

IY5512: Coursework 5:

Worked solutions

1. *What precautions should be taken when choosing passwords?*

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. Of course, the degree to which passwords need to be 'strong' depends on how easy it is to construct a 'guessing attack'.

General 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.

2. *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).

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

$$P = R - C.$$

3. *How can the S/KEY system be attacked if a malicious party succeeds in impersonating the host?*

S/KEY is based on the repeated application of a one-way function of a secret key. First apply the one-way function N times to the secret key (to get the 1st password), then apply $N-1$ times (to get the 2nd password), and so on – giving N one-time passwords.

The one-time passwords $f^i(S)$ must be used in the correct order, since knowledge of the final password reveals all the others. This means that, if an attacker can impersonate the host and send the challenge $i=1$, then the user will respond with $f(S)$, which can be used to impersonate the user.

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.*

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:

- Data Acquisition: reads biometric information from the user using equipment e.g. camera, fingerprint scanner, microphone. This must address environmental issues.
- 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.
- Matching module: measures the similarity of the claimant sample with a reference sample, returning a score.
- Decision module: interprets the score from the matching module, returning yes or no.
- 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?*

Any plausible answer will do!

6. *What are meant by Type I and Type II errors in a human authentication system? Describe how this relates to threshold setting.*

A **Type I error** is where the system fails to identify a valid user (a 'false rejection'). A Type II error is where the system accepts an impostor (a 'false acceptance' or 'impostor pass').

The value of the acceptance threshold is crucial to the performance of the system and depends on the security requirements of the application. If the threshold is relatively high (i.e. it is tough to meet), more valid users will be rejected (the false non-match rate will be high) but less impostors will be accepted (the false acceptance rate will be low). On the other hand, if the threshold is relatively low (i.e. it is easy to meet), more impostors will be accepted (the false match rate will be high) but less valid users will be rejected (the false non-match rate will be low). There is thus a trade-off between these two types of errors; that is, the threshold setting will depend on the security requirements of the application.

7. *Describe how an identity management system based on the use of HTTP redirects can be attacked. How can the damaging effects of such an attack be reduced?*

HTTP allows a web server (e.g. a service provider (SP)) to redirect a web client (i.e. a user's web browser) to another website. Thus a web server can set up an SSL session and then redirect the user browser to a third party identity provider (IdP) site for the purposes of authentication. The IdP can authenticate the user and then redirect the user back to the SP, and simultaneously transparently pass the SP assurances about user identity. This approach is widely used in identity management systems.

It has the advantage of being essentially invisible to user. There is minimal overhead on the user – the user simply needs to establish an authentication relationship with a third party IdP. It saves the user the need to authenticate to the SP web site, so it may be very convenient. The SP is offered a third party guarantee regarding identity of user.

Given that the only 'reliable' link that the server has to the user is the SSL connection, using SSL and HTTP redirection to provide user authentication seems sensible. This is fine if this does not change the relationship of the user to web servers and services offered, i.e. if the reliance on the security scheme is not increased.

However, the user may not be connected to genuine web server – in which case the browser may be redirected to a fake (malicious) IdP. Alternatively, a genuine (but fraudulent) SP might also falsely redirect the user browser. False redirection means that the user may very well divulge authenticating information (for use with a genuine IdP) to the fake IdP. The malicious party can now impersonate the user to this IdP. If the affected IdP is used for only one SP, then the impact is no worse than existing risks for the use of SSL. However, if the IdP is used for multiple SPs, then the impact is much more serious – since impersonation to all servers may be possible.

The fact is that browsers are simply not designed to offer a sound basis for user communications security. Users cannot reliably determine who they are talking to, even when SSL security is in use. Hence, in making life simple for users, users may be unaware of the risks.

HTTP redirection vulnerabilities can be significantly reduced by using a more secure means of user authentication to the IdP. For example, authentication could be based on tokens, one-time passwords and/or challenge-response. In such a case, theft of long-term authenticating information via false redirection is no longer possible.