Hacker Highschool
SECURITY AWARENESS FOR TEENS

LESSON 9
E-MAIL SECURITY

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Stephen F. Smith, Lockdown Networks

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

9.0 Introduction

Everyone uses e-mail. It is the second most used application on the internet next to your web browser. But what you might not realize is that a significant portion of network attacks and compromises originate through e-mail. And with respect to your privacy, misuse of e-mail has the potential to disclose either the contents of your message, or give a spammer information about you. The purpose of this module is to give you information on how e-mail works, safe e-mail usage, e-mail based attacks, and security strategies for e-mail.

9.1 How E-mail Works

Just like airmail is sent through the air, 'e'-mail is sent through the 'e' – the 'e' in this case being the web of electronic connections within and between the networks that make up the Internet. When you send an e-mail from your computer, the data is sent from your computer to an SMTP server. The SMTP server then searches for the correct POP3 server and sends your e-mail to that server, where it waits until your intended recipient retrieves it.

9.1.1 E-mail Accounts

E-mail accounts are available through many different sources. You may get one through school, through your work or through your ISP. When you get an e-mail account, you will be given a two part e-mail address, in this form: *username@domain.name*. The first part, *username* identifies you on your network, differentiating you from all the other users on the network. The second part, *domain.name* is used to identify your specific network. The username must be unique within your network, just as the domain name must be unique among all the other networks on the Internet. However, user names are not unique outside of their networks; it is possible for two users on two different networks to share user names. For example, if there is one user with the address *bill@bignetwork.net*, there will not be another user on *bignetwork.net* whose user name is *bill*. However, *bill@bignetwork.net* and *bill@smallnetwork.net* are both valid e-mail addresses that can refer to different users.

One of the first things that you will do when you are setting up your e-mail is to enter your e-mail address into your e-mail client program. Your e-mail client is the program that you will use to send and receive e-mails. Microsoft's Outlook Express may be the most widely known (since it comes free with every copy of a Microsoft operating system), but there are many others available for both Windows and Linux, including Mozilla, Eudora, Thunderbird and Pine.

9.1.2 POP and SMTP

After your e-mail client knows your e-mail address, it's going to need to know where to look for incoming e-mail and where to send outgoing e-mail.

Your incoming e-mails are going to be on a computer called a *POP server*. The POP server – usually named something like *pop.smallnetwork.net* or *mail.smallnetwork.net* – has a file on it that is associated with your e-mail address and which contains e-mails that have been sent to you from someone else. *POP* stands for *post office protocol*.

Your outgoing e-mails will be sent to a computer called a SMTP *server*. This server – named *smtp.smallnetwork.net* – will look at the *domain name* contained in the e-mail address of any e-mails that you send, then will perform a *DNS lookup* to determine which POP3 server it should send the e-mail to. *SMTP* stands for *simple mail transfer protocol*.

When you start up your e-mail client, a number of things happen:

1. the client opens up a network connection to the POP server
2. the client sends your secret password to the POP server
3. the POP server sends your incoming e-mail to your local computer
4. the client sends your outgoing e-mail to the SMTP server.

The first thing to note is that you do not send a password to the SMTP server. SMTP is an old protocol, designed in the early days of e-mail, at a time when almost everyone on the Internet knew each other personally. The protocol was written with the assumption that

everyone who would be using it would be trustworthy, so SMTP doesn't check to ensure that you are you. Most SMTP servers use other methods to authenticate users, but – in theory – anyone can use any SMTP server to send e-mail. (For more information on this, see section **9.2.4 Forged Headers**.)

The second thing to note is that, when you send your secret password to the POP server, you send it in a plain-text format. It may be hidden by little asterisks on your computer screen, but it is transmitted through the network in an easily readable format. Anyone who is monitoring traffic on the network – using a *packet sniffer*, for instance – will be able to clearly see your password. You may feel certain that *your* network is safe, but you have little control over what might be happening on any other network through which your data may pass.

The third, and possibly most important thing that you need to know about your e-mails, is that they are – just like your password – transmitted and stored in a plain-text format. It is possible that they may be monitored any time they are transferred from the server to your computer.

This all adds up to one truth: *e-mail is not a secure method of transferring information*. Sure, it's great for relaying jokes, and sending out spunkball warnings, but, if you're not comfortable yelling something out through the window to your neighbor, then maybe you should think twice about putting it in an e-mail.

