SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1, 2014

Outline solutions for Workshop for L8: Access Control Mechanisms

QUESTION 1

Reusable passwords are the authenticator most commonly used for computer systems. However, there are some problems associated with their use.

a) Briefly describe the problems associated with reusable passwords.
b) Which of these problems are specific to user selected passwords?
c) Which problems are more commonly associated with computer generated passwords?
d) Information security expert Bruce Schneier's blog "Schneier on Security" (available at http://www.schneier.com/blog/) has an April 24, 2013 blog posting on password protection mechanisms. The post includes a link to an Ellen de Generes video where a password protection device is discussed. Which of the problems you identified above are discussed in the video? What does Ellen suggest is a security issue with the proposed password protection device?

a) See Lect 8 slide 12:

a. **Easy to share (intentionally or not)**
b. **Easy to forget**
c. **Often easy to guess**
d. **Can be written down**
e. **Don't provide non-repudiation if known to system also**

b) All of these problems apply to user selected passwords.

c) Computer generated passwords stop users choosing weak or easy to guess passwords, but make it more likely that the password will be written down. Computer generated passwords can still be shared or forgotten, and may also be known to the system.

d) Problem is users forgetting passwords. Device is a book to write them all down in (instead of using post-it-notes). Ellen comments that now all the passwords are in the one place, so this password protection device now requires protection. It's a funny video, but this really is a security issue! The security of all of the passwords depends on the protection provided to the record book. You need to think about the threat source to decide what sort of protection is appropriate.

QUESTION 2

Where passwords are user selected, the application of a password checking process should be considered, as a means to ensure quality passwords are used.

a) Read through Section 11.3 *User responsibilities* of AS27002 *Code of practice for information security management* to find the advice to users on selecting quality passwords. Record this advice.
b) Password checking can be *proactive* or *reactive*. Explain the process involved in each case. What sort of checking is performed for QUT Access passwords?
c) What are the advantages and disadvantages associated with each of the methods discussed in part b)?

a) Sect 11.3: Passwords should:

a. **have sufficient minimum length;**
b. **be easy to remember;**
c. **not be based on personal information such as names, telephone numbers, date of birth;**
d. **not consist of dictionary words;**
e. **avoid repeated characters.**

b) Password checking:

- **<u>Proactive password checking</u>: The user chooses a potential password and it is tested to see if it meets defined password criteria. Unsuitable passwords will be rejected and the user must choose another potential password.**
- **<u>Reactive password checking</u>: System administrator periodically runs a password cracking tool (those available to attackers) and seeks those passwords that are easy to recover. Sys admin must meet these users and explain security issue with unsuitable passwords and user's responsibility to choose stronger password.**

c) Advantages/Disadvantages:

- **<u>Proactive password checking</u>:**
  - **<u>Advantage</u>: user cannot use a password that does not meet the system criteria. Also, does not require sysadmin to go and meet users to discuss password choices.**
  - **<u>Disadvantage</u>:**
    - **If there are many criteria and users experience too many potential passwords being rejected, the users will complain.**
    - **If the criteria (algorithm) for an acceptable password are too simple, this may actually aid an attacker by reducing the number of possible passwords (password space) to a much smaller number than might otherwise have been the case.**
- **<u>Reactive password checking</u>:**
  - **<u>Advantage</u>:**
    - **can find unsuitable user passwords and stop them being used (ie better than no checking of passwords), and**
    - **Sys admin must meet these users and explain security issue with unsuitable passwords and user's responsibility to choose stronger password – so provides opportunities for user education.**
  - **<u>Disadvantage</u>:**
    - **user may have been using unsuitable password for a while before reactive checking is done,**
    - **sysadmin knows user passwords can masquerade as user**

