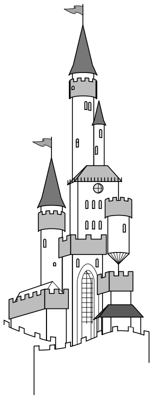
CHAPTER 6

E-mail Security

(Communicating with Other Villages)



The town was growing nicely now, but John knew it wouldnÕt continue unless they stayed in close communication with the nearby towns. JohnÕs town had to know about events in other towns, and they should know about his, so John made road trips to each of the towns to visit with their mayors. The purpose was simple: to meet them and establish good relations and communication.

With each mayor, he talked about sharing information about local events, law enforcement, roads, and other issues that each faced. They agreed to start a newspaper in which they could carry all sorts of local news and events. The paper would be published weekly and sent out to the towns so everyone would know what was going on in the area. A man in JohnÕs town had a newspaper background, so John volunteered to start up the paper in his town. The other towns could have reporters gather stories and send them to the main office via messenger. Then on Fridays, they would publish the paper, and messengers would deliver a stack to each town for distribution to the people.

After his trip, John talked to William, the man with the newspaper background, and he accepted the job. John and William started to work right away at getting things established. In just a week they had the printing press in and set up and had even ordered a few extra parts that William suggested so they could replace ones that might break easily. By the second Friday, they were able to publish the first edition of the Local Journal.

Why E-mail Is Cool

If you’ve used the Internet at all, odds are you’ve used e-mail. In fact, some people have only used the Internet for e-mail. E-mail is one of the oldest and most desired functions made possible by the Internet. Initially, e-mail was used on DARPANET[1] by researchers from all over the globe, for whom time zones had been a really big deal. Asynchronous communication was required, because people were not all at their desks at the same time. With e-mail, they could communicate without regard to time zones. Another big feature of e-mail is being able to write one message and send it to multiple people at the same time. This just wasn't possible with standard mail, and it enabled discussion groups to be formed that couldn't exist in other mediums. The final plus was attachments. Being able to attach a separate document to the mail and send it to someone—or to a group—helped people communicate more quickly and efficiently than they ever had in the past. With all of these things going for it, the popularity of e-mail began to grow.

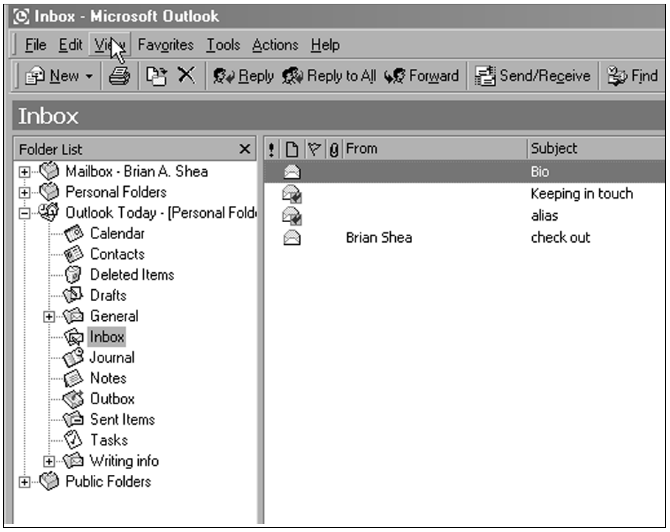
E-mail wasn't an overnight success, but as the network called the Internet grew in size and capability, e-mail was growing right alongside it. As e-mail use increased, the need for greater ease and added features increased too. And with more users, more features, and wider distribution came more security issues. The typical e-mail client being used in Windows today is much more complex than the first mail readers and has more built-in features than were even possible back then. But as the code and features expand, so do the possibilities for security holes that can be found and exploited.

How E-mail Works

E-mail is essentially a text transfer between your machine and the recipient's machine, but it is a lot more complex than that. I'm not going to get into deep analysis of how Internet Mail Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP), or Post Office Protocol 3 (POP3) work, but you do need to understand a few key points about how a message moves through the system if we're going to talk about security (see Figure 6-1).

