Distributed Systems: Concepts and Design

Chapter 11 Exercise Solutions

11.1 Describe some of the physical security policies in your organization. Express them in terms that could be implemented in a computerized door locking system.

11.1 Ans.

For QMUL Computer Science Department (as in 2000):

- staff have access to all areas of the department except the offices of others, at all hours;
- students of the department have access to teaching laboratories and classrooms at all times except 0.00 to 0.400 and to other areas of the department, except private offices, during office hours;
- students of other departments taking courses in Computer Science have access to classrooms at all times and to teaching laboratories at designated times according tothe the courses taken;
- visitors have access to the Departmental Office during office hours;
- a master key holder has access to all offices.

Note:

– Access rights should be withdrawn when a user ceases to be a member of staff or a student.

– Changes in policy should be immediately effective.

11.2 Describe some of the ways in which conventional email is vulnerable to eavesdropping, masquerading, tampering, replay, denial of service. Suggest methods by which email could be protected against each of these forms of attack.

11.2 Ans.

Possible weaknesses for a typical mail system with SMTP delivery and client pickup from POP or IMAP mail host on a local network:

Weakness	*Types of attack*	*remedy*
Sender is unauthenticated.	Masquerading, denial of service.	End-to-end authentication with digital signatures (e.g. using PGP)
Message contents not authenticated.	Tampering, masquerading.	End-to-end authentication with digital signatures (e.g. using PGP).
Message contents in the clear.	Eavesdropping.	End-to-end encryption (e.g. using PGP).
Delivery and deletion from POP/IMAP server is authenticated only by a login with password.	Masquerading.	Kerberos or SSL authentication of clients.
Sender's clock is not guranteed.	False dating of messages.	Include time certificates from a trusted time service.

11.3 Initial exchanges of public keys are vulnerable to the man-in-the-middle attack. Describe as many defences against it as you can.

11.3 Ans.

1. Use a private channel for the delivery of initial keys, such as a CDROM delivered by hand or by some other rellable method.
2. Include the Domain Name in the certificate and deal only with the correct corresponding IP address.
3. If certificates are delivered through the network, validate them with a 'key fingerprint' – a character string that is derived from the key with a standard one-way function - that was delivered by a separate channel (e.g. on a business card).

11.4 PGP is often used to secure email communication. Describe the steps that a pair of users using PGP must take before they can exchange email messages with privacy and authnticity guarantees. What scope is there to make the preliminary negotiations invisible to the users? (The PGP negotiation is an instance of the hybrid scheme.)

11.4 Ans.

PGP is based on a hybrid protocol like those described on pages 264 and 281. Its primary use is for secure email communication. It provides digital signatures for the authentication of messages string encryption for their secrecy and integrity. The signatures are made using the SHA-1 algorithm to make a digest of the message and RSA or DSS for signing with the sender's private key.

The message is (optionally) encrypted with 3DES or IDEA, using a one-time session key generated by the sender, which is encrypted using RSA with the recipient's public key and sent with the message.

PGP is required to generate public/private key pairs for each user and the one-time session keys used to encrypt messages. Users' public/private keys should be changed from time-to-time. (No keys should be used indefinitely in a secure system because of the danger thst they may be compromised through inadvertent disclosure or as a result of an attack.) To achieve the rotation of public/private key pairs, PGP must generate and store multiple key pairs and give each pair a label or identifer.

Key management is based on a *key ring* held by each user and a collection of PGP key servers accessible on the Internet that hold only the public keys of registered PGP users. The key ring is simply a small database holding keys in data structures that are secure. They are secured using secret key encryption with a *pass phrase* that the use must type in order to allow applications to access the keys in the keyring.

If PGP is thoroughly integrated into an email or other application the necessary actions to generate keys, access the key ring and perform signing and encryption on email messages can all be triggered automatically. The only user action required is the input of the *pass phrase* to decrypt the keyring entries. If users are equipped with smart cards or other physical access keys, the pass phrase could be supplied from the card.

11.5 How could email be sent to a list of 100 recipients using PGP or a similar scheme? Suggest a scheme that is simpler and faster when the list is used frequently.

11.5 Ans.

The idea of this exercise is to contrast the need for PGP to encrypt the session key *n* times (once in the public key of each user) with a scheme where the members of a group would share a single session key. The management and renewal of the shared key can be more easily achieved if the mailing list members are represented as members of a multicast group (pp. 436 *et seq*.).

11.6 The implementation of the TEA symmetric encryption algorithm given in Figure 11.8–11.10 is not portable between all machine architectures. Explain why. How could a message encrypted using the TEA implementation be transmitted to decrypt it correctly on all other architectures?

11.6 Ans.

Byte ordering is an issue. The algorithm as presented assumes that the 4 bytes in a 32-bit word are ordered the same at the sender (encrypter) and the receiver (decrypter). To make it work for all architectures, we would need to transmit messages in a network-standard byte order, and to re-order the bytes to suite the local architecture on receipt.