QUESTION 3

An alternative to reusable passwords is to use one-time passwords. The one-time password system S/KEY makes use of a hash function to produce a series of one-time passwords. Read the article on Wikipedia about S/KEY: `http://en.wikipedia.org/wiki/S/key`, and use the information to answer the following questions:

a) Give an example of a situation in which S/KEY could be used.
b) Explain the basic operation of S/KEY in terms of what is computed and stored
   i. *on the client side* and
   ii. *on the server side* and
   iii. *what is sent* each time the protocol is run.

c) Which property of cryptographic hash functions is required in order for S/KEY to be secure?

a) Example: use for authenticating to a system from an untrusted public computer. Don't want to use a reusable password which may be captured and replayed later.
b) We can write $H^n(w)$ to denote the iteration n times of the hash function H to the original secret w. Thus: $H^2(w) = H(H(w))$, $H^3(w) = H(H(H(w)))$ and so on.

i) To set up the system, begin with the secret w and apply the hash function repeatedly. After the setup $H^n(w)$ is stored on the server.
ii) To authenticate the first time, the client sends $H^{n-1}(w)$. The server computes the hash of this value and compares it with the stored $H^n(w)$. If it matches, authentication of the client is complete.
iii) The server then discards $H^n(w)$ and stores $H^{n-1}(w)$.
iv) To authenticate the second time, the client sends $H^{n-2}(w)$. The server computes the hash of this value and compares it with the stored $H^{n-1}(w)$. If it matches, authentication of the client is complete. and the new value replaces the previously stored hash, and so on.

c) The necessary property to maintain security it that knowing any one-time password does not give away the next one-time password. The next password is the one which, when hashed, gives the current password. That is, to use the current password to compute the next password requires the inversion of the hash function. So we need the hash function to satisfy the *one-way* property (see the slides on hash functions in Lecture 6 Symmetric Cryptography).

QUESTION 4

Hardware tokens are an example of object-based authentication – authentication based on *something you have*.

a) The synchronised one-time password generator is one method to provide user authentication. Describe the operation of the synchronised password generator method using clock-based tokens.
b) Watch the video 'How do RSA SecureID tokens work' available at: http://www.youtube.com/watch?v=k_zpbJF9pmc.
   i. Look carefully at the 6-digit display showing on the device. How often does it change?
   ii. From the explanation given in the video, explain how the system manages a small loss of synchronisation (say, clock drift of one minute) between the device and the authentication server (About 3 minutes in to the explanation).
   iii. What is the probability that an attacker could guess the correct passcode (6-digit number) and gain access?
c) Read the section of the Wikipedia entry on SecureID http://en.wikipedia.org/wiki/SecurID that relates to the RSA security breach in March 2011. What are the hackers alleged to have obtained from RSA, and how would this information be of use to them?
d) Briefly explain the operation of a token-based challenge-response system.
e) Describe one major advantage and one major disadvantage for hardware tokens, when compared to standard user-selected passwords.
f) Compare the two token-based methods (clock based or counter based). What is a possible advantage of each compared with the other?

a) See slides 29-32.

i. **The user enters PIN which is used together with clock on token to produce the current value.**
ii. **The value changes for each time period. The user sends the current value to the host.**
iii. **The host computes the same value using the algorithm with inputs: user's ID, PIN and clock value.**
iv. **The host compares the received value with the computed value and accepts user as authentic if the values are the same.**

b) **From the RSA SecureID video:**
   i. **The 6 digit display changes every minute.**
   ii. **If the clocks are not synchronized, the value sent will not be the same as the one the host is expecting. When values don't match, the host system calculates the value for the minute prior to time on the host clock, and one minute after. If one of these values matches, then the host system permits access and stores an offset value, so that it knows in future that user module has a clock time different by that mush from the host clock time.**
   iii. **The value has 6 digits, so if an attacker is just randomly guessing a 6 digit number, there's a one in a million chance that they will guess it correctly.**

c) **The attackers in the RSA breach are alleged to have obtained the seed inputs for the RSA SecureID tokens (the set of symmetric keys – each device uses a unique symmetric key, and the key used is linked to the serial number on the device). If these values and the time and algorithm are known, the attackers can produce all of the 6 digit codes that the devices display, so could use this to gain access to protected systems.**

