Email in the New Era, Version 1
Guang Chen
July 21, 2001

Preface

This work note is based on a presentation given to a Graduate Symposium in August 2000 on how e-mail can be effectively and safely used in this new era.

Introduction

The Internet provides one of the easiest communications tools ever afforded mankind. E-mail is a fundamental part of the Internet. E-mail technology provides comprehensive communication, productivity and effectiveness. E-mail has undoubtedly revolutionized the way we conduct business and communication. E-mail address has become another unique identified attribute of people.

On June 30, 2000 President Clinton "e-signed" a bill into law that makes electronic signatures as valid as their ink counterparts. It is seen as paving the way for a new era of electronic commerce in which companies and individuals could complete transactions online instead of in person. E-mail with its legal electronic signatures would generate enormous traffic on the web, and play an increasingly important role in the new electronic era.

On the other hand, E-mail has also thrown open the door to many negative issues such as junk e-mail, invasion of privacy, security, e-mail based attacks (spamming), and so on.

This paper first discusses the influence of e-mail technology in the business and government environments, a couple of e-mail benefits (although most of the security related paper only focus on the e-mail issues), and then introducing some e-mail issues mentioned above with some possible solutions. The author thinks that although there is a long way for people to go to finally eliminate all E-mail issues, it does not make sense to discard this effective communication tool due to its negative side just as we would not throw out a clean baby with his dirty bath water.

A couple of e-mail benefits emphasized:

E-mail is as fast and casual as a phone call, but can be stored and retrieved with infinitely greater efficiency than paper letters or taped conversations. For any worldwide operation with offices and clients, it's a great way for people to communicate with their partners and customers both locally and in satellite locations simultaneously. E-mail is also a great way to circumvent the time zone issue. In many cases, when verbal conversation alone is not enough, immediate reachable e-mail, written documents with some graphics and screen shots could play a key role in any business conversation around the world. That is

why e-mail is rapidly becoming the dominant communications channel between organizations and their customers. For almost all business companies, e-mail and e-messaging are an integral part of business, and not just in the race to acquire "market". It can aid in strengthening the overall customer relationship, creating more touch points with the customer and learning more about the customer. Organizations that do this effectively will be very successful in the online world. This is true for B2B (business to business), B2C (business to customer) as well as G2C (government to customer) organizations.

Again, President Clinton on Friday June 30, 2000[1], used an electronic card and his dog's name as a password to "E-sign" into law a bill, which is officially known as the "Electronic Signatures in Global and National Commerce Act." This bill is intended to boost and broaden e-commerce dramatically, eliminate legal barriers to using electronic technology to form and sign contracts, collect and store documents, and send and receive notices and disclosures. Clinton said firms could potentially save billions of dollars by sending and retaining monthly statements and other records in electronic form. "Eventually, vast warehouses of paper will be replaced by servers the size of VCRs," Clinton said. It's estimated that in several years, hard copies of legal papers will be seen only in museums.

David Garson[2] studied the e-mail impact on "electronic democracy" in his book titled "Computer Technology and Social Issues". Based on his research, many local governments, like the city of Santa Monica, provide electronic mail to officials and their citizens. Citizens can submit comments to city officials and get an answer within 24 hours. In fact, based on my knowledge, now almost all of Senators and Congress Members provide their e-mail to people for communication. Even the White House provided people direct electronic mail access to President Clinton and Vice President Gore during the Clinton administration.

Outside of the United States there is also a significant example that can be cited where computers and telecommunications have been useful tools for democracy. During the pro-democracy upheavals in China in 1989, computer-based telecommunications, e-mail and fax played a key role in providing news about protests and alternatives to state-controlled broadcasts (Leitschuh, 1989; Lyons, 1989; Krasnoff, 1989)[3] .

Within a company itself, e-mail can give the lowest level of employees a means to express their feelings, opinions, and suggestions to the highest levels of management. This freedom effectively improves the new workplace Equal Employment Opportunity (EEO) environment. EEO ensures that every individual, regardless of race, color, religion, age, sex, disability or national origin, has an equal opportunity in the workplace. This includes all privileges and conditions of employment such as recruiting, hiring, work conditions, compensation, training, upgrading, promotion and lateral movement, demotion and termination.

A couple of e-mail issues and possible solutions to be discussed:

Privacy via Security

E-mail is quick, convenient, and cheap but it is as insecure as it is quick, convenient, and cheap. There are many reasons why the e-mail is unsecured with no privacy.

