NB Refer to lecture handouts for diagrams for DES and Needham-Schroeder.

E4.44 Network Security Specimen Exam Paper 1 - SPRING 2004

Answer 4 questions

Time allowed: 3 hours

1. (i) Fig 1.1 shows the round structure for DES encryption. Explain how decryption can be achieved with this structure.

   (ii) Fig 1.2 shows how the per round keys are generated in DES. What is meant by weak keys and identify the four such weak keys. What impact does use of a weak key have on DES

   (iii) What is meant by an exhaustive key search? How many keys should be investigated to find a particular key used in DES?

   (iv) Explain how the security of DES may be increased by the use of 3DES. By how much does 3DES improve the strength of DES?

   (v) In the IDEA algorithm addition is performed modulo 2^{16} and multiplication is performed mod $2^{16}+1$. Given that these operations transform a 16-bit message segment into another 16-bit message segment though the application of a 16-bit key explain how these operations can be reversed.
   In order to create a new algorithm with the same structure as IDEA but with simpler operations using 8-bit numbers it is proposed to perform addition modulo 2^8 and multiplication modulo 2^8+1 . Discuss whether these operations would be reversible.

2. (i) Show that for two prime numbers p and q and n = p.q, ϕ(n) = (p-1).(q-1).

   (ii) In RSA explain why the message to be encrypted must be smaller than the public key modulus n. A small message less than a third of the length of the public key modulus n (in binary form) is encrypted in RSA using a public key exponent of 3. How can the ciphertext be deciphered without the use of the private key?

   (iii)Explain how the Diffie-Hellman key exchange can be used to establish a session key in secret key cryptography. Explain why a passive observer would be unable to establish the session key despite observing all communications.

   (iv) How can a bucket brigade attack be launched against a Diffie-hellman key exchange? Discuss one way in which protection against such an attack can be provided.

3 (i)You are provided with the following:

- an RSA facility complete with public/private key pair
- a CBC facility incorporating the IDEA block cipher
- a message digest facility employing the MD5 algorithm.

You are required to send a block of data of size 1 Mbyte through an insecure network to a recipient who knows the message digest you are using, your secret key in IDEA and your RSA public key. Explain how you would use your security facilities (each facility for one operation) to provide the security services of privacy, message integrity and source authentication.

(ii) How would you achieve the above if the RSA facility were not available? Discuss the relative security strengths of your solutions to (i) and (ii).

(iii) In order to reduce the computing power required for MD5 it is proposed to devise a new message digest function in which the message is first divided into 64-bit blocks. The odd numbered blocks (first, third, fifth etc) are added together modulo 2^{64} to provide the high order half of a 128-bit message digest. The even numbered blocks are added together in a similar fashion to form the low order half of the message digest. Discuss the security implications of using this message digest in your designs for (i) and (ii) above.

4 (i) Explain the terms "proof of submission" and "non-redudiation" in an electronic mail system. Explain the importance of non-repudiation in a system if e-commerce.

(ii) An attacker is intent on disrupting secure communications by inserting bogus packets (with correct TCP checksum) into the communications. Discuss how such an attack would succeed in systems protected by IPSec and SSL.

(iii) What is meant by "Endpoint Identifier Hiding"? Explain one method by which it may be provided.

(iv) What is meant by "Perfect Forward Secrecy"? Does Kerberos offer Perfect Forward Secrecy?

5. (i) What functions should be provided by a public key infrastructure? Is it possible to operate a public key security system without a public key infrastructure?

(ii) Discuss the following models of public key infrastructure citing practical examples which follow the model.

(a) anarchy

(b) oligarchy
(c) policy based certificate hierarchy

(iii) A particular PKI issues Certificate Revocation Lists whenever the number of revocations made since the last list was issued exceeds a pre-set figure. Discuss how such a system could be attacked.

6. (i) Figure 6.1 shows the Needham- Schroeder system of authentication. Explain the purpose of each of the five messages in the interaction. What are the functions of the numbers N_1, N_2, and N_3?

(ii) In Kerberos V4 a client and its server are connected to different KDCs. Explain the process by which the client authenticates itself to the server.

(iii) Explain how the process in (ii) differs in Kerberos V5. What are the other differences between Kerberos versions 4 and 5?

