Exam Papers Encryption Report

Introduction

Increasingly there are demands to securely prepare files and send them via email. In particular there is a demand evident for a system to allow examiners to prepare papers using electronic means. This often involves examiners in different locations who currently have to circulate papers in print form via standard mail. E-mail therefore offers a quick and efficient solution as long as security can be assured. However, if encryption can be seen to work for exam preparation, then it could be utilized for circulating other sensitive documents.

At a preliminary meeting involving representatives of the Proctors Offices, OUCS, the Medical Division, the Physics Departments, and the Law Faculty, key issues were discussed. Most importantly three recommendations emerged from this (under the advice of the security team at OUCS):

1) The only way to effectively maintain security was via file encryption, e.g. encoding the file so that it can only be decoded and read by nominated people. This had to be done at the point of creation (e.g. as soon as an examiner begins work on a paper using a word-processor, for example, it should be encrypted).

2) OUCS, with representative users from other departments, should therefore be asked to co-ordinate a trial of the user software available for encryption. Two packages were chosen – PGP and GPG. The first is a commercially available product and the second is a free piece of software.

3) Any machine storing exam papers and other sensitive material (e.g. in a Faculty/Department Office) should be kept off the network.

Software Trial: Basic Details

The trial aimed to see how usable these products were (e.g. PGP and GPG), in terms of the possibility of the average user utilizing them securely. As a result of the trial OUCS was asked to produce a set of recommendations for the Proctors. Users in OUCS and the Law Faculty took part in the trial.

Recommendations

The University regulations for preparation of exam papers should be expanded by the Proctors Office to allow staff to use the recommended encryption software (e.g. PGP) to prepare the material and exchange encrypted files.
The recommended encryption software will be PGP.
OUCS will only support PGP only, in terms of training and documentation; and could offer basic training on encryption software aimed at academics. It could run some preliminary sessions in Michaelmas Term, and would create a web site offering guidance and documentation on encryption.
When it comes to installing PGP this should be performed (or at least checked) by the appropriate IT Support Officer.
If PGP is accepted the University may wish to consider in the future purchasing the Universal Series 200. This allows for centrally managed security for email, file, and full disk security; minimising the risk of lost keys (for example). This would be maintained by OUCS but would involve a cost and new central funding would need to be secured.
Any machine that is being used to store a large collection of sensitive material should ideally be kept off the network. However, departments could also look to the PGP facility of allowing 'Full

Disk Encryption'. This would encrypt all the files on a machine, allowing them only to be read by nominated people. This would also secure data in the event of theft (and thus could be considered also for laptops with sensitive data contained on them).
Although GPG would not be supported by OUCS, users would still be allowed to use it (as it offers the same security level) but it is recommended only for highly IT-literate people, as its installation, user commands, and interface is far from intuitive.

Further Details of the Trial

This trial was carried out by OUCS staff, and comments were received by representatives from the Law Faculty who carried out their own trial. Other departments who originally signed up for the trial were unable to find the time to complete it. They were all reasonably IT literate but with limited or no experience of encryption or the tools/software used for encryption. The aims of the trial were:

To see how users responded to the basic concepts of public-key encryption.
To determine which tool users found easiest to use.
To highlight any possible problems users may have with encryption and the software.
To identify/highlight any possible pitfalls users may encounter.

The test involved:

Downloading and installing the appropriate software.
Creating a keypair (private/public key).
Creating a revocation certificate.
Distributing the public key.
Encrypting documents/emails for other recipients.
Encrypting files and folders for your own use.
Key revocation and deleting.

A brief overview of the principles of encryption was supplied to all the testers along with some basic instructions on how to use the software. However the testers were expected to locate and use the available on-line documentation for the relevant software.

Results of the Trial

The report from the Law Faculty stated that the download and installation was time consuming and fairly complicated. They also commented that use of the software was complicated, that the idea of public and private keys was not easy for a novice to understand, and that the documentation was not very clear. Although they did manage to encrypt and open an encrypted document problems were reported when using mail clients with the software. After two hours they "hadn't figured out how to use the software, nor how to find the relevant key on the user's computer, nor how to open the encrypted document on the receiver's computer."

Within OUCS two out of three users completed the PGP test without too many problems. They successfully downloaded the software, were able to create a keypair and distribute their public keys. They were able to successfully encrypt a document that only they would be able to read. They also managed to share their public keys and import other people's keys before transferring encrypted documents intended only for specific individuals.

The other user successfully downloaded and installed the PGP software and created a keypair. However they ran into problems distributing their public key. Instead they sent their private key, meaning that the recipient of the key would be able to 'steal' the identity of the sender and read

documents that were not intended for themselves. This is one of the major possible pitfalls of public key encryption. The key was also sent with no passphrase meaning that the recipient of the key could use it freely.

All users reported some problems with the software interfering with their mail clients. However this trial was not intended to test how the software worked specifically with mail clients so the users were given advice on how to turn off this functionality. In practice this would not necessarily be a problem if guidance was given on the correct configuration.

The trial of GPG was abandoned as it was deemed too complicated to install and use, and people generally did not have the time.

Overall the trial suggested the following (hence the recommendations noted earlier):

1) Both pieces of software will clearly encrypt files and provide acceptable security levels. However there are clear differences in terms of usability and cost.

PGP is more usable and would be more applicable to the average user. GPG is far less usable and the trial of it had to be abandoned. Although there is nothing to stop individuals from using GPG (as it is compatible with PGP) it would be preferable, from a training and support point of view, to recommend a single solution - PGP.

The remaining observations, therefore, relate solely to PGP.

2) The download and install process involves registration and a number of forms to be filled in. The process itself, however, was successfully carried out by reasonably IT literate staff.

3) The main issues arose with the users' lack of understanding of public key encryption. Training and guidance will therefore need to be provided for potential users. They will need, in particular, to be made aware of what public-key encryption is, what the security implications are, and what are the possible pitfalls associated with public-key encryption.

4) Some of the major pitfalls that were highlighted during this trial were:

The importance of keeping your private key secret and secure.
Key distribution – i.e. not sending your private key. This would allow anyone receiving that private key to read private, encrypted documents intended only for the true owner of the private key.
Use of strong, secure, passphrases: public key encryption is only as strong as the passphrase used to protect your public key.

However, it was noticed that once users knew what they were trying to do and why, it became easier for them to use the software to achieve their goals.

5) Training should also be provided in use of the software itself and it may be worth producing a step-by-step user guide rather than relying on the documentation that comes with the software. This conclusion was emphasised by the tests carried out by the Law Faculty.

Jonathan Ashton & Stuart Lee
OUCS
August 2006

http://www.pgp.com/.
http://www.gnupg.org/.
An individual user licence of PGP (stand-alone) is £57pa or £144 perpetual licence, but for the Universal 200 series managed solution this would be in the region of £155 per user, or £178 per user with full disk encryption. In addition funds would need to be found for a central server, maintaining the central server, and overall administration costs. For 100 users then this would be in the region (in total) of around £25k (with about £8k recurrent).