First, someone who wants to send a message must be running software that "understands" IMAP, SMTP, or POP3 and can use these protocols to

[1] Defense Advanced Research Project Administration Network



From	Subject
	Bio
	Keeping in touch
	alias
Brian Shea	check out

Figure 6-1 Outlook e-mail client

communicate with the surrounding systems. These protocols are the accepted methods for sending, receiving, and forwarding e-mail messages on the Internet. This is similar to John's meeting with the mayors to decide about using a newspaper to communicate information. Someone has to decide how the information exchange will be done, and then everyone can start talking. Unless everyone uses the same rules, however, we'll end up with our own version of the Tower of Babel. Think of the messengers in our example as the protocols IMAP, SMTP, and POP3. These protocols were established by using the RFC (Request For Comment) system to establish and modify standards used on the Internet. RFCs are maintained by the Internet Engineering Task Force (you can find more information about IETF at www.ietf.org/rfc.html). IMAP is RFC 2061, SMTP is RFC 821, and POP3 is RFC 1957. Each of these actually has more than one RFC, and you can find them all at www.ren.nic.in/rfc.html, but the RFC I've listed for each protocol is the one that started the protocols we now use for our e-mail system.

E-mail users are like the reporters in our example. They write the "stories"—e-mail messages—and send them to the "central office." In the case of e-mail, though, the central office is a collection of computers on the Internet. For our purposes, you can think of the place where you send your e-mail as the mail computer at your ISP. Typically this is a group of machines (called a cluster) that handles the mail for an ISP, especially if you use a larger Internet provider such as AOL, Earthlink, MSN, or Yahoo!.

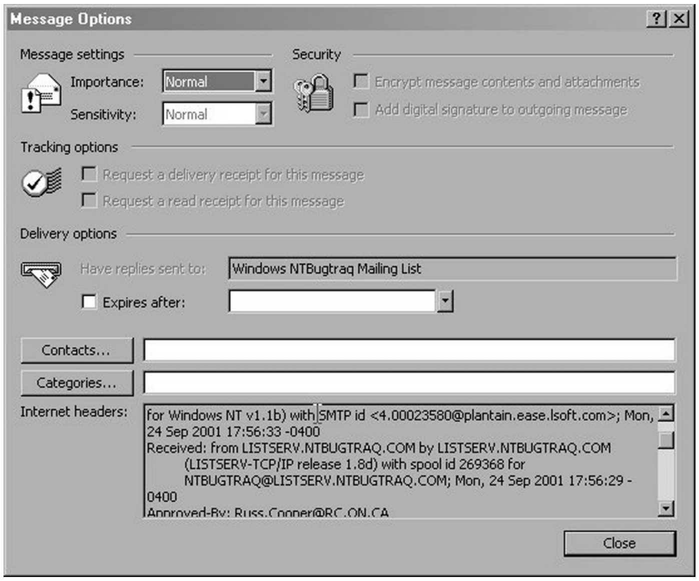
This central office then distributes the message to all the intended recipients, whether one or many. It uses the same protocols we used for sending our message, and it "talks" to several mail systems (usually) on the way to delivering the mail to the recipient. The mail system uses DNS (Domain Naming System, the Internet's naming system) to determine if the domain in the e-mail address is valid; then it sends the message along to the SMTP server in that domain. When the message arrives, this server looks up the username. If the username exists, the message is placed in the user's mailbox for retrieval; if not, the mail bounces back to the sender with an "Undeliverable" message.

Security Issues with E-mail Systems

E-mail is a reasonably secure medium to use for communications. It certainly isn't infallible, but the average user with nonsensitive information can be confident that things are getting to the recipient and not being read by anyone else. Let's look at some of the weaknesses in the e-mail system and see what you can do to avoid them or prevent their affecting you.