Does that sound paranoid? Well, yeah, it is paranoid, but that doesn't necessarily make it untrue. Much of our e-mail communications are about insignificant details. No one but you, Bob and Alice, care about your dinner plans for next Tuesday. And, even if Carol desperately wants to know where you and Bob and Alice are eating next Tuesday, the odds are slim that she has a packet sniffer running on any of the networks your e-mail might pass through. But, if a company is known to use e-mail to arrange for credit card transactions, it is not unlikely to assume that someone has, or is trying to, set up a method to sniff those credit card numbers out of the network traffic.

9.1.3 Web Mail

A second option for e-mail is to use a web based e-mail account. This will allow you to use a web browser to check your e-mail. Since the e-mail for these accounts is normally stored on the web e-mail server – not on your local computer – it is very convenient to use these services from multiple computers. It is possible that your ISP will allow you to access your e-mail through both POP and the web.

However, you must remember that web pages are *cached* or stored on local computers, sometimes for significant lengths of time. If you check your e-mail through a web based system on someone else's computer, there is a good chance that your e-mails will be accessible to someone else who uses that computer.

Web based e-mail accounts are often free and easy to get. This means that they offer an opportunity for you to have several identities online. You can, for instance, have one e-mail address that you use only for friends and another that is only for relatives. This is usually considered acceptable, as long as you are not intentionally intending to defraud anyone.

Exercises:

1. You can learn a lot about how POP e-mail is retrieved by using the telnet program. When you use telnet instead of an e-mail client, you have to enter all the commands by hand (commands that the e-mail client program usually issues automatically). Using a web search engine, find the instructions and commands necessary to access an e-mail

account using the telnet program. What are the drawbacks to using this method to retrieve e-mail? What are some of the potential advantages?

2. Find three organizations that offer web based e-mail services. What, if any, promises do they make about the security of e-mail sent or received using their services? Do they make any attempts to authenticate their users?
3. (possibly homework) Determine the SMTP server for the email address you use most frequently.

9.2 Safe E-mail Usage Part 1: Receiving

Everyone uses e-mail, and to the surprise of many people, your e-mail can be used against you. E-mail should be treated as a post card, in that anyone who looks can read the contents. You should never put anything in an ordinary e-mail that you don't want to be read. That being said there are strategies for securing your e-mail. In this section we will cover safe and sane e-mail usage and how to protect your privacy online.

9.2.1 Spam, Phishing and Fraud

Everybody likes to get e-mail. A long time ago, in a galaxy far far away it used to be you only got mail from people you knew, and it was about things you cared about. Now you get e-mail from people you never heard of asking you to buy software, drugs, and real estate, not to mention help them get 24 million dollars out of Nigeria. This type of unsolicited advertising is called spam. It comes as a surprise to many people that e-mail they receive can provide a lot of information to a sender, such as when the mail was opened and how many times it was read, if it was forwarded, etc. This type of technology – called web bugs – is used by both spammers and legitimate senders. Also, replying to an e-mail or clicking on the unsubscribe link may tell the sender that they have reached a live address. Another invasion of privacy concern is the increasingly common "phishing" attack. Have you ever gotten an e-mail asking you to login and verify your bank or E-bay account information? Beware, because it is a trick to steal your account information. To secure yourself against these types of attacks, there are some simple strategies to protect yourself outlined below.

9.2.2 HTML E-Mail

One of the security concerns with HTML based e-mail is the use of *web bugs*. Web bugs are hidden images in your e-mail that link to the senders' web server, and can provide them with notification that you have received or opened the mail. Another flaw with HTML e-mail is that the sender can embed links in the e-mail that identify the person who clicks on them. This can give the sender information about the status of the message. As a rule, you should use a mail client that allows you to disable the automatic downloading of attached or embedded images. Another problem is related to scripts in the e-mail that may launch an application ,if your browser has not been patched for security flaws.

For web based e-mail clients, you may have the option of disabling the automatic download of images, or viewing the message as text. Either is a good security practice. The best way to protect yourself against HTML e-mail based security and privacy attacks is to use text based e-mail. If you must use HTML e-mail, beware!