E.44 Network Security Specimen Exam Paper 1 Answers

1 (i) Reverse rounds and keys (i.e. replace round 1 with round 16 and key1 with key 1 and configure round structure for decryption)
(ii) The weak keys are such that all per round keys are the same. The 4 weak keys are as follows:
28 zeros followed by 28 ones
28 ones followed by 28 zeros
56 ones
56 zeros (in the above the parity bits have been ignored)
(iii) An exhaustive key search is a test using all possible keys. In a search of the DES key space a number of 2 raised to the power of 56 would be required.
(iv) 3DES is encryption with key 1 followed by decryption with key 2 followed by encryption with key 1. Since the effective key length is 112 bits the strength is increased by 2 raised to the power of 56.
(v) Addition is reversed by adding the 16-bit output with the additive inverse of the key used in the original operation. Similarly multiplication is reversed by multiplying the result of the original operation by the key's multiplicative inverse.
It is always possible to find the additive inverse. Since 257 is prime it will also be possible to find the multiplicative inverse. Both operations are reversible.

2 (i) There are pq – 1 positive integers less than pq. In order to find Euler's function for n we need to remove those which are relatively prime to n. There are q-1 multiples of p and p-1 multiples of q in thid category. Euler's function for pq is therefore
$pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1)$
(ii) The message must be smaller than n because the operations are taken mod n and a message longer than n could not be distinguished from its value mod n.
The message may be deciphered by finding the normal cube root.
(iii) Refer to lecture handout for an explanation of Diffie-Hellman. An observer cannot (i.e. operation is computationally infeasible) find a from g raised to the a mod p.
(iv) Refer to lecture handout for an explanation of the bucket brigade attack and possible methods of protection

3 (i) A possible approach would be to use MD5 to form a digest of the message. The digest should then be signed with the private key of RSA. The message and signature should then be encrypted with CBC/IDEA.
(ii) If the RSA facility were not available source authentication could be provided by forming a keyed has of the message using MD5 and the IDEA key. Encryption would follow as before. This would not provide non-repudiation and it would generally be . weaker than the (i) regarding authentication as the same key has been used for authentication as encryption.
(iv) The proposed message digest function is a poor function since it would be relatively simple to find many messages with the same digest. Thus if the signature or MAC is known for one message it would be possible to reuse this signature or MAC for a number of alternative messages.

4 (i) Proof of submission is proof that a message was submitted to the electronic mail system. Non-repudiation enables a recipient of a message to prove in a court of law that it was sent by a particular sender. Non-repudiation in e-commerce prevents

initiators of transactions later claiming that the recipient or some other party made the transaction in their name.

(ii) IPSec would reject the packets and would not pass them to TCP. In SSL such packets could cause the session to break.
(iii) Refer to lecture handout
(iv) Refer to lecture handout. Kerberos does not provide Perfect Forward Secrecy since it uses master keys which are long term secrets.

5 (i) Refer to lecture handouts. It is possible to operate a public key security system without a PKI but there would be little trust in the public keys used.
(ii) Refer to lecture notes for (a) PGP, (b) web browsers and (c) PEM
(iii) Since recipients of the CRL would not know exactly when the CRL would be issued they would not be alarmed if it were intercepted and removed.

6 (i) First message is a comms request with the nonce N1. The nonce is included to prevent replay by an attacker who has obtained an old key of B. KDC's reply in the second message includes the returned nonce and provides a ticket encrypted under B's master key. It also includes a session key for a and B to communicate securely. All thgis information is secured by encryption under A's master key. In the third message A asses the ticket to B so that B can find the session key. To check whether B has done this correctly A also issues a challenge in the form of a number N2 which is sent encrypted under the session key KAB. The fourth message confirms that B has found N2 (which it proves by returning N2 – 1 encrypted under the session key) and also sets A a challenge with the number N3 encrypted under the session key. In the final message A responds to the challenge by returning N3 – 1 encrypted under the session key.. To summarise the functions of the numbers used in the protocol, N1 is to prevent replay whilst N2 and N3 are challenges in an authentication protocol.

(ii) In V4 each KDC must be registerd as a principal with every other KDC. A client's home KDC arranges a secure session with another KDC which can then arrange a secure session with a server registered with it as a principal.

(iii) In V5 the KDC's do not need to be registered as principals with all other KDCs but may communicate through a hierarchy of KDCs. Refer to lecture handouts for other differences between V4 and V5.