Spoofing

Spoofing means someone gets you to believe that a piece of e-mail was sent from someone other than the actual sender. Often this is done as a joke, such as sending you mail that appears to come from president@ whitehouse.gov or getting you to respond by making you think the sender is known or nonthreatening. The address set for the reply isn't necessarily the one that shows in the "From" line. The technique for doing this is relatively simple and will not be covered here, but the good news is that it's easy to detect the correct sender. The e-mail headers contain the correct information about where the message originated (see Figure 6-2) and the entire path it traveled. Even if someone



Importance: Normal

Sensitivity: Normal

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Have replies sent to: Windows NTBugtraq Mailing List

□ Expires after:

Internet headers:

```
for Windows NT v1.1b) with SMTP id <4.00023580@plantain.ease.lsoft.com>; Mon,
24 Sep 2001 17:56:33 -0400
Received: from LISTSERV.NTBUGTRAQ.COM by LISTSERV.NTBUGTRAQ.COM
        (LISTSERV-TCP/IP release 1.8d) with spool id 269368 for
        NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM; Mon, 24 Sep 2001 17:56:29 -
0400
Approved-By: Russ.Cooper@RC.ON.CA
```

Figure 6-2 Viewing an e-mail header in Microsoft Outlook

is savvy enough to alter the headers at their location, you can easily see (if you know what to look for) that the message was faked. The lesson here is that you cannot always trust that your e-mail is coming from the person you see in the "From" line. If a message is asking for personal information, passwords, or anything sensitive, tell them you would rather not discuss it by e-mail, and ask them for a phone number or postal address. Real companies with legitimate business will usually do this happily; scammers and crooks will not.

DNS Redirecting

DNS redirecting is a technically challenging hack (clever or creative use of computer code) and not easily accomplished. Here's an example. If I know I want to get at the mail from a specific target—say, business data from Coca-Cola—I might try to "redirect" traffic from cocacola.com to a fake address I set up. Now traffic sent to cocacola.com will come to me instead of going to the real company. With a bit of extra effort, I can then re-forward the mail to the real Coca-Cola so they'll never know I read it first (they might experience a delay in receiving it). Wow, sounds serious! Yes, it is, and fortunately, it is not easy. In fact, with current DNS systems, such attacks are more and more difficult to do. The advantage for home users and small businesses is that redirecting takes lots of effort, so you won't be worth targeting unless the payoff is high. Small businesses and home users do not typically approach this level of payoff, so the likelihood of such an attack against them is minimal.

ÒRead As HTMLÓ

Mail clients that allow you to "Read as HTML" should be turned off, left off, and if at all possible, never used. Period. Although control seems to be getting better, this was a bad idea from the beginning. By letting senders write computer code that I allow to run on my system, I automatically give them a shot at taking control of my system. HTML (Hypertext Markup Language) is what makes the World Wide Web look and operate the way it does. HTML looks nice, so someone thought having e-mail in that same format would be a good thing. It isn't. I can send HTML-formatted messages that contain scripting, links to external servers, and a variety of redirects or commands that can run on your system as the HTML runs on your mail reader. The fastest way for me to do this is to send spam mail (I'll cover spam mail in a bit) to your address that makes some claim for a vacation prize or something that might make you want to read a bit further. While you're reading, the HTML redirects the mail reader to get data from a remote system, not from the e-mail message anymore. This remote system can contain code that tries to install Trojan-horse software, gain access to your system, or just plain wreck your system by deleting key files. You think you're possibly winning a free trip to Hawaii, but instead your hard drive is being erased. Not good. You open yourself up to literally hundreds of exploits when you use "Read as HTML" as your mail option. Many of these are being patched, but it's a losing battle. Turn off that "Read as HTML" option and prevent these attacks. If you want Web content, go to the Web.

Scripting Issues

Some e-mail programs allow senders to imbed scripts or macros in messages. Then they try to run the script or macro when you read the message. If someone trying to break into your system wrote that script or macro, it can be bad. There are two main avenues through which you are vulnerable to these attacks: turning on "Read as HTML" (just discussed) and using Microsoft Word as your e-mail editor. The newer versions of Microsoft Word now come with macro protection, but older versions might not or the protection might be disabled. That means a macro can be run if it is imbedded in the mail message. Again, if the message is from someone malicious, the macro can cause all sorts of havoc. The best way to avoid this one is to ensure that your MS Word is up-to-date (version 6.0 or later is sufficient) or to ensure that you are running an antivirus program that can scan e-mail for macros. All of this is also true for MS Word documents that come to you attached to e-mail messages.