For the business environment, employees should be aware that e-messages transmitted via the company electronic mail system are considered the company property and not private by many companies. All e-mail may be reviewed or monitored at any time by the company or in accordance with the legal process. All business e-mail messages are retained for a period of time and subject to discovery in legal proceedings. Pushing the delete button, which only removes your selected e-mail messages from your personal mail , does not do much because another copy of them still sits on the e-mail system.

For the non-business environment, e-messages sent many months ago also may remain on your ISP's (Internet Service Provider's) server or in a backup. So you really need to be aware that a-mail leaves a written record long after it has been erased. Any skilled person can recover the e-mail message's ghost somewhere deep in the bowels of a networked system.

Moreover, except for your ISP e-mail server or system administrator, other skilled people are able to invade your privacy because of the nature of e-mail travel. An e-mail might take 10 hops (go through 10 routers) before it reaches its destination. This would create at least ten spots where someone could be "sniffing", or tapping into your e-mail. Especially this is troublesome if outsiders or crackers intrude into your firm's computer network; they are able to gain the same access privilege as your e-mail system administrators. So using e-mail, you really should not expect too much your privacy. For sensitive matters, ordinary e-mail is definitely inappropriate.

However, simple precautions can keep the use of e-mail from being too risky. For example, first, with encryption, e-mail is a relatively secure and workable means of communication. Encryption permits the sender to be quite confident that no one will intercept the message, and permits the recipient to be quite confident that the message was not tampered with. One popular encryption program introduced by SANS is PGP, which stands for Pretty Good Privacy. PGP permits the user to select the length of the "key" that is used to encrypt and authenticate messages. The longest possible key is recommended. For example a length of 1024 bits (about 445 decimal digits) maximizes the length of time that would be required to crack the encryption. Typically, using Password Crackers, Inc. to test all possible 5 – 8 digit, lowercase and character digit only passwords would generate 16,273,555,776 passwords. This would take a professional with Password Crackers, Inc. approx. 1.5 days to complete testing. If we were to extend this to all possible 6 digit passwords, 7 and 8 character lower case passwords and all 7, 8 and 9 character digit only passwords, there would be 992,274,938,496 possible passwords to test. This would take approximately 88 days. To brute-force test for all possible

passwords up to Microsoft's 15 character limit would take 132,226,510,327,857,000 years[4]
.

But, the way of encryption only prevents some outsiders from invading your privacy during the e-mail travel. Your e-mail server administrators still can decrypt any encrypted e-mail. This is why many companies claim that e-messages transmitted via the company electronic mail system are considered company property and not private, although results from a recent survey in US companies indicates that it is much more unacceptable for employees to tolerate the companies watching employees using e-mail than by using video. There are 44% employees and 30% employers who can not accept a way to supervise employees' e-mail[5].

Second, if there is to be a connection between the Internet and one's computer network, the connection must be through perimeter defense devices such as firewalls. The firewall is a computer that passes things back and forth between the Internet and one's own network. The firewall computer could be configured to pass only pure e-mail, and block anything else (such as executable programs) from coming in or out. The firewall is the cost-effective, practical and most common way to protect your e-mail systems from outside attacks.

A third precaution when you sets up a connection between your network and the Internet is to change the access codes to be different from their initial-set values.

Finally, you can have e-mail without having any connection at all between your own network and the Internet. Many small firms simply have their employees check their e-mail by dialing out with a modem to reach the Internet service provider. Doing that, the employees' own computers, and other computers in the firm network, are almost isolated from outside attack. This is because they are not connected with the Internet 7 by 24 as DSL users are. This also is the major reason Russia had not been attacked by the "Love Bug" virus because Russia's major computer networks have not been connected with the Internet[6]. Of course, modems that connect to the Internet should not be configured as a mode of auto-answer, otherwise, these modems still play a role of permanent (7 by 24) connection from your network to the Internet.

