Email A Postcard Written in Pencil

Lawrence R. Rogers
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA

When was the last time that you sent someone a postcard? Probably on your last vacation. The front of the postcard showed a beautiful picture of the place you visited, and the back contained your message. You wrote something light, such as "Having a wonderful time; wish you were here." Whatever you wrote, it really didn't matter much if someone else read it-it wouldn't be a problem for you or for them. You certainly wouldn't send credit card information or a bank account number on a postcard. You know that your postcard's message should suitable for the world to read.

You probably wrote the note using a pen, though you were not really thinking that someone might change your words after you wrote them. Nevertheless, even if they did change your words, you said nothing earth shattering, so who cares, right?

Now, when was the last time that you exchanged email with someone? Probably earlier today or most certainly not long ago. Did you know that that email is a lot like your vacation postcard, except that your email "postcard" is written in pencil, not pen? What a scary thought.

Email is usually written using one of the many Mail User Agents (MUAs) available on the market. Examples are Eudora, Outlook, and Lotus Notes. There are many MUAs and each has many features, some even useful. The MUA you use has the features you need and want, and is probably easy to use. Although there are differences between MUAs, and some differences are substantial, they all usually produce a text file to be sent through the Internet using Mail Transfer Agents (MTAs).

MTAs use a well-known and well-documented protocol (a set of rules for computer-to-computer communication), the Simple Message Transfer Protocol, affectionately referred to as SMTP. MTAs use SMTP to move email messages from computer system to computer system, eventually stopping (hopefully!) when the mail reaches its intended destination. How SMTP works is beyond the scope of this article, but suffice it to say that it does its job well and efficiently. Like the Post Office, MTAs use SMTP to deliver mail come rain or shine.

Let's examine an email message from start to finish. You first compose an email message with your Mail User Agent, and then you hand it over to your Mail Transfer Agent. Your MTA sends it to the next MTA and so on, using SMTP, until the message reaches its destination. The MTA at the destination computer system writes it to a computer disk somewhere-a mailbox-and the message waits there for the intended recipient to read it using their MUA. When they respond to the message, the process begins all over again.

Now, anyone who can gain access to your message as it is transferred from agent to agent can read it. For example, a nefarious bloke can change his (or her) MTA to save a copy of all mail somewhere on their disk, say, for later review. Another nefarious bloke could sniff the Internet traffic as it passes by and also read the very same message. Both techniques are easy to do

technologically and are virtually undetectable. Just like that postcard that passes through many hands between writer and reader, email can be read by anyone who can view the message as it passes by their electronic eyes.

Well then, if the blokes can read such a message, they probably can rewrite it too. Indeed they can. The technology doesn't prevent people from altering and resending a captured message. While changes to the postcard written in pen may be easier to detect (it's hard to erase ink cleanly), changes made to the email message written in pencil are virtually undetectable.

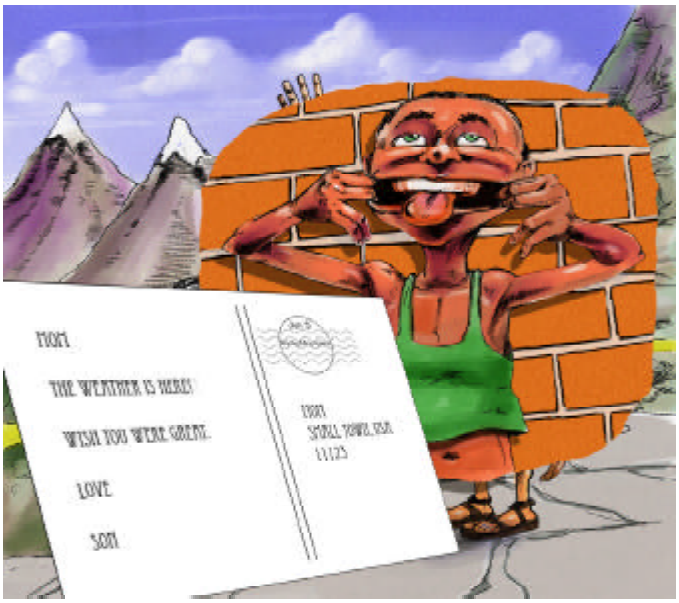
So what do you do about this? You can use the modern version of approaches used by royalty centuries ago. Julius Caesar used a cipher to encode a message so that only those who knew the code could read it, and the medieval kings sealed messages with wax imprinted with their ring to guard against tampering. Now we protect messages from unauthorized readers and from tampering with encryption and digital signatures.

Encryption is the process by which plain text-the message on the back of the postcard-is transformed into ciphertext through a cryptographic algorithm. An algorithm is a procedure for solving a problem, usually a mathematical one. There are many different cryptographic algorithms and they can be loosely categorized as either weak or strong. Strength is measured by the amount of time and computer resources-CPU time, memory, disk space-required to transform the ciphertext into its original plaintext.

Pivotal to each encryption algorithm is a key used in the transforming the text. In general, the more bits in the key, the stronger the encryption for a given algorithm. A strong cryptographic algorithm that uses a key with many bits produces cyphertext that is hard to decrypt. Through encryption, the email message can be transformed into a mass of symbols and letters that all can view but only few can decrypt and read.

A digital signature is another mass of symbols and letters that tells the message reader that the message received was the one sent and clearly identifies who sent it. The digital signature turns the message written in pencil into one written in indelible ink, and it verifies that the message came from the right person.

So much for theory-what products are available? There are many. One of the more popular products is PGP, which stands for Pretty Good Privacy. There are both free and commercial versions, and both provide encryption and digital signatures. PGP comes with plug-ins that augment some Mail User Agents by adding encryption and digital signatures. If your MUA is not supported by PGP, you can



still use PGP to encrypt and sign, but it's not as straightforward to do.

The key to any encryption and digital signature scheme is the key management system (pun intended). PGP uses its own scheme of key servers where you can find keys of others with whom you wish to exchange email. You can also use the key server to provide your key for others to retrieve. After you have created a key and published it, others can verify your signature and send you encrypted mail.

PGP keys are guarded by a pass phrase, which is longer and stronger than a password. Pick a long one, usually a phrase that includes punctuation, numbers, and anything that obscures it. Your key isn't any good without the pass phrase so don't forget it. Commit it to memory; don't write it on a sticky note and put it on your monitor; don't keep it in your desk drawer. This is a bit of data that you should never write down anywhere.

PGP and similar technologies give you the freedom to say what needs to be said using email as the transportation mechanism. You can encrypt your message so that only those you want to read the message can read it. You can also sign a message so that the readers can verify its integrity and author. If you can't use encryption or digital signatures to secure your email, just watch what you say. The whole world may be watching.