CSS322 – Quiz 7

Security and Cryptography, Semester 2, 2010

Prepared by Steven Gordon on 14 February 2011
CSS322Y10S2Q07, Steve/Courses/CSS322/Assessment/Quiz7.tex, r1683

Question 1 [3 marks]

Consider a computer system where the requirements for user authentication are to allow users to select any password they wish, and they are allowed to make an unlimited number of incorrect attempts. Explain a technique that you would implement to make the system more secure against online attacks. Also explain a disadvantage of that technique.

Consider a computer system where the requirements for user authentication are to allow users to select any password they wish. This computer system does not have enough memory to store logs. Explain a technique that you would implement to make the system more secure against online attacks. Also explain a disadvantage of that technique.

Answer. *The system can be made more secure against online attacks using the following methods:*

- *Limit the number of incorrect password attempts the user can make before the system is locked. This means the attacker cannot try many possible passwords. The disadvantage is that a malicious user could perform a denial of service attack on the system: make many incorrect password attempts on the accounts of other users, so that the other (normal) users are locked from their account.*

- *Introduce a delay between each password attempt. This means it will take longer for an attacker to try many passwords. For example on a computer system the attacker may normally automate the password attempts at a rate of 1000 per second. To try a dictionary of 200,000 passwords would take 200 seconds (about 3 minutes). However if the system introduces a delay of 1 second between each attempt, then the attacker can only make attempts at 1 per second. To try the dictionary would now take 55 hours. The disadvantage of this is that it may be inconvenient for the normal user when they accidentally enter the wrong password—they have to wait some time before trying again.*

- *Log and monitor all password attempts. This means if an attacker is making attempts a user or system administrator will know about the incorrect attempts and can later either attempt to find the attacker or at least warn the user to use a secure password. The disadvantage of this is that it doesn't prevent attacks, only detects them (i.e. an attack is still possible).*

Question 2 [2 marks]

What is the entropy of my [10 | 8 | 10 | 8] character password, which was randomly chosen from the set of [uppercase and lowercase English letters | uppercase English letters and numbers | lowercase English characters, the space character and the underscore character | uppercase and lowercase English letters and numbers]?

Answer. *The entropy of a random password is the number of bits that would be needed to represent that password. It can be calculated as:*

$$h = n \times \log_2(s)$$

where there are n characters chosen from a set with a maximum of s characters. (a) There are 52 uppercase and lowercase English letters giving an entropy of $10 \times \log_2(52) \approx 57$*. (b) There are 36 uppercase letters and numbers, entropy is* $8 \times \log_2(36) \approx 41$*. (c) There are 28 letters including space and underscore, entropy is* $10 \times \log_2(52) \approx 48$*. (d) There are 62 letters and numbers, entropy* $8 \times \log_2(62) \approx 47$*.*

Question 3 [5 marks]

A company has developed a new protocol, called *BAHTP*, that is used by a client application on computers in shops around Bangkok to send sales information to a central server in the company main office in Rangsit. The protocol uses TCP/IP. Based on your expert knowledge of OpenSSL libraries, you have been hired by the company to modify the client/server applications so that all communications between them are secure.

(a) Draw a protocol stack of a computer using Ethernet physical and data link layers, that illustrates the protocols in use by the secure client application. [2 marks]

Answer.

BAHTP

SSL/TLS

TCP

IP

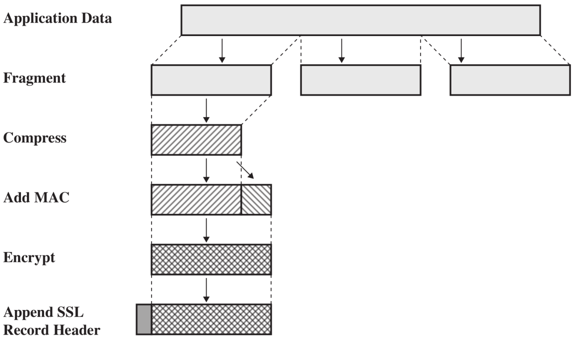
Ethernet DLL

Ethernet PHY

When using the secure application, a secure session and connection has been established. The following information is stored by the client computer for this session/connection (also shown below is the general operation of SSL record protocol):

(b) Write an equation that expresses the SSL record operation on a single fragment, F from the client application that produces the packet to be sent P. Use the variables above and || for the concatenate/append operator. For function names you *must* use the algorithm names (i.e. you cannot use E() for encrypt, H() for hash; refer to specific algorithms). Denote the SSL header as SSL. [3 marks]

- Session ID: id
- Compression method: null
- CipherSuite: [TLS_RSA_WITH_RC4_128_MD5 | TLS_DH_RSA_WITH_DES_CBC_SHA | TLS_DHE_DSS_WITH_AES_256_CBC_SHA | TLS_RSA_WITH_AES_256_CBC_SHA256]
- Master secret: s
- Server random: r_s
- Client random: r_c
- Server MAC secret: m_s
- Client MAC secret: m_c
- Server encrypt key: e_s
- Client encrypt key: e_c



Answer.

i.

$$P = SSL||\text{RC4\_128}(e_c, F||\text{HMACMD5}(m_c, F))$$

ii.

$$P = SSL||\text{DES\_CBC}(e_c, F||\text{HMACSHA}(m_c, F))$$

iii.

$$P = SSL||\text{AES\_256\_CBC}(e_c, F||\text{HMACSHA}(m_c, F))$$

iv.

$$P = SSL||\text{AES\_256\_CBC}(e_c, F||\text{HMACSHA256}(m_c, F))$$