Buffer Overflow Attacks

A buffer overflow attack sends something that is too large to fit into a fixed-size memory buffer in the e-mail client, in the hopes that the part that doesn't fit will overwrite critical information rather than being safely discarded. These attacks can be used as Denial of Service attacks, because when a program's memory gets randomly overwritten the program will generally crash. When a server sends lots of e-mail or connection requests within a short period of time, it will definitely slow the speed, or crash. In 1997[7], Space shuttle astronauts' lives were put at risk by an overload to NASA's communication system, the agency told the BBC in a program to be aired Monday[8]. It is in some cases

possible to supply program instructions for the victim's computer to be executed by carefully crafting the exact contents of what overflows the buffer. However, this is the result of a bug in the program under attack. A properly written e-mail client will not allow random strangers to run programs on your computer without your consent. Programs subject to buffer overflows are incorrectly written and must be patched to permanently correct the problem.

Buffer overflows in mail programs occur in handling the message headers and attachment headers. The email client uses them to process and to know details about the message and what to do with it. The message headers and attachment headers can be pre-processed by the mail server to limit their lengths to safe values.

On the other hand, companies can set up routers to create an access list that logs the source address of malicious packets. By doing this, targeted sites can ask their service providers to trace the machine address of the packets through each router on their network and contact other providers if the packets jump network boundaries.

There are many machines that don't keep logs, and attacks that spoof packet addresses are difficult to trace unless data is collected during the attack. Also there are many Internet service providers that aren't willing to trace packets and get data in real time unless it is a big attack. Companies should develop contacts with law enforcement and be prepared to quantify financial losses to overburdened investigators.

Moreover, if more network managers installed a type of filtering known as RFC2267 to their I/O interfaces, it would be more difficult to launch attacks with spoofed packet addresses. As the packet leaves the router, these filters apply a set of rules to insure that the packet complies with an internal source address before it is sent. This would prevent a compromised machine from being used by an attacker to send a flood of packets with inaccurate addresses against a target. Especially, it would be very effective for service providers to install these filters.

Other tips on preventing denial-of-service attacks :
1. Monitor your own network to make sure your machines aren't being compromised for a denial-of-service attack network.

2. Hire multiple Internet service providers that can provide fail-over during attacks; increase aggregate bandwidth and distribute Web sites on networks around the world.

3. Disable IP-directed broadcast capabilities, which can be triggered by a malicious incoming packet to flood other hosts in a network.

4. If you are a customer of a co-location site, investigate what kind of protection you will receive from fellow customers.

Trojan Horse Attacks

Trojan Horse Attacks are attacks where an executable program or macro-language script that grants access causes damage, or does other unwelcome things. It is mailed to the victim as a file attachment labeled as something innocuous such as a greeting card or screen saver. These are also often hidden in something the victim is expecting, such as a spreadsheet or important document. These attacks are usually used to breach security by getting a trusted user to run a program that grants access to an UN-trusted user, or to cause damage such as attempting to erase all of the files on the victim's hard disk. Trojan Horses can also steal information or resources or implement a distributed attack, such as distributing a program that attempts to steal passwords or other security information.

The receivers most run the program for the Trojan Horse Attacks to succeed. Therefore it can be avoided simply by not running programs that have been received in e-mail until they have been checked over, even if the program seems to be harmless, but especially if it comes from someone you don't know well.

Under the certain circumstances, even if your system administrator (or someone claiming to be your system administrator) e-mails you a program and asks you to run it, be very suspicious and verify the origin of the email by contacting your administrator directly. Through the Internet you receive many bogus e-mails. For example, on June 30 6:57 PM ET, 2000[9], some users, including Reuters', reporters of Microsoft Corp.'s free Hotmail e-mail service are getting a bogus message, purportedly from a company official, threatening to cancel their accounts because the service is bogged down with too many customers.

The message, allegedly from a "Jon Henerd" of the "Hot-mail Admin. Dept.," tells recipients they will be kicked off the service if they do not prove that they actively use their accounts by forwarding the e-mail. "Hotmail is overloading and we need to get rid of some people and we want to find out which users are actually using their Hotmail accounts. If you do not pass this letter to anyone we will delete your account said the message.

Microsoft quickly responded by saying the message was a prank and that Hotmail, one of the largest Web-based e-mail services in cyberspace, was in great health. "It's a chain e-mail that is a hoax. There is no truth in it whatsoever," a company spokeswoman said. Microsoft does not employ anyone named "Jon Henerd," and Microsoft is considering posting a message on Hotmail telling users to ignore the crank e-mail, she said[10].

However, some bugs in the e-mail client, a poor design or unknown reasons may allow the attack message to automatically execute the Trojan Horse attachment without user intervention, through either the use of active HTML, scripting or buffer overflow exploits. This is an extremely dangerous scenario. To prevent this, people need to used to change the names of executable file attachments first, whenever received, so that the operating system no longer thinks they are executable (for example, by changing "LOVE.EXE" to SUSPECT1.EXE").