9.2.3 Attachment Security

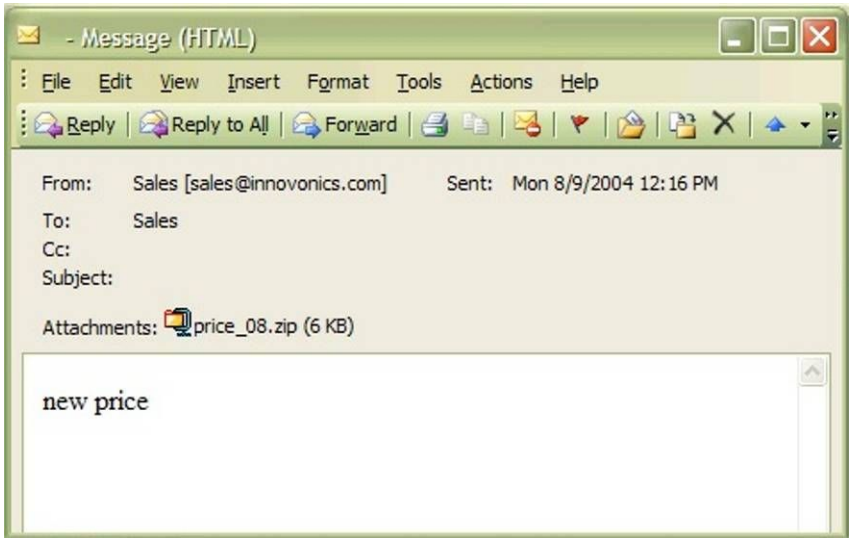
Another real concern related to received e-mail security is attachments. Attackers can send you malware, viruses, Trojan horses and all sorts of nasty programs. The best defense against e-mail borne malware is to not open anything from anyone you don't know. Never open a file with the extension .exe or .scr, as these are extensions that will launch an executable file that may infect your computer with a virus. For good measure, any files you receive should be saved to your hard drive and scanned with an antivirus program. Beware of files that look like a well known file type, such as a zip file. Sometimes attackers can disguise a file by changing the icon or hiding the file extension so you don't know it is an executable.

9.2.4 Forged headers

Occasionally you may receive an e-mail that looks like it is from someone you know, or from the "Administrator" or "Postmaster" or "Security Team" at your school or ISP. The subject may be "Returned Mail" or "Hacking Activity" or some other interesting subject line. Often there will be an attachment. The problem is that it takes no technical knowledge and about 10 seconds of work to forge an e-mail address. (It also – depending on where you live – may be *very* illegal.)

To do this, you make a simple change to the settings in your e-mail client software. Where it asks you to enter your e-mail address (under *Options*, *Settings* or *Preferences*) you enter something else. From here on out, all your messages will have a fake return address. Does this mean that you're safe from identification? No, not really. Anyone with the ability to read an e-mail header and procure a search warrant can probably figure out your identity from the information contained on the header. What it does mean is that a spammer can represent himself as anyone he wants to. So if Fannie Gyotoku [telecommunicatecreatures@cox.net] sells you a magic cell phone antenna that turns out to be a cereal box covered with tin foil, you can complain to cox.net, but don't be surprised when they tell you that there is no such user.

Most ISPs authenticate senders and prevent relaying, which means that you have to be who you say you are to send mail via their SMTP server. The problem is that hackers and spammers often run an SMTP server on their PC, and thus don't have to authenticate to send e-mail, and can make it appear any way they want. The one sure way to know if a suspicious e-mail is legitimate is to know the sender and call them up. Never reply to a message that you suspect may be forged, as this lets the sender know they have reached an actual address. You can also look at the header information to determine where the mail came from, as in the following example:



