message encryption as another colored line within the two colored lines of SSL and VPN, but I trust you can visualize that is what is signified by changing the line colors on that part of the message path. The triple layers of encryption are really a bit of overkill, but result from the fact that all connections in and out of the CA country need to be hidden at all times. The message encryption layer is really only necessary as the message travels on public Internet connections used by the person outside of the CA country.

The spy scenario also illustrates the best reason for using the e-mail forwarding service shown in these diagrams. A spy working for an ISP could observe the address for the forwarding service, (e.g., johndoe@iname.com) but would not see the final destination address (e.g., johndoe@secretservice.com). It is a slim line of protection, but reasonable assuming there are not spies working for every possible combination of ISP and forwarding services who could then correlate the addresses they were observing.

> Presumably project Echelon might have the capability for correlating large amounts of seemingly unrelated data, but that is beyond the capabilities of smaller countries, unless they are making intelligence trades with the countries involved in Echelon. If such intelligence trades are being made, then there will be much more serious problems for expatriates working in CA countries than just having their e-mail contacts revealed. If, however, your intentions are to conceal criminal activity within the U.S., projects Echelon, Carnivore and Magic Lantern could be a real threat.