A more recent example is the W32.Sircam. Based on Message Labs in UK[11], it was first captured on 18 July 2001. In the last 3 days, it had spread in 73 countries included in the United States (768 infected), Great Britain (574 infected) and Mexico (344 infected). Mark Sunner, CTO in the Message Labs said that W32.Sircam is in its attached file with .BAT, COM, EXE, LNK, PIF, etc[12]. and is able to infect all exist e-mail clients. It has extremely self-reproductive ability to target office documents such as Excel and Word and will attached that document to an email, which is sent to everyone in the user's address book. Moreover, it is able to automatically delete the infected files and causes hard disk and buffer overflow and operating system crash.

The worm is particularly dangerous because it arrives with a random subject line, and cannot be identified by the subject line and message, therefore filtering for subject lines and attachments is ineffective, according to Symantec's David Banes.

Obviously, it is so important for you to identify, filter, detect or discard attachments that may put you at risk. Installing updated anti-virus software (which detects and removes macro-language Trojan Horses) is the most common way to protect you from Trojan Horse attacks. Also you should always open data file attachments in the program's "do not automatically execute macros" mode.

Conclusion

E-mail has dramatically improved the efficiency, quality, and productivity of people's daily communication. E-mail has also improved civic Democracy. However, it has also thrown open the door to many issues as introduced above. Even if the electronic civic Democracy is also limited by the very propensity of on-line communications to dramatically increase the volume of information flow. For example, "White House E-mail" did not mean Bill Clinton, or George Bush read your message. Rather, the White House selected a software package that "read" e-mail and responded with the electronic equivalent of form letters. Although form letter responses had long dominated White House mail operations, up to then at least some human being had actually examined each incoming letter. The new on-line system increased access to the White House, but access was reduced to poll-like tally results calculated by e-mail software[13].

So although e-mail technology increases comprehensive communication productivity and effectiveness, yet, the road to final elimination of all E-mail issues is very long. E-mail and the Internet are still relatively new tools for human being's knowledge. There is a lot of room to continuously study and to continuously improve the use of e-mail, e-mail privacy and e-mail security. For now, the only thing we can do is to pay close attention on any recent research, news, regulations, laws and updated products.

Reference

[1] Murphy, Dave, "President Clinton Makes E-Sign Act Law" http://www.insiderreports.com/storypage.asp_Q_ChanID_E_WB_A_StoryID_E_20000859.

"Clinton To E-sign Digital Signature Law" by Reuters, http://www.iwayforms.com/dutch/news/20000705.htm

[2] Garson, David. (1997). Computer Technology and Social Issues, Harrisburg, USA: Idea Group Publishing, (P45).

[3] Garson, David. (1997). Computer Technology and Social Issues, Harrisburg, USA: Idea Group Publishing, (P46).

[4] Yung, Jia, "Information Security: is there any wall that is able to completely isolate wind?", http://www.peopledaily.co.jp/GB/channel5/569/20000215/384.html

[5] "E-mail and Sound-mail Security Bring Much Concerns." http://www.peopledaily.co.jp/GB/channel5/569/20000330/26217.html

[6] People's Daily On-line, 05/09/2000 09:43, "Why the Love Bug did not love the Russia?

[7] "Hacker compromised astronaut safety", http://news.bbc.co.uk/hi/english/sci/tech/newsid_816000/816510.stm

[8] "Hacker risked astronauts' lives ", http://www.landfield.com/isn/mail-archive/2000/Jul/0008.html

[9] "Fake e-mail threatens to cut Microsoft Hotmail users By Reuters", http://detnews.com/2000/technology/0007/02/technology-84496.htm

[10] "Fake E-Mail Threatens to Cut Hotmail Users", http://www.info-sec.com/viruses/00/viruses_063000a_j.shtml

[11] "New W32.Sircam.worm is loose and trickier then Code Red worm", http://www.securitynewsportal.com/article.php?sid=1166

[12] "UK Specialist Warned Sircam Spreads Very Fast", http://content.sina.com/news/63/43/634317_1_gb.html

[13] Charles, Deborah. "Clinton Uses 'Smart' Card to Sign Digital Law", Retrieved Friday Retrieved Friday June 30 5:03 PM ET from the Yahoo.