WHITE PAPER

Confidential and Authenticated Email Communication

PTP software provides necessary security for email. PTP is designed to be an independent "personal encryption tool". First, the problem.

Email security is a problem because

1) Email isn't secure
2) The internet is not secure
3) PC's, servers and Windows are not secure
4) People are not secure in their procedures
5) Data is valuable, so there are people out there who want your information

The assertions above are accepted as given nowadays but if you want chapter and verse there are many articles on the web explaining why this situation exists. The common denominator in all these problems is the complexity of big systems.

> There are no complex systems that are secure. Complexity is the worst enemy of security…
>
> Ferguson & Schneier 2003 Practical Cryptography Wiley Publishing Inc.

EMAIL SECURITY

> While the University e-mail server is generally secure, Information Services cannot absolutely exclude the possibility that someone may be able to obtain illegal access to it. In addition we have no control over who might have access to the content of messages that pass through systems outside the University network. It is prudent to treat e-mail like a postcard and not send in plain text anything that you regard as confidential.
>
> University of Exeter 2007

PTP turns your "postcard" emails into "sealed letters delivered by courier".

Encrypting the email effectively seals it and digital signatures ensure its delivery to the correct person and no-one else.

Encrypting email is not enough on its own, and one reason is "password management". The encryption is only as strong as the password. More importantly, you have to manage the password. If you regularly send encrypted files to a number of different people you somehow have to get the passwords to those people. This creates some serious loopholes. How do you get the passwords to them ? Do you use the same password ? Do you change it every time ? Where do you keep all these passwords ?

DIGITAL CERTIFICATES

PTP solves this with Digital Signatures, but we don't require you purchase a Digital Certificate. With Digital Signatures no passwords have to be transmitted or managed.

Software which uses Digital Signatures normally demands that you purchase and register a Digital Certificate. Why ? Because the authorities want your details ? Because its a profit opportunity for someone ? Can we trust any organisation to hold and control our digital signatures ?

In 2007 the UK national tax office HMRC managed to LOSE the details of 25 million people on 2 CD's including bank account details. What organisation can we trust to hold our data safely ?

Here are some more problems with Digital Certificates:

1) What if the Certification Authority (CA) loses its secret key ?
2) What if the CA issues false certificates ?
3) Digital Certificates only work for a limited time before they expire
4) There are many CA organisations, which do you choose ?
5) The CA organisations are mainly commercial companies.
6) They accept little or no responsibility for the certificates
7) Most CA structures are multi-level with a certificate chain
8) The impossibility of linking every certificate to an individual
9) The CA can impersonate anyone on the system
10) What if someone steals your identity ?
11) Digital Certificates are extremely difficult to revoke.
12) Registering and using Digital Certificates is complex

Basically, if the CA can be subverted, then the security of the entire system is lost.

Its amazing really that many people have chosen a Certification Authority and registered their information after seeing them on the web for the first time just a few minutes before.

All a Digital Certificate is trying to do is prevent impersonation. Encryption and Digital Signatures cannot stop someone pretending to be someone they are not. That job is supposed to be done by the Digital Certificate Authority, which is nothing more than a commercial company selling digital certificates.

The management of Digital Certificates is called Public Key Infrastructure (PKI).

Here is what Ferguson and Schneier have to say about PKI:

> "PKI's simply don't work in the real world like they do in the dream. That's why the PKI hype of a few years ago never matched the reality."
>
> IBID p323.

For email security the only reason you would want a Digital Certificate is if you wanted to exchange confidential information with complete strangers. The Certification Authority is supposed to be there so that if John Smith sends you an encrypted and signed document you can check up on who John Smith is, more accurately which John Smith it is. In other words which John Smith owns the Digital Signature being used.

That is fine (though not without problems) in the case of a web site like Amazon. They do want to be able to exchange confidential data with complete strangers, viz your credit card details. Therefore they have a Digital Certificate. Next time you check out and pay on a website look for the padlock symbol. Click it and you can view the vendor's complete Digital Certificate. Its complicated, and it has to be, they are collecting thousands of credit card details every day.

