DR. ROLF OPPLIGER
UNIVERSITY OF BERNE
INST. FOR COMP. SCIENCE AND APPLIED MATHEMATICS
SWITZERLAND

SECURITY CONCEPTS FOR CORPORATE NETWORKS *F4*

SECURITY CONCEPTS FOR CORPORATE NETWORKS

Rolf Oppliger
Dieter Hogrefe

University of Berne
Institute for Computer Science and Applied Mathematics
Länggassstrasse 51
CH-3012 Berne, Switzerland

Tel. +41 31 631 49 03
Fax. +41 31 631 39 65
Internet: {oppliger,hogrefe}@iam.unibe.ch

CR Category and Subject Descriptor: C.2.0 [Computer Systems Organization]: Computer-Communication Networks — general; K.6.5 [Computing Milieux] Management of Computing and Information Systems — security and protection

General Terms: Management, Security, Standardization

Additional Key Words: Corporate Network, OSI, Security Architecture

Abstract

The current, widespread use of computer networks has led to increased concerns about security. This paper deals with network security in general, and concentrates on corporate networks in particular. A method to develop security concepts for corporate networks is introduced, and stepwise refined.

1 Introduction

It is assumed that the reader of this paper is familiar with the fundamentals of computer networks, open systems, and OSI networks. A computer network consists of interconnected computer systems that can either be closed or open. Closed systems are proprietary, usually being able to communicate only with systems of the same manufacturer. In using standardized protocols to provide standardized services, open systems are free to communicate with other open systems, forming an OSI network (Open Systems Interconnection). OSI standards are being developed by the Joint Technical Committee 1 (JTC1) of the International Standards Organization (ISO), and the International Electrotechnical Commission (IEC).

Corporate networks use public services to interconnect geographically distributed local area networks and private branch exchanges. Public services are offered in wide area networks; examples are leased lines, circuit switched lines, and services that are provided in packet switched data networks [OS94].

A security concept is needed to make a corporate network comparably secure [Opp92, OH92, OH93]. A method to develop security concepts for corporate networks is introduced in this paper. It is organized as follows: Possible attacks are outlined in section two. The method is shortly described in section three, and stepwise refined in sections four and five. Conclusions are drawn in section six.

2 Attacks

Attacks threaten the security (confidentiality, integrity, and availability) of corporate networks, and data that are stored or transmitted within. There are passive and active attacks to be distinguished:

- The confidentiality of data is threatened by passive attacks. The situation is shown in figure 1. The data traffic between the sender and the receiver is observed by the intruder. It has to be distinguished, whether the intruder is able to interpret the data, or not.
  - In a passive wiretapping attack the intruder is able to interpret the data, and to understand its information accordingly.
  - In a traffic analysis attack the intruder is not able to interpret the data. He can only learn from the origins, destinations, frequencies and sizes of messages or data units. The fact that two entities are communicating may already be compromising in itself; this may be true for stock-brokers and military commanders.

  The feasibility of passive attacks primarily depends on the physical transmission media in use. Radio and satellite links are very easy to intercept, whereas

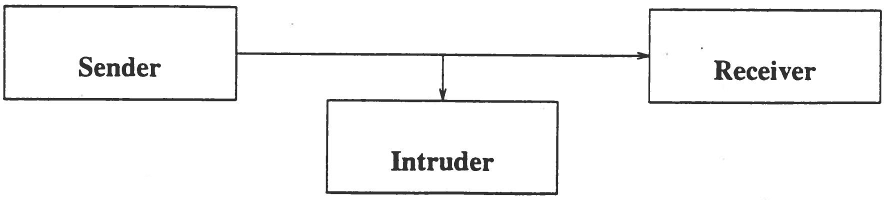

Figure 1: Passive attack

metallic conductors, like twisted pairs or coaxial cables, can only be tapped if they are physically accessible by the intruder. The tapping of light wave conductors is even more difficult.