This is an e-mail from someone I don't know, with a suspicious attachment. Normally, I would just delete this but I want to know where it came from. So I'll look at the message header. I use Outlook 2003 as my e-mail client, and to view the header you go to view>options and you will see the header information as below:

```
Microsoft Mail Internet Headers Version 2.0
```

```
Received: from srv1.mycompany.com ([192.168.10.53]) by mx1.mycompany.com
over TLS secured channel with Microsoft SMTPSVC(6.0.3790.0);
       Mon, 9 Aug 2004 11:20:18 -0700
Received: from [10.10.205.241] (helo=www.mycompany.com)
      by srv1.mycompany.com with esmtp (Exim 4.30)
      id 1BuEgL-0001OU-8a; Mon, 09 Aug 2004 11:15:37 -0700
Received: from kara.org (67.108.219.194.ptr.us.xo.net [67.108.219.194])
      by www.mycompany.com (8.12.10/8.12.10) with SMTP id i79IBYUr030082
      for <sales@mycompany.com>; Mon, 9 Aug 2004 11:11:34 -0700
Date: Mon, 09 Aug 2004 14:15:35 -0500
To: "Sales" <sales@mycompany.com>
From: "Sales" <sales@innovonics.com>
Subject:
Message-ID: <cdkdabgurdgefupfhnt@mycompany.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="--------cfwriebwwbnnfkkmojga"
X-Scan-Signature: 178bfa9974a422508674b1924a9c2835
Return-Path: sales@innovonics.com
X-OriginalArrivalTime: 09 Aug 2004 18:20:18.0890 (UTC) FILETIME=
[868FEAA0:01C47E3D]
----------cfwriebwwbnnfkkmojga
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 7bit
----------cfwriebwwbnnfkkmojga
Content-Type: application/octet-stream; name="price_08.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="price_08.zip"
----------cfwriebwwbnnfkkmojga—
```

Now, the part I'm interested in is highlighted above. Note that the "Received" is from kara.org at an IP that appears to be an xo.net DSL line, which does not agree with innovonics.com, the purported sender.

Also, if I look up innovonics.com's mail server using nslookup, its address comes back as follows:

```
C:\>nslookup innovonics.com
Server:  dc.mycompany.com
Address:  192.168.10.54
```

```
Non-authoritative answer:
Name:    innovonics.com
Address:  64.143.90.9
```

So, my suspicion was correct, and this is an e-mail that is carrying some malware in an executable file posing as a zip file. The malware has infected the person's computer on the DSL line, which is now a zombie, sending copies of the malware to everyone in the infected computers address book. I'm glad I checked it out!

Exercises:

1. Citbank and PayPal are two of the most common targets of phishing emails. Research what Citibank or PayPal are doing to fight / control phishing.
2. Research whether your bank or credit card holder has a published statement about the use of email and personal information.
3. (possibly homework) Research a spam email you have received and see if you can determine the real source.

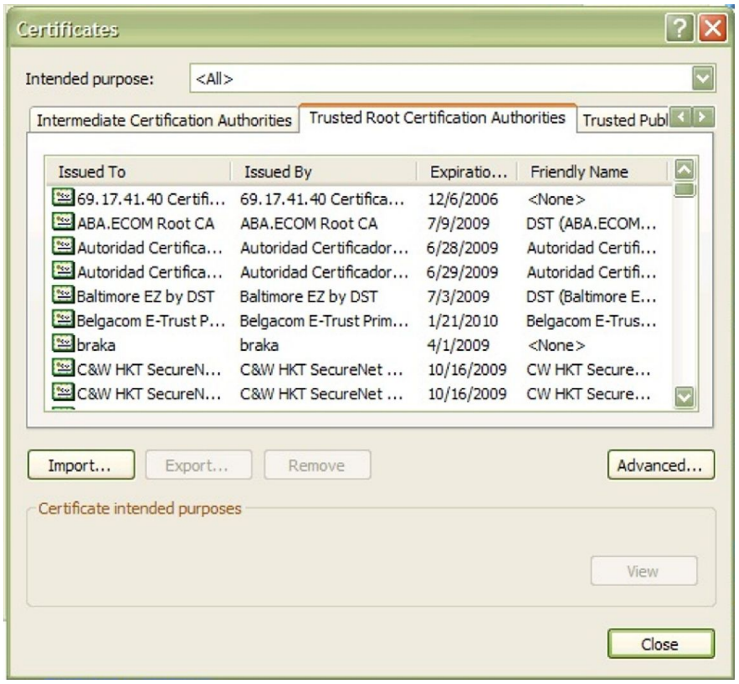
9.3 Safe E-mail Usage Part 2: Sending

Sending mail is a little more care free. There are some things you can do to make sure your conversation is secure though. The first is to ensure your connection is secure (see section **9.4 Connection Security** for more information). There are also methods to allow you to digitally sign your messages, which guarantees that the message is from you and has not been tampered with en route. And for maximum security, you can encrypt your messages to make sure no one reads them.

Digital signatures prove who e-mail comes from, and that it has not been altered in transit. If you establish the habit of using digital signatures for important e-mail, you will have a lot of credibility if you ever need to disown forged mail that appears to be from you. They also allow you to encrypt e-mail so that no one can read it except the recipient. PGP in particular offers high levels of encryption which to break would require extreme computing power.