Attachments

Speaking of attachments, a world of problems can come from files attached to e-mail messages. In this case, it isn't technically the mail system that is the security threat; that system is simply the delivery mechanism. Never trust files attached to mail messages—scan every one of them. In particular, you should always scan executable files (for example, .exe, .cmd, .bat, .pl), document files (such as .xls or .doc), and script files (such as .vbs, .js, .java, and .wsh). Even better is to scan everything to be sure someone hasn't renamed a file just to get it past your scanners. An exploit went around for a while in which people would rename a file to have two extensions (technically, one extension and a name with a period in it), resulting in a file called something like readme.txt.vbs. If a computer's file-viewing options were set at default, this appeared as "readme.txt" and seemed harmless, but double-clicking the file would run the VBS script. A subsequent patch from Microsoft prevents this behavior from working.

Unsolicited Commercial E-mail (UCE aka spam)

Unsolicited commercial e-mail (UCE), also known as spam mail, is a spreading phenomenon (see Figure 6-3). It wasn't until people started using e-mail in large numbers that spam started appearing on the scene. As soon as folks realized they could use e-mail to reach

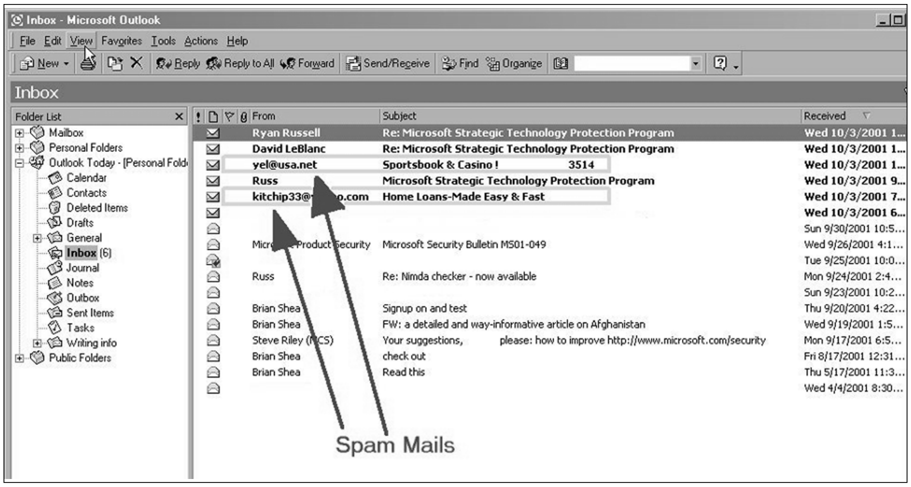
Encryption in E-mail

One way to ensure privacy of your e-mail stands above all the rest in terms of reliability. That is *encryption*. If you encrypt your e-mail, it can be read only by the intended recipient. Well, thatÕs assuming that the key is strong and that the encryption program is correctly installed and coded to allow no back doors or administrative overrides. When I say a strong key, what I mean is one that is 256 bits or more in length. As a general rule, the key is stronger as it uses more bits. We also must assume that the code breaker doesnÕt have massive computing power available. By massive, I donÕt mean the newest Pentium chip or even a dual or quad processor system, but a supercomputer. If you use a program for encryption, you can ensure that not just anyone can read your e-mail message. If the recipient of the mail has the right decryption key, that person will be set. Several options for e-mail encryption exist, and some are better than others for specific mail programs. I favor PGP[2] on my system. ItÕs the program I started using first, IÕm familiar with its use, and it is very user-friendly. Searching on the Internet for e-mail and encryption will yield a large number of links you can visit to get more information about encryption and about products or services suitable for your needs. If you go to dir.yahoo.com/Computers_and_Internet/Security_and_Encryption/, youÕll be able to dig deeper into e-mail, encryption, and security.

customers and that enough customers were out there, the marketing types went to work and began figuring out how to fill your mailbox with “useful” information. The truth is that the vast majority of the public didn’t want that junk mail coming into their e-mail boxes as well as their real mailboxes, so most companies have stopped. Why, then, do you see so much spam? Frankly, some people are willing to annoy millions of people if it means a few bucks in their pockets. Most spam mailings qualify in one or a few of the following categories.

- **Make money fast:** This is usually raw scam mail. It includes work-from-home offers and get-rich-quick schemes. These mailings are usually a pure scam, attempting to get money out of you. *You* are not the one who will “get rich quick” if you answer this mail.