Now, its relatively easy for the Certification company to verify who Amzon is. It's not so easy for an anonymous individual like John Smith. Do we trust them to get it right ?

At the end of the day it doesn't matter, because in practice you don't need to be able to exchange confidential data with complete strangers by email. The people you exchange confidential information with are going to be known to you. Therefore, who is in the better position to validate the identity of your email correspondents, an anonymous commercial company on the web, or you ?

PTP allows you to certify your correspondents yourself, using exactly the same technology as the Certification Authorities, only better.

With PTP you do not have to purchase or register a Digital Certificate, and neither do your correspondents.

ENCRYPTION

While encryption is not enough on its own, it is absolutely a necessary part of the security. PTP is effective because it combines Digital Signatures and very strong encryption. These two components, authentication and encryption should not be confused and are both essential for proper security.

Cryptography is a whole branch of mathematics on its own and it is impossible for the email user to evaluate the various encryption models available. That's why the industry has tried to create a standard, so that you can trust the standard. Unfortunately, like PKI, the dream doesn't work out in practice.

I believe that the HMRC 2007 security breach was a watershed which confirmed what many people already thought, that the authorities and large organisations cannot be trusted to act responsibly. The reason is that they necessarily employ hundreds of people in a complex structure and they cannot totally control it all.

So when it comes to encryption standards you have to ask who influences the standards and what are their motives. The big organisations would like an option to de-crypt our data should they choose to, and that is the bottom line on encryption standards.

The current (US Government) "standard" is the cleverly named Advanced Encryption Standard (AES). In fact it is not particularly advanced and its not widely accepted as a standard, not by cryptographers anyway. Here is what the two leading experts in the field have to say about it:

> **"We have one criticism of AES: we don't quite trust its security…what concerns us about AES is its simple algebraic structure."**
>
> Ferguson & Schneier 2003

Lets be honest, a lot of experts think that the United States and British authorities at the very least can crack AES encryption and read AES-encrypted files, but we can't prove it.

The previous standard to AES was DES (Data Encryption Standard), but no-one seriously uses DES any more. The problem with DES was its small key size (56) and small block size (64), which were par for the computers of its time.

People have tried to extend the life of DES by doing it 3 times on each file and this is called 3DES, but there is no future in it, although its actually quite secure.

There is one benefit of these standards however. Because they are published algorithms anyone can take a crack at breaking them. If you have a totally new algorithm you never know it has a weakness unless people try to attack it. DES in particular has been around a long time and while it is known to have weak key lengths, the basic structure of DES is accepted as being sound.

We should differentiate here between DES and DEA. DES is the Data Encryption Standard and DEA is the Data Encryption Algorithm. DES uses DEA but it only uses small key lengths and block sizes. Many years of analysis of DEA by cryptographers have shown no weaknesses in the algorithm itself. PTP uses DEA as part of a bigger algorithm and it uses large key lengths and block sizes. The "wrapper" we use for DEA is RSA or Public/Private Key encryption.

RSA solves the problem of transmitting keys over the internet. Users have 2 keys, a Public Key which everyone can know and which anyone can use to Encrypt, and a

Private key which only you know and which you use to Decrypt. In other words you don't need to send me a secret key over the internet before I can encrypt a message for you. The math is quite involved but there are plenty of explanations on the internet if you are interested.

By combining RSA and DEA with a strong key length (384 bits) and large block size (512 bytes) PTP performs a very strong encryption. In addition to that, we combine them in a secret way which is unpublished. This secret additional methodology does not break the internal strength of the RSA and DEA models but it combines them in a very clever way. This unique methodology is registered to the author under the trade mark "Cyphermax".

> Mary had a little key, it's all she could export
> And all the email that she sent was opened at the Fort.
>
> Professor Ron Rivest Professor of Computer Science, MIT.