9.3.1 Digital Certificates

A digital certificate is unique to an individual, kind of like a drivers license or passport, and is composed of 2 parts. These parts are a public and private key. The certificate is unique to one person, and typically certificates are issued by a trusted Certificate Authority, or CA. The list of Certificate Authorities you trust is distributed automatically (if you are a Microsoft Windows User) by Windows Update and the list is accessible in your browser under tools>internet options>content>certificates. You can go here to view certificates installed on your machine (yours and others), and other certificate authorities you trust.



You can disable the automatic update of CAs, and choose to remove all CAs from the list, although this is not recommended. Instructions on how to do this are on Microsoft's web site.

9.3.2 Digital Signatures

A digital signature is generated by your e-mail software and your private key to assure the authenticity of your e-mail. The purpose of the signature is twofold. The first is to certify it came from you. This is called non-repudiation. The second is to ensure the contents have not been altered. This is called data integrity. The way an e-mail program accomplishes this is by running the contents of your message through a one way hash function. This produces a fixed size output of your e-mail called a message digest. This is a unique value, and if the mathematical algorithm that produces it is strong, the message digest has the following attributes.

- The original message can't be reproduced from the digest.
- Each digest is unique.

After the digest is created, it is encrypted with your private key. The encrypted digest is attached to the original message along with your public key. The recipient then opens the message, and the digest is decrypted with your public key. The digest is compared to an identical digest generated by the recipients' mail program. If they match, then you're done. If not, your mail client will let you know the message has been altered. There are 2 types of signing / encryption functions, S/MIME and PGP. S/MIME is considered to be the corporate and government choice, possibly because it uses the less labor intensive certificate authority model for authentication, and because it is more easily implemented through Microsoft's Outlook Express e-mail program. PGP is more often the choice of the computer user community, because it is based on a non-centralized *web of trust* for authentication, where a user's trustworthiness is validated through the 'friend of a friend' system, where you agree that, if you trust me, then you can also trust those people who I trust, and because members of the computer user community don't really care if it takes them four hours to figure out how to

make PGP work with Thunderbird – they consider these types of challenges to be a form of *recreation*.

9.3.3 Getting a certificate

If you are interested in getting a digital certificate or digital ID, you need to contact a *Certificate Authority* (Verisign and thawte are the most well known, although a web search may find others.) Both require you to provide identification to prove to them that you are who you are. You can get a free certificate from thawte, but they require a significant amount of personal information, including a government identification number (such as a passport, tax id or driver's license). Verisign charges a fee for its certificate and requires that you pay this fee with a credit card, but asks for less personal information. (Presumably, Verisign is relying on the credit card company to validate your personal information.) These requests for information may seem intrusive, but remember, you are asking these companies to vouch for your trustworthiness. And – as always – check with your parents or guardians before you give out any personal information (or run up large balances on their credit cards).

The biggest disadvantage to using a certificate authority is that your private key is available to someone else – the certificate authority. If the certificate authority is compromised, then your digital ID is also compromised.

9.3.4 Encryption

As an additional layer of security, you can *encrypt* your e-mail. Encryption will turn your e-mail text into a garbled mess of numbers and letters that can only be read by its intended recipient. Your deepest secrets and your worst poetry will be hidden from all but the most trusted eyes.

However, you must remember, that, while this may sound good to you – and to all of us who don't really wish to be exposed to bad poetry – some governments do not approve. Their arguments may – or may not – be valid (you can discuss this amongst yourselves), but validity is not the point. The point is that, depending on the laws of the nation in which you live, sending an encrypted e-mail may be a crime, regardless of the content.

9.3.5 How does it work?

Encryption is fairly complicated, so I'll try to explain it in a low tech way:

Jason wants to send an encrypted message. So the first thing Jason does is go to a Certificate Authority and get a Digital Certificate. This Certificate has two parts, a Public Key and a Private Key.

If Jason wants to receive and send encrypted messages with his friend Kira, they must first exchange Public keys. If you retrieve a public key from a Certificate Authority that you have chosen to trust, the key can be verified back to that certifying authority automatically. That means your e-mail program will verify that the certificate is valid, and has not been revoked. If the certificate did not come from an authority you trust, or is a PGP key, then you need to verify the key fingerprint. Typically this is done separately, by either a face to face exchange of the key or fingerprint data.