[2] Freeware program developed by Philip Zimmermann



From	Subject	Received
Ryan Russell	Re: Microsoft Strategic Technology Protection Program	Wed 10/3/2001 1...
David LeBlanc	Re: Microsoft Strategic Technology Protection Program	Wed 10/3/2001 1...
yel@usa.net	Sportsbook & Casino ! 3514	Wed 10/3/2001 1...
Russ	Microsoft Strategic Technology Protection Program	Wed 10/3/2001 9...
kitchip33@[illegible]o.com	Home Loans-Made Easy & Fast	Wed 10/3/2001 7...
		Wed 10/3/2001 6...
		Sun 9/30/2001 10:5...
Micr[illegible] Product Security	Microsoft Security Bulletin MS01-049	Wed 9/26/2001 4:1...
		Tue 9/25/2001 10:0...
Russ	Re: Nimda checker - now available	Mon 9/24/2001 2:4...
		Sun 9/23/2001 10:2...
Brian Shea	Signup on and test	Thu 9/20/2001 4:22...
Brian Shea	FW: a detailed and way-informative article on Afghanistan	Wed 9/19/2001 1:5...
Steve Riley ([illegible]CS)	Your suggestions, please: how to improve http://www.microsoft.com/security	Mon 9/17/2001 6:5...
Brian Shea	check out	Fri 8/17/2001 12:31...
Brian Shea	Read this	Thu 5/17/2001 11:3...
		Wed 4/4/2001 8:30...

Figure 6-3 Example of spam mailings

- **Lose weight now, miracle cures, and such:** These also are usually scam mails. They claim to be selling cures for common ailments or conditions, often preying on people who are desperate or who want to find the Easy Answer. Weight loss is a big target of these mailings.
- **You won $$$$$:** This is usually some form of sales pitch. The message claims you won a vacation or might win some prize to get you to visit a Web site or click on a link. The sender is usually getting money for the page hits or clickthroughs on the link, and there probably is not a prize to be won.
- **Selling of mass-mailing software:** Of course mass e-mailers also like to sell their own stuff through mass e-mail. CDs with names and e-mail addresses, software for generating mass mailings, and “instructional programs” on how to use mass mailing effectively are often sold through mass mailings.
- **General sales:** Most any product that can be sold might be a mass-mailing candidate, but remember one thing. Most companies care if they are angering 96 percent of the audience to get at the 4 percent who might respond. Most legitimate companies stay away from mass mailings because of the amount of rejection and anger a mass-mailing campaign can generate.

What Makes It Junk Mail?

Reading through this section, you might be wondering what makes a message junk mail. How do you know when itÕs junk? Well, if you donÕt want it, itÕs junk. Perhaps you subscribe to a mailing list. You actively signed up and requested that service, so mail from that source obviously isnÕt junk. How about advertising from a company you have purchased from before? Some people would say this is okay, but some wouldnÕt like it. Then there is the random mailing you receive from someone who bought your name and address from a list. Most people seem not to like that very much. But your mailbox is exactly that: yours. You get to determine what is and what isnÕt junk mail.

Many legitimate businesses with whom you have an existing ÒrelationshipÓ (you bought something or used their services) might send you mail as a follow-up or to try to keep your business with them. Such messages often tell you that if you donÕt want to receive their offers, you can elect not to get them. This is called Òopting out.Ó Or perhaps you sign up for a service and the form includes ÒDo you want to receive additional information about services and specials we offer?Ó If you select yes, you have Òopted inÓ to being on their mailing list.

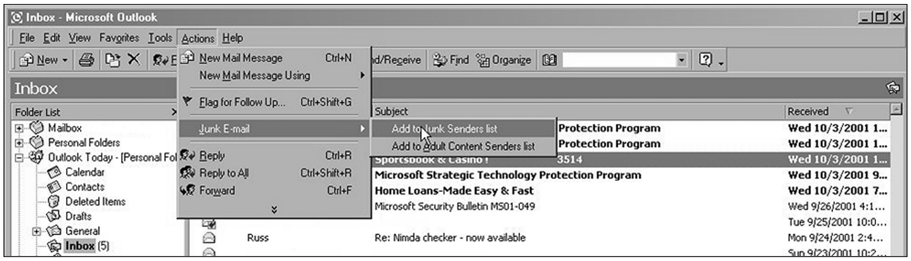
The laws governing UCE can vary from state to state; however, most states have laws on the books or being considered that will give you the right to opt in or opt out of mailing lists, with senders required to provide a valid mailing address, phone number, and/or e-mail address in their mail so recipients can complain or contact someone about the contents. Failure to provide legitimate addresses or options for getting off lists can be illegal in some states, and if you can track down the sender, they can be prosecuted.