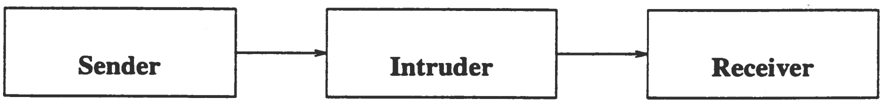

Figure 2: Active attack

- The integrity or availability of data in transmission is threatened by active attacks. The situation is shown in figure 2. The data traffic between the sender and the receiver is fully controlled by the intruder. He can modify, extend, delay, destroy, copy, or reply messages or single data units. He can also flood the receiver. Provided with the authentication information of some legitimate user, he can masquerade, and pretend to be someone else. If passwords are used for authentication purposes, and if these passwords are transmitted within the network, the intruder can catch them with a passive wiretapping attack. As a matter of fact, the transmission of passwords is a major vulnerability of most computer networks that are in use today.

Natural disasters, like lightnings, fires, floods, or earthquakes, threaten the safety of corporate networks. Because they can be controlled by architectural and organizational counter-measures to a certain degree, they are not subject to this paper.

A corporate network is said to be secure, if it is able to prevent from passive and active attacks. This goal is hard to reach, not only because of the huge size of a corporate network, but also because of its heterogenity; there may be various computer systems from different manufacturers, possibly running different operating systems, communication and application software, interconnected to one corporate network. Gateways may exist to public networks and other corporate networks.

A corporate network provider has to develop different security concepts for the network. The choice of an appropriate conecpt is left to the top management; it has to take the responsibility. A method is needed to develop different security concepts; a possibility is introduced in the next section.

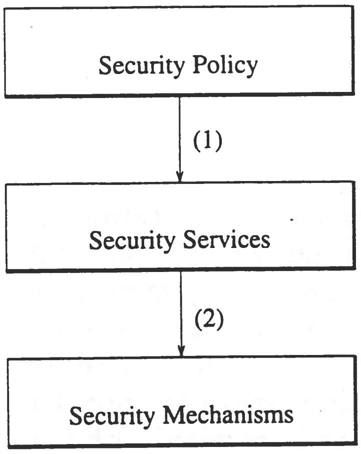

Figure 3: Security Concept

3 Method

A method to develop different security concepts for a corporate network can be based on a layered approach (compare figure 3). On the top level, there is a security policy to be defined for every security concept. Based on this security policy, and knowing the actual situation, and the possible forms of attack, a set of security services has to be derived. This step is indicated with (1) in figure 3. Possible scurity services are authentication, confidentiality, integrity, non-repudiation, and access control services.

Security mechanisms have to be studied or developped for every security service that is required for a policy. This step is indicated with (2) in figure 3. Security mechanisms need to be simple, cost-efficient, and secure. As a matter of fact, they have to be exchangeable; whenever better mechanisms are found or developped, they must be replaced.

Security services and mechanisms are discussed in the following sections. The terminology of the OSI security architecture [ISO89] is needed for this discussion. The use of this terminology doesn't imply that the method can only be applied to corporate networks that follow OSI standards; other security services and mechanisms can be used in addition or instead.

4 Security Services

The OSI security architecture enumerates five calsses of security services:

1. Authentication services
2. Data confidentiality services

3. Data integrity services
4. Non-repudiation services
5. Access control services

Authentication services are to verify the identities of entities, peer-entities, or data origins. Data confidentiality and data integrity services are to protect the confidentiality and integrity of data in transmission; they prevent from passive and active attacks. There are connection and connectionless data confidentiality and integrity services. Protection can be restricted to some particular fields within the data units, too. There is a traffic flow confidentiality service to prevent from traffic analysis attacks. Connection integrity services can be provided with or without recovery. In some cases it might be vital for the receiver (sender) to prove that data were sent (received) by the stated originator (intended receiver); non-repudiation services can be used therefore. Finally, there are access control services to prevent entities from accessing and using OSI resources in an unauthorized way.

Authentication, data confidentiality, and data integrity services represent orthogonal security functions, wheras non-repudiation is a stronger version of authentication. Access control services are not much related to the other security services.