This way we have the benefit of the methodology and algorithms of DEA and RSA standards which are battle tested in the field over many years (in all Chip & Pin systems for example), but by using large keys and block sizes and combining them in a secret way we make the complete PTP algorithm extremely resistant to attack.

To summarise,

1) PTP uses the tried and tested encryption standards RSA and DEA
2) PTP adds large key lengths and large block sizes
3) PTP wraps RSA and DEA components together with Cyphermax
4) PTP then uses Digital Signatures to secure delivery

The complete package assures intact delivery to the intended recipient, "Person To Person".

WHY YOU NEED PTP - THE INTERNET IS NOT SECURE

So you click send and off goes your email. You expect it to arrive at the PC of whoever you sent it to. Have you ever considered what happens in between ?

"Because e-mail connects through many routers and mail servers on its way to the recipient, it is inherently vulnerable to both physical and virtual eavesdropping. Current industry standards do not place emphasis on security; information is transferred in plain text, and mail servers regularly conduct unprotected backups of e-mail that passes through. In effect, every e-mail leaves a digital paper trail in its wake that can be easily inspected months or years later." – Wikipedia

Try this,

Click Start/All Programs/Accessories/Command Prompt

Then, in the black DOS window type the following

```
tracert  microsoft.com  <enter>
```

Or any other domain name, eg skype.com or bt.com (just miss off the www of any web address).

What you see listed are the internet servers your communication with Microsoft (or whoever) has to go through before it reaches its destination. This is how the internet works. Millions of servers route traffic around the world. Messages hop from one site to another until the destination is reached. This is the internet's strength, because it doesn't depend on any one route or any one server.

The overall effect is that rather than being a transmission down a single piece of wire, an email transmission is a akin to a radio transmission. Your recipient will receive it but many others could be listening in.

Another problem is that (unlike a letter which is at least sealed) copies and traces of emails are left on the intermediate servers and these are then backed up to other media so potentially there are dozens of points where your documents can be intercepted even after the email has been delivered.

PC's AND SERVERS NOT SECURE

When email arrives at the other end it sits in a mailbox somewhere. That mailbox is either in a mail server belonging to a company or public organisation, or it is at an ISP (Internet Service Provider). How safe is it there ? All mail systems have technical administrators who have access to mail. Are any organisations "safe" from employees ?

At some point it arrives in your Inbox which, in turn, is in the mail client (eg Outlook) on your desktop PC or your laptop, or possibly on your Blackberry or other palmtop device. How safe is it there ? Lets examine the possible problems.

Someone could have access to your PC simply because it is switched on and unattended. Laptops, iPhones and iPads can be lost or stolen (in 2007 the British Government's tax offices HMRC 'lost' 41 laptops). Someone might know how to switch on and use your PC, maybe its not password protected, or maybe the password is known. Another possibility is that someone can log in to a dormant account that you never use such as "Guest" or "Administrator". Have you blocked access to all accounts on your PC apart from the one you normally use ?

PTP doesn’t save any intermediate files to your disc while it does its job. Most products do that, which leaves a trace on disc which could be “data mined”.

The following quote is from the WinZip manual.

> “When you open or view a file from an archive, WinZip must extract the file to a temporary location so that the associated program can open it. If you subsequently close WinZip without first closing the program that is using the file, WinZip may not be able to delete the temporary copy of the file, thereby leaving it on disk in unencrypted form. The associated program may also make one or more backup copies of the decrypted file, and WinZip will not be able to delete these. In addition, as described above, it may be possible for someone to later recover deleted files using file recovery software or the Recycle Bin.”
>
> WinZip Manual 2007

Disc drives create a whole new class of security problems due to they way they work. Essentially when a file is deleted it is not really deleted. Even when it is deleted from Recycle Bin it is still not deleted. Deleting only gets rid of the disc file index entry so that the file appears to have gone. It is extremely difficult to get rid of all traces of a file form disc.