You've surely guessed that I'm not fond of junk e-mail. I'd go so far as to say I really hate the stuff; it's a waste of my time. I'm not alone in that opinion, either. Many states have made junk mailing through e-mail illegal or restricted by requiring valid return addresses or "opt-out" choices that get you off the list that got you the mail in the first place. The problem often is that the sender either doesn't know or doesn't care and sends the mail anyway. Return addresses might be forged or incorrect, and links to pages are often redirected—all in attempts to hide the identity of the real sender. So many people get mad about junk e-mail that lawsuits, death threats, and hacker attacks have all been directed at mass-mailing companies. Yep, you read that right: death threats. I'm not so against junk e-mail that I'd threaten someone, but I do think the fact that people will go to great lengths to hide who they are when sending out spam mail indicates an inherent admission that what they are doing is wrong. In many cases, the mailings are part of con games or scams targeting people who will send money or credit card information over the Internet. Then the company just disappears with the money or information.

Getting Off E-mail Lists

Here's how you can get off mailing lists. First let me warn you, it can be a lot of work. You have to opt out of all the mailing lists you are on. This means when it says "Click here to be removed from our mailing list," you do it. If a message doesn't offer opt-out, deleting the mail is often the easiest choice, but you can do more. Use your e-mail program to view the headers of the e-mail, and look for the original sender in the headers (you can usually find that information near the top of the header, as in Figure 6-2). Then send mail to that address and request removal from the list. Often the sender's address is forged, but this is worth a shot. (Note that by responding to the mail at all, you verify for the sender that your address is valid. Some will still remove you from the list when asked; others won't.) If you live in a state with anti-spam laws, report the sender to your State Attorney General or just forward the mail there. (Each state is different; check with the Attorney General before forwarding spam mail.) If you don't want to go to the trouble of responding and possibly making the problem worse, your best bet is to *never* respond to any mass mailing. Not only does this make their efforts not profitable because you don't buy anything or give out any money, but they can't verify that your address is valid and keep sending you mail.

If you don't want to fight the mail but you don't want it in your inbox, you can try blocking it. Check the instructions for your e-mail program (see Figure 6-4). Most have junk-mail filters that you can enable to stop



From	Subject	Received
	Protection Program	Wed 10/3/2001 1...
	Protection Program	Wed 10/3/2001 1...
	Sportsbook & Casino ! 3514	Wed 10/3/2001 1...
	Microsoft Strategic Technology Protection Program	Wed 10/3/2001 9...
	Home Loans-Made Easy & Fast	Wed 10/3/2001 7...
	Microsoft Security Bulletin MS01-049	Wed 9/26/2001 4:1...
		Tue 9/25/2001 10:0...
Russ	Re: Nimda checker - now available	Mon 9/24/2001 2:4...
		Sun 9/23/2001 10:2...

Figure 6-4 Adding names to junk-mail list in Outlook

junk mail from coming in after you have identified the sender as an originator of junk mail. Third-party programs are also available that claim to be junk-mail blockers. I haven't tried any of these yet, but you might want to check them out.

E-mail Security Checklists

Following is a quick checklist you can use to determine if you've covered all the bases for securing your e-mail. If you have questions about this list, go back to that section of the chapter to get details or look in the Help section of your e-mail program.

- Do you use an e-mail program that allows "Read as HTML"? Is it turned off?
- Are you using an antivirus scanner that can read e-mail and attachments?
- Do you opt out of junk e-mail lists?
- Do you encrypt sensitive information in e-mail messages?
- What key strength do you use for your encryption?
- Who can decrypt your messages? (Who has the key for decrypting your e-mail?)