

# PTP SECURITY

## WHITE PAPER

Email security is a problem because

- 1) The internet is not secure
- 2) PC's, servers, Windows, Explorer and Outlook are not secure
- 3) People's procedures are not secure
- 4) Current solutions rely on Digital Certificates which are not secure
- 5) Traditional encryption methods are not secure
- 6) All data is valuable and needs to be protected

PTP Security software is designed to overcome all the above problems. We encrypt emails and attachments in a special way which guarantees that they will only be opened by their intended recipients.

### 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 trail in its wake which can be inspected months or years later.

Try this on your PC:

Click START/All Programs/Accessories/Command Prompt

Then, in the black DOS window type the following

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

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 akin to a radio transmission. Your recipient will receive it but many others could have access to it.

Another problem is that (unlike a letter which is at least sealed) copies and traces of emails can be left on intermediate servers, particularly at the ISP, 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. In other words, copies of your emails and attachments are left behind in the pipework which delivers them. If they are not encrypted they are at risk of being read for many years.

### PC's, SERVERS, WINDOWS, EXPLORER AND OUTLOOK ARE 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, Blackberrys and palmtops can be lost or stolen. 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”.

Disc drives create a whole new class of security problems due to the 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 quite difficult to completely get rid of all traces of a file from disc. Only encrypted data is safe on disc. Data protected by password but not encrypted on disc can be data mined.

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.

In general anything produced by Microsoft comes under intense attack all over the globe to try and break it, hence the constant stream of security updates. Their products are so complex and change so often that it impossible for them to be really secure.

### EMAIL SOFTWARE (eg OUTLOOK) 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 ? Scrap PCs are being sent all over the world where criminals extract 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. Even if you delete an email it just gets moved to the Deleted Items folder. Even when you delete it from there, guess what, it still isn't deleted and it remains on disc.

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.

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 ?

### 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 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.

### DIGITAL CERTIFICATES ARE NOT SECURE

PTP uses Digital Signatures, but we don't require you purchase a Digital Certificate.

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 ?

Here are some 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) They have certificate admin staff who come and go
- 8) Most CA structures are multi-level with a certificate chain
- 9) The impossibility of linking every certificate to an individual
- 10) The CA can impersonate anyone on the system
- 11) What if someone steals your identity ?
- 12) Digital Certificates are extremely difficult to revoke.
- 13) Registering and using Digital Certificates is complex
- 13) Certification Authorities are companies which are bought and sold
- 14) Do you really want ANY organisation to hold your encryption keys ?
- 15) Who within an organisation can use their private key, anyone ?
- 16) Your private key is held on your PC, what if it is lost or stolen ?
- 17) Certification Authorities don't accept any liability for mistakes.
- 18) We have no idea how good their internal security structures are
- 19) Under what circumstances must they disclose your data to 3<sup>rd</sup> parties ?
- 20) The whole Digital Certification edifice is so complex its bound to go wrong

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

Digital Certificates make the otherwise excellent RSA Public/Private key system over-complex, expensive and less secure.

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 cryptologists 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.”

Practical Cryptography 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 Amazon 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 ?

With PTP you do not have to purchase, register and maintain a Digital Certificate, and neither do your correspondents. This is a major advantage in terms of both user convenience and security.

Why do Microsoft use Digital Certificates with their S/MIME encryption ? The reason is that Microsoft are so big and ubiquitous that the government authorities take a keen interest in any encryption tools they put out. That has to be an influence on the decision to use Digital Certificates which ultimately are under the control of the security services.

They love the idea that everyone in the world using encryption has all their details and keys lodged with the certification authorities. Unfortunately its not secure.

### TRADITIONAL ENCRYPTION METHODS ARE NOT SECURE

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.

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 risk with encryption standards.

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”.

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.

However even if you had a massive encryption key and a brilliant secret algorithm it is mathematically possible that someone could guess it first time.

All we can say is that PTP encryption is more resistant to attack than anything else currently available, and anything else we have developed to date, and is going to be unbreakable in our lifetime. We already have encryption systems in the field which have been running uninterrupted for more than 20 years without a hitch. This experience and track record is incredibly important when assessing the strength of PTP encryption.

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”.

## CONCLUSION

Today all data is valuable. By piecing together seemingly unimportant bits of information about you, its possible to impersonate you over the internet in order to commit fraud. We have a duty, possibly a legal duty, to protect our data and that of our clients and correspondents and the organisations we work for.

PTP Security provides a solution which works and requires no training or administration.