PTP does not write any unencrypted data to disc and nothing is left behind from its activities. Once the file is encrypted and signed by PTP it can safely be sent by email through the internet and no unencrypted traces are left in the intermediate nodes and servers on its journey from sender to intended recipient.

EMAIL SOFTWARE IS NOT SECURE

If you receive a confidential attachment you normally copy it from Outlook to somewhere on your hard disk so that you have a copy you can keep, edit and generally use. You may well treat this file with the security it deserves. However, what about the copy left lying in the Inbox folder ? These normally hang around in there forever, or until the PC is thrown out. How many people clean up their email boxes when they throw out a PC ? What happens when the PC is swapped ? I saw a report recently where old PCs were being sent to Nigeria. Someone there was extracting the bank account details of the previous owners from the hard drives (data mining) and using this information for identity fraud.

When you add an attachment you browse the hard drive for the file you want and a copy is taken for the attachment. When you send the email the copy obviously sets off over the internet. However, in most cases a copy is sent to the Sent Items folder of Outlook and there it remains, unencrypted and waiting to be found.

PTP doesn't leave confidential stuff lying around in your email folders.

Email boxes normally contain thousands of old emails ready to be mined by the unscrupulous. I know its convenient when you have lost a document to be able to trawl through the Inbox and Sent Items folders to find a copy, but that convenience has to be weighed against the security costs. With PTP the attachments left behind in Outlook are completely safe.

> There are no complex systems that are secure. Complexity is the worst enemy of security…
>
> Ferguson & Schneier 2003 Practical Cryptography Wiley Publishing Inc.

Software packages takeover your PC. They install bits of themselves all over the place and you have no idea where or why: on the hard drive, in the Start Menu, on the desktop, in the task bar tray, in your Office applications, in your email applications, in File Explorer, in Internet Explorer, in your drivers, in your DLL's, in the Registry.

They just take over, and all these components use up resources on your PC, resources you have paid for. Bit by bit they make your PC go slower. Have you noticed how a brand new PC seems really quick, but after a while gradually starts to degrade ? Its because all these bits of recourses are being gobbled up by software fighting amongst themselves for your attention.

PEOPLE ARE NOT SECURE

Most security breaches occur because of human error. We have to accept that email is not secure and that someone out there wants our information. Only then will we see the need for the extra discipline that all security demands.

For example we now accept that immobilisers are necessary on our motor cars, which demands we carry about an electronic key fob and that we look after it properly ie we don't just pop it down by the front door. That new habit has to be learned the easy way or the hard way.

The new habit for email has to be to secure confidential documents. Not all emails require encryption security, but for the ones that do we need to get into the habit of taking the necessary steps to protect ourselves. There are some steps necessary to carry out the correct level of security, but with PTP we have reduced these to the absolute minimum compatible with our goals.

HOW PTP WORKS – IN A NUTSHELL

PTP works in a very clever and subtle way which is difficult explain simply. Look on the list of contacts in PTP as a list of very special PERSONAL KEYS. Unlike normal keys which can both lock and unlock, PTP keys can only lock. Lets say you have Alice, Bob and Carole in your list. Once you lock (encrypt and sign) a file for Alice you can't unlock it. Only Alice can unlock it, because only she has the unlock key. To unlock it she needs two things, her personal copy of PTP setup with her own user id, and her PTP password which never leaves her head. With PTP no-one has to share passwords in order to share secure documents. PTP is a very personal product.

If you lock (encrypt) a file for the special contact called 'myself' then you can unlock (decrypt) it yourself. This is useful for storing documents safely on your PC, or forwarding them by email so that you can pick them up later. You can also backup documents for yourself in encrypted form on a remote web server or FTP server.

We believe that within the law we have a right to protect our data. The purpose of PTP is very simple - to deliver your data with total security only to the person you address it to.

CONCLUSION

PTP (Person to Person) only does one job, but it does it extremely well. It doesn’t have any frills or thrills, no fancy graphics, no layers of hidden features you don’t need. Its just solid dependable software that won’t let you down, at a reasonable price, and you are only paying for what you use.