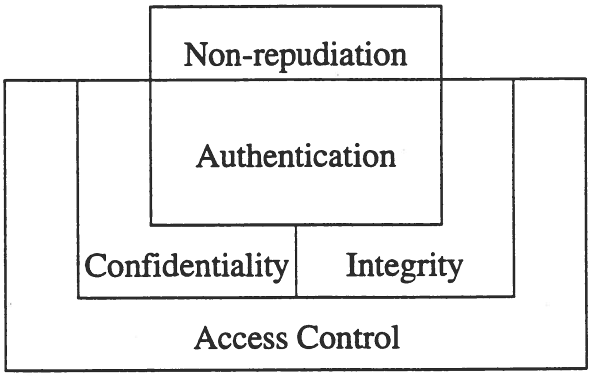

Figure 4: Security Services

Figure 4 illustrates the five classes of OSI security services. Authentication services are fundamental. Although confidentiality, integrity, and non-repudiation services are based on authentication services, they can be offered independantly from each another, in order to extend the overall level of security. Access control services can be left to application processes; they needn't be offered in corporate networks.

5 Security Mechanisms

Security mechanisms are used to provide security services. There are eight classes of security mechanisms enumerated within the OSI security architecture.

1. Encipherment is a fundamental security mechanism. It is used to provide most of the security services (alone or together with other mechanisms). Within a cryptosystem a plaintext message is transformed to a ciphertext, using a certain key. It has to be distinguished, whether the sender and the receiver are using the same key (secret key cryptosystem, SKC), or not (public key cryptosystem, PKC). Within a PKC each user holds a pair of keys, consisting of a public key and a private key. The public key can be given to anyone, whereas the private key must be kept secret [DH76].

   With regard to OSI, it has to be distinguished, whether encipherment is being done in layer one or two (link encryption), or in a higher layer, typically the presentation or application layer (end-to-end encryption). With link encryption every trunk can use its own cryptosystem. One drawback of link encryption is based on the fact that all data units have to be decrypted within the relay stations: If these stations can't be trusted, the data units can be compromised here. This is not true for end-to-end encryption. The problem of end-to-end encryption is based on the fact that some basic routing information can't be encrypted here, enabling traffic analysis attacks.

2. Digital signatures provide an equivalent for hand-written signatures; only one person is able to sign, but everybody else can verify the correctness of the signature. A simple digital signature scheme can be constructed within a PKC: The sender encrypts the message using his private key. Everybody knows the corresponding public key and can decrypt the message, authenticating automatically the sender. For long messages it is common to hash the message first, sign the result digitally, and send the message together with the digitally signed hash function result to the receiver. The National Institute of Standards and Technology (NIST) has published a Digital Signature Standard (DSS) back in 1991 [NIS91]. The discussion about this standard is not yet closed [RHA92].

3. If the confidentiality of a message is protected through encipherment, its integrity is protected, too. But there are situations that require the unique protection of integrity. In these situations the use of encipherment is too expensive, and data integrity mechanisms are sufficient enough. In data transmission the integrity of data units is protected through checksums. To prevent active attacks, these checksums must be protected, too. Cryptologically protected checksums are further referred to as message authentication codes (MACs). MACs protect the integrity of data units, they don't protect the integrity of data streams. Sequence numbers, and cryptological chaining can be used here.

4. Authentication exchange mechanisms are to provide entity authentication services. There are simple and strong authentication exchange mechanisms to be distinguished [ITU87]: Simple mechanisms depend on the transmission of some authentication information of a particular users, wheras strong mecha-

nisms are using cryptological protocols to hide this information. The transmission of a password is a typical, and commonly used simple authentication exchange mechanism, whereas challenge-response systems and zero-knowledge interactive proof systems are used for strong authentication.

5. In establishing a constant data flow between communicating entities, traffic padding mechanisms are to prevent from traffic analysis attacks. The aim is to make it impossible for an intruder to distinguish data that carry information from data that don't carry information.

6. Routing control mechanisms are to avoid vulnerable links from being used for data transmission. A network with alternative routes is required here, one of which is comparably safe.

7. The security of security mechanisms sometimes depend on the public availability of certain parameters, like public keys in a PKC. Notarization implies that these parameters can be certified and published by a trusted certification authority. ITU-T X.509 describes a hierarchical layering of certification authorities [ITU87].

8. Access control mechanisms have to make sure that users can only access resources in a correct and predefined way. Discretionary and mandatory access controls are used in closed systems. They are not suitable in open systems; discretionary access controls because of a missing limitation of subject and object sets, and mandatory access controls because of possible incompatibilities among the security labels.