Now let's assume that both Kira and Jason are using compatible encryption schemes, and have exchanged signed messages, so they have each others public keys.

When Jason wants to send an encrypted message, the encryption process begins by converting the text of Jason's message to a pre hash code. This code is generated using a mathematical formula called an encryption algorithm. There are many types of algorithms, but for e-mail S/MIME and PGP are most common.

The hash code of Jason's message is encrypted by the e-mail program using Jason's private key. Jason then uses Kira's public key to encrypt the message, so only Kira can decrypt it with her private key, and this completes the encryption process.

9.3.6 Decryption

So Kira has received an encrypted message from Jason. This typically is indicated by a lock Icon on the message in her in box. The process of decryption is handled by the e-mail software, but what goes on behind the scenes is something like this: Kira's e-mail program uses her private key to decipher the encrypted pre hash code and the encrypted message. Then Kira's e-mail program retrieves Jason's public key from storage (remember, we exchanged keys earlier). This public key is used to decrypt the pre hash code and to verify the message came from Jason. Kira's e-mail program then generates a post hash code from the message. If the post hash code equals the pre hash code, the message has not been altered en route.

Note: if you lose your private key, your encrypted files become useless, so it is important to have a procedure for making backups of your private and public keys.

9.3.7 Is Encryption Unbreakable?

According to the numbers, the level of encryption offered by, for example, PGP is unbreakable. Sure, a million computers working on breaking it would eventually succeed, but not before the million monkeys finished their script for *Romeo and Juliet*. The number theory behind this type of encryption involves factoring the products of very large prime numbers, and, despite the fact that mathematicians have studied prime numbers for years, there's just no easy way to do it.

But encryption and privacy are about more than just numbers. However, if someone else has access to your private key, then they have access to all of your encrypted files. Encryption only works if it is part of a larger security framework which offers protection to both your private key and your pass-phrase.

Exercises:

1. Is encryption of email legal in the country that you reside in? Find one other country that it is legal in,and one country where it is illegal to encrypt email.
2. Science fiction writers have imagined two types of futures, one in which people's lives are transparent, that is, they have no secrets, and one in which everyone's thoughts and communications are completely private. Phil Zimmerman, creator of PGP, believes in privacy as a source of freedom. Read his thoughts on why you need PGP at http://www.pgpi.org/doc/whypgp/en/. Then look at science fiction writer David Brin's article 'A Parable about Openness' at http://www.davidbrin.com/akademos.html in which he makes a number of points advocating openness as a source of freedom. Discuss these two opposing viewpoints. Which do you prefer? Which do you think would most likely succeed? What do you think the future of privacy will be like?

9.4 Connection Security

Last but not least is connection security. For web mail, ensure you are using an SSL connection to your ISPs e-mail. A small lock icon will appear in the bar at the bottom of your browser. If you are using POP and an e-mail client, ensure that you have configured your e-mail client to use SSL with POP on port 995 and SMTP on port 465. This encrypts your mail from you to your server, as well as protecting your POP / SMTP username and password. Your ISP should have a how-to on their web site to configure this. If they don't offer a secure POP / SMTP connection, change ISPs!

Exercise:

If you have an e-mail account, find out if your account is using SSL for its connection. How do you check this in your e-mail client? Does your ISP provide information regarding an SSL connection?8.0 Introduction

Further Reading

Can someone else read my e-mail?
http://www.research.att.com/~smb/securemail.html

MIT's PGP freeware page
http://web.mit.edu/network/pgp.html

General news on Internet privacy issues:
Electronic Privacy Information Center
http://www.epic.org/
and
Electronic Frontier Foundation
http://www.eff.org/

More about PGP
http://www.openpgp.org/index.shtml

How Reading an Email Can Compromise Your Privacy
http://email.about.com/od/staysecureandprivate/a/webbug_privacy.htm

Avoiding E-mail Viruses
http://www.ethanwiner.com/virus.html

A Brief Overview of E-mail Security Questions (with a short advertisement at the end)
http://www.zzee.com/email-security/

A Brief Overview of E-mail Security Questions (with no advertisement)
http://www.claymania.com/safe-hex.html

Windows Based E-mail Precautions
http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html
http://computer-techs.home.att.net/email_safety.htm

Differences Between Linux and Windows Viruses (with information on why most Linux e-mail programs are more secure)
http://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses/