CORPORATE NETWORK SECURITY

R. Oppliger, D. Hogrefe

Institute for Computer Science, University of Berne, Switzerland

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. Passive and active attacks are outlined in section one. Counter-measures to prevent corporate networks from being attacked are discussed in section two. The security architecture for OSI networks is introduced in section three. This architecture might be of interest for corporate networks, too. Conclusions are drawn in section four.

Introduction

It is assumed that the reader of this paper is familiar with computer networks, open systems and OSI networks. Computer network is a generic term for any kind of interconnected computer systems. These systems can be closed or open. Closed systems are proprietary, usually being able to communicate only with other 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).

Computer security is to protect resources within a computer system from losses of confidentiality, integrity or availability [1]. Within a network, communication security has to complement computer security; it is necessary to prevent data in transmission from being attacked passively or actively.

Passive Attacks:

The confidentiality of data in transmission is threatened by a passive attack. This 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 in transmission, or not:

In a passive wiretapping attack the intruder is able to interpret the data, and to understand its information accordingly.

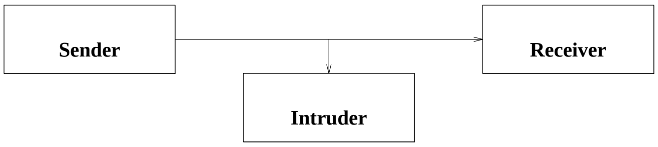

Figure 1: Passive attack

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 the data in transmission. The fact that two entities are communicating may already be compromising in itself. This can be true for stock-brokers or 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 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 much more difficult.

Active Attacks:

The integrity or availability of data in transmission is threatened by an active attack. This 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 single data units or parts of the data stream.

Figure 2: Active attack

Provided with the authentication information of some legitimate user, he can even 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 get them during a passive wiretapping attack. It doesn't matter, whether the passwords are encrypted or not; the intruder can reply the passwords in both cases. As a matter of fact, the transmission of passwords is a major vulnerability of most computer networks today.

Natural disasters, like lightnings, floods or earthquakes, threaten the availability of information that is stored within computer systems. Because these threats can be controlled by architectural and organizational counter-measures to a certain degree, they are not subject to this paper.

Passive attacks are hard to detect but can easily be prevented, whereas active attacks are easy to detect but hard to prevent.

Corporate Networks

Corporate networks (CN) are to satisfy corporate communication needs of companies or families of companies [2, 3]. These needs exist in the local, and in the wide area domain. In most European countries private networks can only be provided in the local domain, whereas communication in the wide area domain has to make use of services that are provided in public networks [4, 5]. These services are further referred to as public services.

To satisfy its communication needs, a company can either use public services to build a CN of its own, or it can outsource telecommunication and subscribe a so-called managed network service (MNS). MNS are provided by large companies within their networks for financial or marketing reasons. Security aspects of public services and MNS are discussed next [6].

Public Services:

There are three types of public services that have to be taken into consideration when building a CN. These are leased lines, circuit switched lines and services that are provided within packet switched data networks.

Leased Lines: As a matter of fact, leased lines that are based on metallic conductors can be attacked passively. Encipherment and traffic padding mechanisms can be used to prevent from passive wiretapping and traffic analysis attacks.

Encipherment is being used to hide the information of data in transmission. Within a cryptosystem a plaintext message is transformed into 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 but the private key must be kept secret [7]. In some countries the use of encipherment is mandatory for the transmission of sensitive data, like tax or medical records. Where international interoperability is required, the choice of an appropriate cryptosystem can also be constrained by some import or export restrictions.

Traffic padding mechanisms are to establish a constant data flow between two entities. The aim is to make it impossible for an intruder to distinguish meaningful from meaningless data.

The flexibility in use, the possibility of linking international leased lines together, and the high degree in security have intensified the role of leased lines in corporate networking within the last decade.

Circuit Switched Lines: Encipherment and traffic padding mechanisms can be used to prevent circuit switched lines from being attacked passively, too. But in the contrary to leased lines, circuit switched lines can also be the target to an active attack. One reason for this is the fact that lines are switched without any authentication being done. This missing authentication in circuit switched networks is further referred to as authentication problem. How can a called entity be sure that the calling entity is the one, it claims to be?

The authentication problem has to be looked at separately for the public switched telephone network (PSTN) and the integrated services digital network (ISDN).

The original aim of the PSTN has been the transmission of analog voice signals between human beings. There is no authentication problem for this kind of interpersonal communication. Human beings can identify and authenticate each another through mutually introduction, voice recognition, and specific knowledge. Computer systems can't do so. Hackers have been successfully using this inability to access extraneous computer systems and networks for years. Silent modems and automatic call-back systems can be used to better control access from extraneous PSTN users.

Another vulnerability is based on the fact that the PSTN uses only one channel for signaling and data transmission. Hackers have found possibilities to mislead the clearing systems of the PSTN providers, and to use it for free or at the cost of others. The standardized common signaling system No. 7 (CSS7) will separate the signaling channel from the data transmission channel and render more difficult this kind of attacks.

The CSS7 will not be fully integrated until the ISDN. The ISDN offers two additional features to control the authentication problem: The automatic number identification and the closed user group.

The fact that ISDN services are still provided within the PSTN today is often forgotten, when people talk about the ISDN, and it's security from being attacked passively. The ISDN today is as easy to wiretap as the PSTN. This will only change with an end-to-end use of light wave conductors within the Broadband-ISDN (B-ISDN).

The use of services that are provided within circuit switched networks is always dangerous for a CN. Anybody who has physical access to the network can try to access the CN, too. Access control can only be done on a logical level.

Packet Switched Data Networks: The CCITT recommendations of the X.25 series are the international standard protocols for accessing packet switched data networks. These networks are further referred to as X.25 networks. X.25 services are provided within X.25 networks. There are connectionless and connection-oriented X.25 services. Virtual circuits are established in the connection-oriented case. They can be switched (SVC) or permanent (PVC). PVC resemble leased lines and can be secured accordingly, whereas SVC resemble circuit switched lines and know the same vulnerabilities.

An intruder, who is willing to attack passively a X.25 network, has to overcome an additional obstacle in the connectionless case. This obstacle is based on the fact that messages are divided up into datagrams, which are routed individually through the X.25 network. An intruder who wants to get a particular message must be able to wiretap all possible routes between the sender and the receiver. This is possible but may be very expensive. Obviously, this obstacle doesn't exist for a connection-oriented X.25 service, where all packets are routed the same way.

A vulnerability of connection-oriented X.25 services is based on the fact that subscribers can be overflowed with long sequences of SVC request packets. Although no connection will be established, the attacked subscriber will eventually deny further service. This kind of overflowing attack can be controlled in a X.25 network by defining maximal numbers of SVC request packets that can be sent to subscribers.

Most X.25 networks support the blocking of incoming or outgoing calls, and the definition of closed user groups.

Managed Network Services:

MNS are provided within existing CN. As a matter of fact, MNS subscribers are restricted to the security mechanisms that are used within these CN. A short look at the contemporary situation reveals that access control mechanisms through passwords are the only security mechanisms that are used today. Other security mechanisms are still missing.

MNS subscribers must always take into consideration that the MNS provider can attack the data they transmit passively or actively. So the trustworthiness of the MNS provider is becoming a key factor and must be considered accordingly.

The situation is dangerous, if the MNS provider is serving different companies that are all competing in the same spheres of activity. The situation is even more dangerous, if the MNS provider himself is a competitor of a MNS subscriber in one particular sphere of activity.

OSI Security Architecture

OSI standards are being developed by the Joint Technical Committee 1 (JTC1) of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). An OSI security architecture has been published as part two of the OSI reference model in 1988 (ISO 7498-2).

Five Security services and eight security mechanisms are enumerated in ISO 7498-2 [8].

Security Services:

Authentication services: The identities of peer-entities and data origins have to be verified.

Access control services: Unauthorized entities have to be prevented from accessing and using OSI resources.

Data confidentiality services: The confidentiality of data in transmission has to be protected, and passive attacks must be prevented. A connectionless confidentiality service protects single data units. A selective field confidentiality service is restricted to some particular fields within these data units. A connection confidentiality service protects sequences of data units, whereas a traffic flow confidentiality service prevents from traffic analysis.

Data integrity services: The integrity of data in transmission has to be protected, and active attacks must be prevented. A connectionless integrity service protects the integrity of single data units, whereas a connection integrity service protects the integrity of sequences of data units. Modifications, insertions, deletions, and replays of data units are detected here. Connection integrity services can be provided with or without recovery. Both types of data integrity services can be restricted to some particular fields within data units. The corresponding security services are called selective field connectionless and selective field connection integrity service.

Non-repudiation services: In some cases it might be vital for the receiver to prove that data were sent by the stated originator even when the sender tries to deny it. A non-repudiation service with proof of origin is needed in this case. It may also be vital for the sender to prove that the transmitted data were indeed received by the intended receiver. This proof can be done by a non-repudiation service with proof of receipt. Both non-repudiation services are becoming very important for value-added services, like electronic mail (E-Mail) or electronic data interchange (EDI).

Security Mechanisms:

A security mechanism is a technique that can be used in order to provide a security service.

Encipherment: Encipherment is a fundamental security mechanism that is able to provide or support most security services. With regard to OSI, it has to be decided, 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. This gives an opportunity to the intruder to analyse the traffic.

Digital signature: Digital signature schemes are suitable for authentication, data integrity and non-repudiation services. 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 a 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, sign the result digitally, and send the message together with the digitally signed hash function result to the receiver. In 1991 the U.S. American National Institute of Standards and Technology (NIST) has published a controversial Digital Signature Standard (DSS) [9].

Access control: Access control mechanisms have to make sure that the users of an OSI network 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 in security labelling. New access control mechanisms are required for open systems. Missing possible alternatives, passwords are still used today.

Data integrity: Data integrity mechanisms are to provide integrity and non-repudiation services. If the confidentiality of a message is protected by 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 a data unit is usually protected by a checksum. To prevent an active attack, this checksum has to be protected, too. This can be done by encipherment or one-way hash functions. Cryptologically protected checksums are further referred to as message authentication codes (MAC). A MAC protects the integrity of a data unit. It doesn't protect the integrity of a sequence of data units. Sequence numbers and time stamps can be used here. Another possibility would be cryptological chaining.

Authentication exchange: Authentication exchange mechanisms provide peer-entity authentication services, verifying the identities of entities. This verification can be done in one or two ways, e.g. with passwords or challenge-response systems. Special protocols are needed for mutually distrusting parties [10]. Zero-knowledge schemes are very useful here [11].

Traffic padding: Traffic padding mechanisms are to prevent from traffic analysis.

Routing control: 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.

Notarization: Sensitive information, like public keys in a PKC, can be certified and published by a trusted certification authority.

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

Conclusions

To satisfy its communication needs, a company can either build a CN of its own, or it can outsource telecommunication, and subscribe a MNS. Both possibilities have advantages and disadvantages not only in the economic, but also in the security domain.

To make a CN secure, it is necessary to know all security-enhanced features that are provided together with public services and MNS. In the case of MNS, the subscriber should additionally control, whether his economic interests conflict with one or more interests of the MNS provider.

In the long term it is assumed that network and service providers will have to adapt the OSI security architecture and offer corresponding security services to their customers. Deregulations and liberalizations of telecommunication markets will probably intensify this tendency.

References

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

[2] H. Forner, ed., *Corporate Networks — Netze für Kommunikationsgemeinschaften.* Heidelberg: R.v. Decker, 1992.

[3] T. Valovic, *Corporate Networks: The Strategic Use of Telecommunications.* Norwood: Artech House, 1993.

[4] R. Oppliger, S. Weber, and D. Hogrefe, "Entwurf von virtuell privaten Netzen," in *Kommunikation in Verteilten Systemen* (N. Gerner, H. Hegering, and J. Swoboda, eds.), pp. 428 – 441, Springer-Verlag, 1993. ITG/GI-Fachtagung in München, 3. – 5. März 1993.

[5] S. Weber, R. Oppliger, and D. Hogrefe, "An Optimization Method for Virtual Private Network Design," in *Second IEE International Conference on Private Switching Systems and Networks*, Conference Publication No. 357, pp. 31 – 36, Institution of Electrical Engineers, June 1992.

[6] R. Oppliger and D. Hogrefe, "Sicherheit in unternehmensweiten Kommunikationsnetzen (CCN)," *Praxis der Informationsverarbeitung und Kommunikation*, vol. 15, no. 4, pp. 213 – 217, 1992.

[7] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644 – 654, 1976.

[8] P. Janson and R. Molva, "Security in Open Networks and Distributed Systems," *Computer Networks and ISDN Systems*, vol. 22, pp. 323 – 346, 1991.

[9] R. Rivest, M. Hellman, and J. Anderson, "Debating Encryption Standards," *Communications of the ACM*, vol. 35, no. 7, pp. 32 – 54, 1992.

[10] D. Sidhu, "Authentication Protocols for Computer Networks," *Computer Networks and ISDN Systems*, vol. 11, April 1986.

[11] A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Indetification and Signature Problems," in *Proceedings of CRYPTO '86*, pp. 186 – 194, Springer-Verlag, 1987.