CSE 590YA: Practical Aspects of Modern Cryptography
Winter 2002

Assignment #6

Due in class: February 19

This is a “mini-lab” – for this assignment we would like you experiment with sending and receiving digitally signed and encrypted e-mail.

There are two commonly-used formats for digitally signed and encrypted e-mail: S/MIME and PGP. The S/MIME format uses X.509 certificates to authenticate e-mail addresses; the PGP format uses PGP certificates. In this assignment we assume you’re running on Windows or a Mac and reading mail with a common mail reader (Outlook, Outlook Express, Netscape Mail, etc.) that already supports S/MIME (most common mail programs do), so we’re going to describe how to complete this assignment using S/MIME format messages which will let you experiment with X.509 certificates. If anyone is running on a Unix machine then it may be easier to use PGP with whatever mail client you use already. Let me know and I’ll write up quickie instructions on how to perform equivalent steps using PGP.

Using S/MIME to send & receive signed e-mail

Here are the high-level steps in order to configure your mail program to send and receive signed & encrypted e-mail using the S/MIME format with X.509 certificates.

1. Enroll for a digital certificate with a public CA that contains your e-mail address. As part of the enrollment process you will generate a public/private key pair that you can use to send and receive signed & encrypted e-mail.
2. Configure your e-mail program to use the new key pair to sign mail you send & decrypt encrypted mail you receive.
3. Send a signed e-mail message to bal@farcaster.com and gidon@cs.washington.edu. Please put “CSE590 signed message” in the subject line along with a witty message (to make it interesting ☺).
4. Send a signed & encrypted e-mail to bal@farcaster.com. Please put “CSE590 encrypted message” in the subject and some interesting text in the body. In order to encrypt a message to me you’re going to need my certificate; I’ll send a signed message to the class mailing list and you should be able to reply to that message.

The easiest way to enroll for an S/MIME certificate is to visit VeriSign or Thawte, the two largest public CAs. VeriSign has a free 60-day trial for S/MIME certs (they normally charge $14.95/year), and you should just sign up for the free trial (no need to spend money to complete this assignment). Thawte (now owned by VeriSign, actually) still issues free e-mail certificates. Feel free to use either CA (or try both if you wish);

they interoperate with each other and your browser/mail client should automatically trust both of them.
I would recommend that you start by visiting the VeriSign home page for what they call "Digital IDs for Secure E-mail" (S/MIME certificates) at http://www.verisign.com/products/class1/ . VeriSign has lots of on-line information about how to enroll for a certificate with various flavors of Netscape or IE/Outlook/Outlook Express. The basic process is the same:

1. Visit the "Personal Digital ID Enrollment" form (either click on the "Buy Now" button on the page referenced above or jump directly here: http://www.verisign.com/client/enrollment/index.html).
2. Click on the Enroll Now button.
3. Fill out the First Name, Last Name, E-mail Address and Challenge Phrase fields on the form.
4. Make sure to select "Test drive a 60-day trial" so you don't have to pay any money.
5. Don't bother filling out the credit-card information or street address fields, since you're signing up for a free trial.
6. If you're enrolling through IE, you'll see a drop-down box for the Cryptographic Service Provider to use. You'll want to use the Microsoft Enhanced Cryptographic Provider if it's there. If it's not there then you don't have the strong crypto upgrade installed for your OS. Horrors! Proceed with the Base Provider (weak crypto) and when you send me mail let me know you need a pointer to the strong crypto upgrade and I'll point you to it.
7. Read the nice legalese from VeriSign about their Certification Practice Statement (CPS) that governs their processes.
8. Click on "Accept" to start the ball rolling.

Eventually, VeriSign will e-mail you a URL and hash code to the e-mail address you specified. Once you have that URL & code you can go "pick up" your cert by visiting the URL & entering the code. That will download the freshly-issued certificate to you machine and install it for you.

Once you have the certificate on your machine, you'll need to associate it in your mail client with your e-mail account. VeriSign has some tutorial on how to do this with both OE and Netscape Messenger here: http://digitalid.verisign.com/client/help/tutorial.htm/.
Microsoft also has tutorials for Outlook Express:
http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/pubkeyox.asp
and Outlook:
http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/pubkeyol.asp
You need to associate the certificate you just received as both the "signing" certificate and the "encryption" certificate in your mail program. Once you've done that you should be able to send & receive signed & encrypted e-mail.

From within Outlook, you indicate that you want to sign and/or encrypt a message by creating a new message, clicking the Options button on the Toolbar, clicking the Security

Settings button, and then checking the check boxes for encrypting and/or digital signatures.

From with Outlook Express you sign & encrypt e-mail messages by creating a new message and then selecting the "Sign" and "Encrypt" buttons on the Toolbar.

Once you have everything set up, the first thing you should try to do is send yourself a signed e-mail message. That allows you to verify that you have the certificate appropriately associated with your e-mail account. Once you've received a signed message from yourself, try replying to the message and requesting that the message be both signed and encrypted. You should then receive (and be able to decrypt) the second message. Then try sending me a signed message and a second signed & encrypted message.

Here are some additional helpful hints:

1) If you'd like to try using Thawte certificates instead of VeriSign certificates, visit http://www.thawte.com/getinfo/products/personal/contents.html and then click on the "Join >>" button at the top of the page to step through the enrollment process for free S/MIME Personal Certificates.
2) It looks like Netscape v6.2 doesn't have S/MIME support yet because it's not in the Mozilla build that 6.2 was based on. Netscape 4.x mail clients do support S/MIME, and it looks like the latest Mozilla builds (0.9.7 and 0.9.8) do as well. I've tried this in the past with Netscape 4.x; haven't played with the new Mozilla builds yet so if you want to try go for it...
3) Above all, don't stress out too much if you can't get things to work. Send me mail and I'll try to help you through any rough spots you run into. The point of this exercise is to show you what the current state-of-the-art is in personal (S/MIME) e-mail. After you've gone through this exercise you'll know why we spend so much time trying to make the process of enrolling for certificates automatic within a corporate environment!
4) Finally, unfortunately I'll be on the road starting tomorrow at a week-long conference. I will have e-mail access at least nightly but maybe not more frequently than that. I'll respond to messages as soon as I see them, but as long as you manage to send the messages successfully before next class you'll have completed this assignment. (Getting a response back from me only confirms that you completed the task.)

Good luck!

--bal