d) **See slides 35-37.**
   i. **A challenge is sent in response to an access request. The challenge is generally a number.**
   ii. **A legitimate user can respond to the challenge by performing a task which requires use of information only available to the user (and possibly the host).**
      - **The response is computed as a cryptographic one-way function of challenge and other info such as key and PIN.**
   iii. **User sends the response to the host. If the response is as expected by host, then access is granted.**

e) **<u>Advantage</u>: single use (one time) password is secure against password guessing or replay: reusable passwords are not. <u>Disadvantage</u>: problems if synchronisation between token and host is lost, also security issues around possible loss or theft of token.**

f) **A possible advantage of the clock-based tokens is that they do not require interaction with the host before authentication takes place. A possible advantage of the challenge-based tokens is that they do not require a synchronised clock.**

QUESTION 5

An alternative means for user identification and authentication makes use of biometrics.

a) Briefly define the concept of a biometric.
b) A basic biometric system consists of four main modules. Briefly describe these four modules.
c) A biometric system may operate in either *verification* mode or *identification* mode.
    i. Briefly explain the operation of both of these modes.
    ii. When the system is in use, which of these modes is likely to return a result faster? Explain your answer.

a) A biometric is an automated method of verifying the identity of, or recognising a person based upon a physiological or behavioural characteristic.
b)See slides 39-45

- **Sensor module: captures the biometric signal of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user's finger.**
- **Feature extraction module: processes the acquired biometric signal to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.**
- **Matcher module: features captured during recognition are compared against the stored templates to generate matching scores.**
- **System database module: used by the biometric system to store the biometric templates of the enrolled users.**

c) See slides 46-49

- **In *verification* mode the user claims an identity. A new biometric sample is captured and compared to the stored template corresponding to the user's claimed identity. A decision is made on the closeness of the match. The access request is accepted or rejected.**
- **In *identification* mode the user *does not* claim an identity. A new biometric sample is captured and a search is conducted of the templates of all the users in the database for a match.**
- **Identification is likely to take longer to return a result for an individual, as it requires a search of the database (n-to-1 comparisons) instead of the 1-to-1 comparison process to determine matching required for verification.**

QUESTION 6

Any human physiological or behavioural characteristic can be used as a biometric characteristic as long as it satisfies four basic requirements.

a) Briefly describe each of these four requirements.
b) For a proposed biometric system (a system that employs biometrics for personal recognition) there are three practical aspects that require consideration. These are Performance, Acceptability and Circumvention. Briefly describe what each of these three aspects considers.
c) An article in 2008 noted the publication of the fingerprint of a high ranking German public official: http://www.theregister.co.uk/2008/03/30/german_interior_minister_fingerprint_appropriated/. Relatively inexpensive methods for making use of publically available fingerprints have also been widely reported (example: the news

article relating to Tsutomu Matsumoto's 'gummi bear' fingerprint research: http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/). How could the published fingerprint be used? How does the publication of this fingerprint relate to your answers to parts (a) and (b)?

d) Briefly describe the extent to which each of the following biometric types satisfies the characteristics and issues you described for parts a) and b).
   i. Fingerprints
   ii. Facial recognition

a) The four requirements are:

i. ***Universality:*** **each person should have the characteristic;**
ii. ***Distinctiveness:*** **any two persons should be sufficiently different in terms of the characteristic that it is possible to distinguish between them;**
iii. ***Permanence:*** **the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;**
iv. ***Collectability:*** **the characteristic can be measured quantitatively.**

b) The practical aspects to consider include:

- ***Performance:*** **the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, the operational and environmental factors that affect the accuracy and speed;**
- ***Acceptability:*** **the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;**
- ***Circumvention:*** **how easily can the system be fooled using fraudulent methods.**

c) Someone could make a fake finger and put this fingerprint on it. If authentication is based on the fingerprint alone, this could be used for circumvention of access control systems. Other people could use this to claim the identity of the official and access resources he is entitled to access. *Multi-factor* authentication, where the biometric is only one factor, would improve the security.
When many people possess a usable copy of the fingerprint, we don't have distinctiveness (the system can not tell the difference between the legitimate authorized person and the imposters that can also provide the required information) and the means to circumvent the system is clear.
d) Using ratings of high, medium and low, respectively, where high is the most desirable (for example, High for circumvention means that resistance to circumvention is high).