The OSI security architecture has been extended by a multi-part standard, known as open system security frameworks. Each security framework addresses, at a general level, one specific topic. A working group of JTC1 is dealing with management aspects of OSI security, too.

6 Conclusions

A method to develop security concepts for corporate networks is outlined in this paper. The method follows a layered approach: On the top level there has a policy to be defined for every security concept. Based on this policy, different security services and corresponding mechanisms can be evaluated.

Authentication services are fundamental for any network; if authentication is not given, the discussion of further security services is useless. A lot of research is actually being done in developping authentication and key distribution systems. Examples are Kerberos from MIT [SNS88], NetSP (former KryptoKnight) from IBM [MTVHZ92], SPX from DEC [TA91], and TESS from the European Institute for System Security (E.I.S.S.) [Bet91]. A Kerberos-like authentication system has been chosen by the Open Software Foundation (OSF) for its Distributed Computing Environment (DCE).

Based on the key distribution functionality of an authentication system, data confidentiality, integrity, and non-repuiation services can be added straightforward.

With regard to a corporate network that is actually being built for the Swiss federal administration authorities, the authentication and key distribution systems that are available today are being considered and evaluated by the Institute for Computer Science and Applied Mathematics (IAM) of the University of Berne, and the information security section of the Swiss Federal Office of Information Technology and Systems (BFI).

Acknowledgement

The authors would like to express their thanks to Mr. P. Trachsel and Mr. M. Frauenknecht from the Swiss Federal Office of Information Technology and Systems (BFI) for their support and encouragement.

References

[Bet91] T. Beth. TESS — The Exponential Security System. Report 91/13, Europäisches Institut für Systemsicherheit (E.I.S.S), Universität Karlsruhe, Am Fasanengarten 5, D-76128 Karlsruhe, 1991.

[DH76] W. Diffie and M.E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644 - 654, 1976.

[ISO89] ISO/IEC. Information Processing Systems — Open Systems Interconnection Reference Model — Part 2: Security Architecture. ISO/IEC 7498-2, 1989.

[ITU87] ITU. The Directory — Authentication Framework. Recommendation X.509, November 1987.

[MTVHZ92] R. Molva, G. Tsudik, E. Van Herreweghen, and S. Zatti. KryptoKnight Authentication and Key Distribution System. In Y. Deswarte, G. Eizenberg, and J.J. Quisquater, editors, *Computer Security — ESORICS '92* , pages 155 – 174. Springer-Verlag, 1992. 2nd European Symposium on Research in Computer Security.

[NIS91] NIST. A proposed Federal Information Processing Standard for Digital Signature Standard (DSS). Draft Technical Report FIPS PUB XX, Gaithersburg, MD, August 1991.

[OH92] R. Oppliger and D. Hogrefe. Sicherheit in unternehmensweiten Kommunikationsnetzen (CCN). *Praxis der Informationsverarbeitung und Kommunikation*, 15(4):213 – 217, 1992.

[OH93] R. Oppliger and D. Hogrefe. Corporate Network Security. In *Proceedings of the IEEE Singapore International Conference on Networks and International Conference on Information Engineering (SICON/ICIE '93)*, pages 426 – 430, 1993.

[Opp92] R. Oppliger. *Computersicherheit.* Vieweg-Verlag, 1992.

[OS94] R. Oppliger and P.J. Stüssi. *Unternehmensweite Kommunikationsnetze.* Vieweg-Verlag, 1994.

[RHA92] R.L. Rivest, M.E. Hellman, and J.C. Anderson. Debating Encryption Standards. *Communications of the ACM*, 35(7):32 – 54, 1992.

[SNS88] J. Steiner, C. Neuman, and J. Schiller. Kerberos: An Authentication Service for Open Network Systems. Technical report, Massachusetts Institute of Technology, Laboratory for Computer Science, Cambridge, Massachusetts, 1988.

[TA91] J.J. Tardo and K. Alagappan. SPX: Global Authentification Using Public Key Certificates. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 232 – 244, Los Alamitos, California, 1991. IEEE Computer Society Press.