In particular, `AuditPolicy` allows administrators to determine the channel used for logging security event occurrences. `AuditPolicy` further defines op `set_ audit_selectors`, which can be used to determine the types of eve which an entry should be written into the audit channel. For example, by passin including event types `AuditPrincipalAuth` and `AuditSessionAuth` only a tication events will be logged. Finally, the `selectors` parameter allows administra determine which auditing information is to be written for each event.

Summary

In this section, we have seen an example of how object-oriented middleware su the higher-level security concepts that we have introduced in previous sections. W discussed how the CORBA Security service supports authentication, access contro repudiation and auditing. As with other CORBA services, the security service stand the interface of objects that are needed for security management purposes. We ha that client programmers, server programmers and administrators need different in for controlling the security of a distributed object-based system.

Key Points

- Distributed objects have to rely on networks to be able to communicate wi other. The message traffic on these networks can be eavesdropped tampered with by non-authorized third parties. The construction of trus distributed object systems therefore demands that message traffic is secured such attacks and that infiltration of distributed object systems by atta prevented.
- Encryption techniques are used to prevent eavesdropping and message tam Public or secret key methods are used to encrypt a marshalled object reques it is transmitted using an insecure network.
- The distribution of public or secret keys is achieved by a trusted key distr service which implements a key distribution protocol. The Needham/Sc protocol is such a protocol.
- Encryption is also used for authentication. Authentication establishes the that principals are who they claim to be. It can be achieved by demonstrat the principal possesses a key, which can then be seen as evidence that the is authorized to perform certain operations.
- Access control is based on authentication. Middleware associate credenti principals during authentication. These credentials determine the rights leges that have been granted to the principal to use the distributed object Administrators then assign the required rights to operations of objects o types and the access control of the middleware ensures that only those p who possess sufficient access rights can execute these operations.
- Non-repudiation is concerned with the generation of irrefutable evide principals have requested certain operations or that servers have receiv

requests. Non-repudiation thus makes principals accountable for their activities within the distributed object system.

- Auditing is a passive security mechanism that enables administrators to identify security incidents. Auditing policies determine the events and the details that have to be recorded for these events so that they can be viewed or analyzed by security administrators.

Self Assessment

12.1 Why are distributed systems inherently insecure?
12.2 What are the security threats to which distributed systems are exposed?
12.3 What are the principle methods of attacking a distributed system?
12.4 How can distributed systems be infiltrated?
12.5 What role does encryption play in securing distributed systems?
12.6 What is the difference between secret key and public key encryption?
12.7 What is a key?
12.8 How are keys distributed?
12.9 Why is the Needham/Schroeder protocol for public keys more complicated than the one for secret keys?
12.10 Why are nonces used in the Needham/Schroeder protocol?
12.11 What is authentication?
12.12 How are credentials managed in object-oriented systems?
12.13 What is the relationship between authentication and access control?
12.14 Why is non-repudiation important for electronic commerce?
12.15 Why does non-repudiation hand out tokens for evidence rather than handing out the signed evidence?
12.16 What is the difference between auditing and the other distributed system security mechanisms?
12.17 How is eavesdropping and message tampering prevented in CORBA-based systems?

Further Reading

[Colouris et al., 1994] includes a chapter on the security of general distributed systems. This chapter covers encryption and key distribution in greater depth than we did, but it does not address all of the higher levels of security that are currently supported by object-oriented middleware.

[Garfinkel and Spafford, 1996] is a good professional book on UNIX and Internet security. It provides a good introduction to operating system and network security for the beginner and reviews security from the user and administrator points of view. Its discussions on RPC and Kerberos are also somewhat relevant to security of distributed object systems.

Various encryption techniques have been proposed. The Distributed Encryption Standard (DES) was among the first and originated at IBM in 1977. It was then promoted to a US ANSI standard. DES is based on secret key encryption technology. Phil Zimmermann has gained quite some attention with his public-key-based Pretty Good

Privacy (PGP) [Zimmermann, 1995] due to a legal battle he had to fight with the US government. PGP uses strong 128-bit public key encryption and enables the creation of cypher text that even the most powerful computers of the National Security Agency (NSA) cannot break. When Zimmermann made PGP publicly available under the Gnu License Agreement this was considered by the US Government an illegal export of weapon technology. The US government, however, recently dropped the charges against Zimmermann. SSL was initially used to secure the transport between data entered into a HTML form and a web server where the data is processed by a server script or program. SSL is now also used with object-oriented middleware to secure the data transfer.

The CORBA Security specification of the OMG is defined in Chapter 15 of the CORBAservices specification [Object Management Group, 1996]. It is the result of merging three specifications: the CORBA Security service, revision 1; the Common Secure Interoperability specification; and the CORBAsecurity/SSL interoperability specification. These three specifications are all available from the OMG ftp server `ftp.omg.org`.

[Needham and Schroeder, 1978] first published the Needham/Schroeder protocol. It is used in MIT's Kerberos system [Neumann and Tso, 1994]. Kerberos, in turn, is the basis for key distribution and access control in systems based on remote procedure calls that follow the OSF/DCE standard, upon which Microsoft's COM is based. Microsoft's COM supports authentication, access control and auditing in very much the same way as CORBA. A reasonable introduction to COM Security is provided in Chapter 7 of [Grimes, 1997].