Characteristic	Universality	Distinctiveness	Permanence	Collectability
Fingerprint	Medium	High	High	Medium
Facial recognition	High	Low	Medium	High

Characteristic	Performance	Acceptability	Circumvention
Fingerprint	High	Medium	High*
Facial recognition	Low	High	Low

Fingerprints: A small proportion of people do not have suitable fingerprints for identification because of genetics, age, environment or occupation, so universality is medium. Fingerprints are practically unique and permanent. Fingerprint scanners are affordable and appear on many commodity devices today. It is usually possible to collect a good sample, but may not always be in adverse environments. Taking

fingerprints is a bit intrusive and often associated with criminal activity so not as acceptable as some other methods.
***There are a range of different methods used, and some are easier to circumvent than others.**

Facial recognition: Is a non-intrusive method commonly used by humans. It scores well on universality and acceptability. There are different methods to obtain an accurate quantitative sample so collectability is good. Measurements can vary considerably with lighting and viewing angle which detracts from permanence. Moreover, facial measurements on their own provide a questionable basis for identification, so uniqueness and performance are rated low. This also affects circumvention, particularly if the subject does not cooperate (for example by presenting a different viewing angle).

QUESTION 7

a) The matcher module in a biometric system computes a matching score ***s*** that quantifies the similarity between the user input and the template representation stored in the database. Briefly explain how the matching score ***s*** and the threshold ***t*** are used to determine mate pairs.
b) For the terms *false match rate* (FMR) and *false non-match rate* (FNMR)
   i. Clearly explain what each term means.
   ii. Give an example related to facial recognition to illustrate your explanations.
c) Explain how the FMR can be reduced.
d) Explain how the FNMR can be reduced.
e) Explain how the trade-off between security (low FMR) and practicality (low FNMR) is related to the threshold *t*.
f) Can you think of an example where it is more important that the false match rate must be very low?
g) Can you think of an example where it is more important that the false non-match rate is low?

a) Pairs of biometric samples generating scores s higher than or equal to t are inferred as mate pairs (i.e., belonging to the same person). Pairs of biometric samples generating scores lower than t are inferred as non-mate pairs.
b) False match rate (FMR): the rate at which biometric measurements from two different persons are incorrectly declared to be from the same person. Example: the rate at which the system makes an error and decides the face of one person actually matches the stored template of a different person.
False non-match rate (FNMR): the rate at which two biometric measurements from the same person are incorrectly declared to be from two different persons. Example: the rate at which the system makes an error and decides the face of one person does not match the stored template of that person, when it actually is that person.
c) Reduce FMR by increasing t.
d) Reduce FNMR by decreasing t.
e) Both FMR and FNMR are functions of the system threshold t. If t is decreased to make the system more tolerant to input variations and noise, then FMR increases. On the other hand, if t is raised to make the system more secure, then FNMR increases accordingly. So it's a tradeoff.
f) Want False Match Rate to be very low in high security situations where it is critical to only allow in the authorized person, and preferable to lock out authorized user rather than admit unauthorized user. Say accessing the controls of a high security facility.

g) Want False Non Match rate to be low in situations where it is important that the required user is not excluded, even if other candidates are included. Say scanning for a known criminal at a border checkpoint. Picking up many wrong candidates, and then going through the pool of possibilities and excluding them is better than setting the threshold high and letting the criminal escape.