

IY2760/CS3760: Coursework 3

Solutions

1. PGP (Pretty Good Privacy) is a set of encryption and signature functions, a free version of which (GnuPG or GPG) is available for download on the Internet. It uses public key certificates but does not require the use of Certification Authorities (CAs). Describe some advantages and disadvantages of the PGP Keyring approach to public key management in comparison with the use of CAs.

[10 marks]

To use PGP, each user chooses a set of trusted people. He/she exchanges his/her public key with every member of this set. The set of public keys the user obtains through swapping in this way is known as a 'key ring'. When a signed message arrives, the user can only verify the signature if he/she has the appropriate key in his/her key ring. Equally, a user can only encrypt a message for another party if the user has the intended recipient's public key in his/her key ring.

There is a facility to not only accept a trusted person's personal public key but all keys they own (their key ring). This is done on the assumption that if I trust you, I will also trust who you trust.

This method of key management sounds unsafe, but in practice it seems to work.

When using CAs, each user must register with at least one CA and also submit his/her public key. In turn they get a copy of the CA's public signature verification key by trusted means. The CA generates a public key certificate for the user (a signed version of a concatenation of user name, user public key and expiry date). Anyone with the CA's public key can verify all public key certificates generated by that CA, and thereby obtain a trusted copy of a user's public key.

These two approaches have the following advantages and disadvantages:

- *In PGP the method of key management relies on trusting many individuals, some of whom may be unknown to the user (when using the facility of accepting another user's entire key ring). This is obviously a potentially dangerous situation. However, the method is quick, easy and fairly secure.*
- *With a CA, trust is placed in one organisation, who will (one hopes) take great care over key management as their business depends on their reputation. This method is comparatively long and drawn out (at least for initialisation) and a little more complicated, but potentially more secure.*

- *The CA approach is much more likely to be acceptable to a large organisation, whereas PGP is simpler to use for secure communications between individuals.*

2. What precautions should be taken when choosing passwords?

[5 marks]

Passwords should not be combinations of symbols likely to be found in any dictionary or other special 'password-guessing' list. This rules out the use of all natural language words and proper nouns. It is also advisable to avoid names followed by (or preceded by) a single numeric digit.

The best advice is to construct the password according to the following rules:

- *Avoid words in any common languages (including proper nouns).*
- *Always include one and preferably two non-alphabetic characters in a password.*
- *Avoid short passwords (passwords should always contain at least 6 and preferably 8 characters). Note that Unix usually ignores any characters after the eighth in a password.*
- *Avoid using any too closely specified publicly suggested method for generating passwords (apart from the use of random strings). Devise your own method of choosing a memorable but unguessable string – e.g. an anagram of a word intermingled with a number or two.*

3. What is wrong with the following 'challenge-response' user identification system?

Every user has a calculator capable of displaying 11 digits, and every also has a secret 10-decimal digit password. When a user wishes to authenticate him/herself to the system, the system generates a random 10-digit number and sends it to the user. The user (using the calculator) computes the sum of his/her secret password and the random number and returns it to the system, which then performs the same calculation (and hence verifies the user's identity).

[5 marks]

Suppose an interceptor is armed with the following information:

- *Complete knowledge of the system;*
- *A 10-digit challenge, C say, and the matching response, R say, from a user.*

The interceptor will know that, if the user password is P, the following equation must hold:

$$R = P + C.$$

Hence the interceptor can very easily reconstruct the password by calculating

$$P = R - C.$$

4. Distinguish between user *identification* and identity *verification* schemes. List the five component modules of an architecture for a typical biometric system for personal identification, and briefly describe the purpose of each module.

[10 marks]

User identification involves determining the claimed identity of a user. Identity verification (or user authentication) involves verifying whether or not a claimed identity is correct.

The five components of a typical biometric system are as follows:

- 1. Data Acquisition: reads biometric information from the user using equipment e.g. camera, fingerprint scanner, microphone. This must address environmental issues.*
 - 2. Feature Extraction: this involves extracting the distinguishing features from the raw data provided by the data acquisition component, and transformed this into a small set of bytes.*
 - 3. Matching module: measures the similarity of the claimant sample with a reference sample, returning a score.*
 - 4. Decision module: interprets the score from the matching module, returning yes or no.*
 - 5. Storage module: maintains the templates for enrolled users. Templates may be stored in the biometric device, in a conventional DB or on a portable device such as a smartcard.*
5. Think of a human characteristic (not mentioned in the course notes) that might be used for identity verification for computer users. What sort of parameters would you measure?

[10 marks]

Any plausible answer will do.

6. Within the various categories of malware, what is the main difference between worms and viruses? Name real-life examples of a worm and a virus, and briefly explain how these particular examples propagate themselves.

[8 marks]

Both viruses and worms propagate themselves, but in different ways. A virus is a program fragment that infects other programs by modifying them to include a copy of the virus code, which can then go on to infect other

programs. A worm is a replicating but non-infecting program that uses network connections to spread from system to system.

Concept was the first widely disseminated macro virus for Microsoft Word. It spread via infected word documents, e.g. sent as email attachments. Infected files were 'regular' Word documents that contained a special macro containing the virus. When it was originally circulated it took advantage of the fact that the macro system in Word had essentially unlimited powers and users were not warned about macros present in files that they opened. As a result of this virus (and other related viruses), Microsoft put much stricter controls on the operation of macros.

The 'original' computer worm was (perhaps accidentally) unleashed on the Internet by Robert Tappan Morris in 1988. The Internet Worm used sendmail, fingerd, and rsh/rexec to spread itself across the Internet.