11.7 Modify the TEA application program in Figure 11.9 to use cipher block chaining (CBC).

11.7 Ans.

Left for the reader.

11.8 Construct a stream cipher application based on the program in Figure 11.9.

11.8 Ans.

Left for the reader.

11.9 Estimate the time required to crack a 56-bit DES key by a brute-force attack using a 500 MIPS (million instruction per second) workstation, assuming that the inner loop for a brute-force attack program involves around 10 instructions per key value, plus the time to encrypt an 8-byte plaintext (see Figure 11.13. Perform the same calculation for a 128-bit IDEA key. Extrapolate your calculations to obtain the time for a 50,000 MIPS parallel processor (or an Internet consortium with similar processing power).

11.9 Ans.

Suppose we have a computer with a 64-bit, 2000 MIP cpu, and a short sample (8 bytes or one 64-bit word) of plain text with the corresponding encrypted text. A program can be constructed with an inner loop of N instructions, to generate all possible key values in the range $0 - (2^{56} - 1)$ and apply the an encryption algorithm to the plain text with each key value in turn. If it takes T_{enc} seconds to apply the encryption algorithm to an 8-byte plain text, then we have the following estimate of the average time t to crack a key of length L by brute force:

$$t = \frac{2^L}{2}(N/(2000 \times 10^6) + T_{enc}) \text{seconds}$$

If N= 10 (i.e. we require an inner loop of 10 instructions) and T_{enc} = 8/(18.963 x 10^6) seconds for the DES algorithm (i.e. the fastest time to encrypt 8 bytes given in Figure 7.13), we have:

$$t = 2^{55}(10/(2000 \cdot 10^6) + 8/(18.963 \cdot 10^6)) \approx 1.78 \times 10^8 \text{ seconds}$$

i.e. about 500 years. A 200,000 MIPs parallel processor is 100 times faster, so assuming an efficient parallel algorithm, the cracking time would be ~5 years.

For IDEA, the equation is:

$$t = 2^{128}(10/(2000 \cdot 10^6) + 8/(18.963 \cdot 10^6)) \approx 1.5 \times 10^{32} \text{ seconds}$$

or about 5 x 10^{24} years!

11.10 In the Needham and Shroeder authentication protocol with secret keys, explain why the following version of message 5 is not secure:

$$A \rightarrow B: \quad \{N_B\}_{K_{AB}}$$

11.10 Ans.

The purpose of message 5 is for A to convince B that K_{AB} is fresh. B will be convinced if it knows that A has K_{AB} (because it will know that A cannot be merely re-playing overheard messages). The suggested version of message 5 is not secure because A would not need to know K_{AB} in order to send it, it could be sent by copying message 4.

11.11 Review the solutions proposed in the discussion of the 802.11 Wireless Equivalent Privacy protocol design, outlining ways in which each solution could be implemented and discussing any unresolved issues or drawbacks. (5 answers)

*11.11 Ans.*i) Sharing a single key:

Solution, use a public-key based protocol for negotiating individual keys.

How would authorized users establish their credentials? They would need a certificate signed by an authority such as the administrator of the network. As a simple (primitive) solution could get the certificate using a physical channel (e.g. on a memory stick from the sys admin). But a more sophisticated scheme would have the sys admin establish a database contianing a set of certificates for authorized users. The users would establish their identities using public key certificates in order to utilize their authorization. Once the authorization has occured, the protocol to establish a shared encryption key would proceed in a manner similar to (or even using) SSL/TSL.

*11.11 Ans.*ii) Base stations are never authenticated:
Solution, base stations should supply a certificate.

The certificate could be supplied as part of the exchange that is described above. Care is needed to ensure that the public key in the base-station certificate is used to establish the shared key.

11.11 Ans. iii) Inappropriate use of a stream cipher:
Solution: Negotiate a new key after a time less than the worst case for repetition. An explicit termination code would be needed, as is the case in TLS.

The worst case for repetition is in the order of hours. A base station should initiate the negotiation of new keys without disruption of communication using a protocol similar to the TLS *change cipher spec* mechanism. Drawbacks: the TLS mechanism must be implemented everywhere. It may not be possible to perform a cipher change without interruping a real-time datastream.

11.11 Ans. iv) The RC4 stream cipher weakness
Solution: Provision for the negotiation of cipher specifications

the main problem is the inflexibility of hardwiring the cipher spec into the protocol definition. Solution is to allow communication partners to negotiate a cipher algorithm as in TLS. This requires a handshake protocol, similar to the *change cipher spec* mechanism required in the previous answer.

11.11 Ans. v) Users often didn't deploy the protection
Solution: Better default settings and documentation.

The issue here is the importance given to security by administrators and users. It's worth noting that the failure to do so has resulted in several recorded incidents of loss of privacy and some decisions to suspend the use of WiFi networks.
