LOCAL NETWORK CRYPTOSYSTEM ARCHITECTURE

Thomas A. Berson
R. Kenneth Bauer

Sytek, Inc.
1153 Bordeaux Drive
Sunnyvale, CA 94086
(408) 734-9000

ABSTRACT

This paper describes the end-to-end cryptosystem features of a commercially available broadband local network. The principles of operation of the network are described. The key distribution protocol is a session layer function which uses secret master keys and one or more key distribution centers. A stream cipher based upon DES is used at the transport layer for encryption of data.

INTRODUCTION

Contemporary local network realizations allow tens of thousands of user nodes to share a common broadcast medium. Any of these nodes may establish communication with any other. This flexibility of interconnection is one of the chief advantages of such a local network, but it does lead to problems for those users who are concerned with protecting their transmitted data against interception or modification by other users of the network.

Encryption of data between end-users is an effective safeguard against its unauthorized interception or modification. Encryption equipment has traditionally been obtained separately from the network and added in by the user. This approach suffers from: a) lack of interoperability amongst users, b) interference with proper operation of the network, and c) high cost.

In this paper we describe a local network which was designed from the first to incorporate an end-to-end cryptosystem. First we shall describe the principles of operation of the network, then the way in which the encryption/decryption and key distribution functions of the cryptosystem are placed in the protocol hierarchy of the network. We shall then describe protocol used for key distribution, and finally the cryptographic algorithm and its use for data encryption.

LocalNet (tm), A BROADBAND LOCAL NETWORK

The network which is the subject of this paper is a commercially available product called LocalNet (tm of Sytek, Inc.). LocalNet uses as its transmission medium the coaxial cable, fittings, connectors, amplifiers, etc. which were developed for CATV distribution systems. To this, LocalNet adds network front end devices (termed packet control units, or PCUs) which handle all network protocols up through the presentation layer and which provide interfaces to a variety of user terminal and host devices. We will give a brief description of those aspects of LocalNet operation which are pertinent to the cryptosystem. For further description of LocalNet see [2].

The topography of CATV transmission systems is tree-like. The tree is rooted in a location called the "head-end," which is where programs are inserted for distribution to viewers in CATV distribution applications.

The coaxial transmission plant used by LocalNet provides approximately 300 MHz. of useful bandwidth to its operator. (Components are just now coming on the market which provide 400 MHz). This bandwidth is the cable system owner's to allocate as he wishes. One simple way to allocate this bandwidth for data transmission is to allocate one half of it to transmissions toward the head-end and one half to transmissions away from the head-end. A device (called a LocalNet Tverter) is installed at the head-end.This acts very much like a satellite transponder in that it receives a range of frequencies, shifts all received energy in frequency, amplifies it, and retransmits it. This scheme of allocation is referred to as a "midsplit" system. Other standard allocation schemes, such as "subsplit," can also be accommodated by LocalNet.

Figure 1 illustrates a midsplit system. The low frequencies are used for transmission toward the head-end. Two different channels are shown by the

CH1739-2/82/0000-0138$00.75 © 1982 IEEE

Reprinted from COMPCON SPRING, February 1982

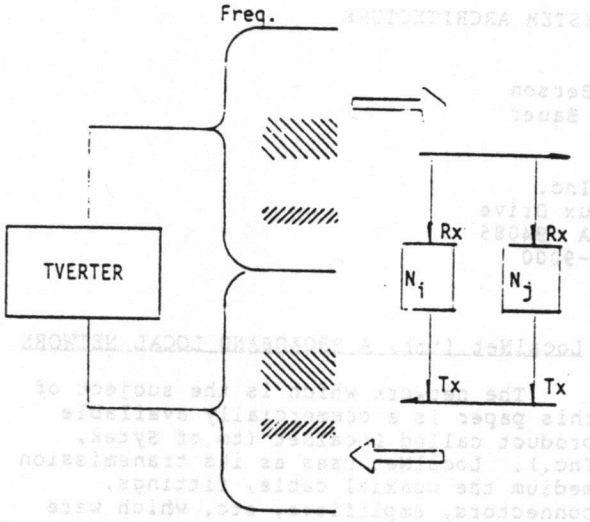

Figure 1: A channel consists of a pair of frequencies: one in the reverse direction and one in the forward direction. Many nodes share the same channel.

diagonal striped lines. The Tverter shifts all received energy upward by a fixed frequency and retransmits it in the upper half of the spectrum. Network nodes tuned to the same channel, shown as Ni and Nj, contain radio transceivers all of which transmit at the same low frequency and which all receive at the same high frequency.

The sharing of a channel by the many nodes tuned to it is controlled by one of several distributed protocols such as carrier sense multiple access with collision detection (CSMA/CD) [4,8,12,3]. These allocate the channel to nodes in accordance with their presented traffic. A great many network sessions can share the bandwidth provided by a single channel. LocalNet supports 120 channels of 128 Kbps data rate each and 5 channels of 2 Mbps each.

A LocalNet PCU is organized around an internal bus to which are connected one or more microprocessors devoted to protocol processing or interface support computation. Also connected to the PCU bus are a modem and a transceiver for connection to the cable, appropriate amounts of ROM and RAM, and devices for serial, parallel or DMA interface connection. Two special provisions are made for support of the cryptosystem. First, some of the RAM is provided with a backup battery power supply so that stored keys can survive a power outage. Second, a Federal Data Encryption Standard (DES) chip is connected to the internal bus.

NETWORK PROTOCOLS

The smooth integration of the cryptosystem with other network functions (such as the establishment of connections, the transport of data, the control of errors, and the avoidance of congestion) requires that the cryptosystem's functions be assigned to appropriate levels in the network's hierarchy of protocols. The two main cryptosystem functions which must be accommodated are 1) key distribution, and 2) encrypted transmission and reception.

Figure 2 is a diagram showing LocalNet protocol layers and their relationship to one another. The names of the layers, from Link through Presentation, are shown at the left. It will be seen that there are two alternative link layers upon which is built a network layer which provides for the transport of packets. The transport layer utilizes these packets to implement bytestreams whose delivery, freedom from error, and sequency are guaranteed. These guarantees are exploited by the algorithm which is used for encrypted transmission. The actual encryption and decryption of user data occurs at this level.

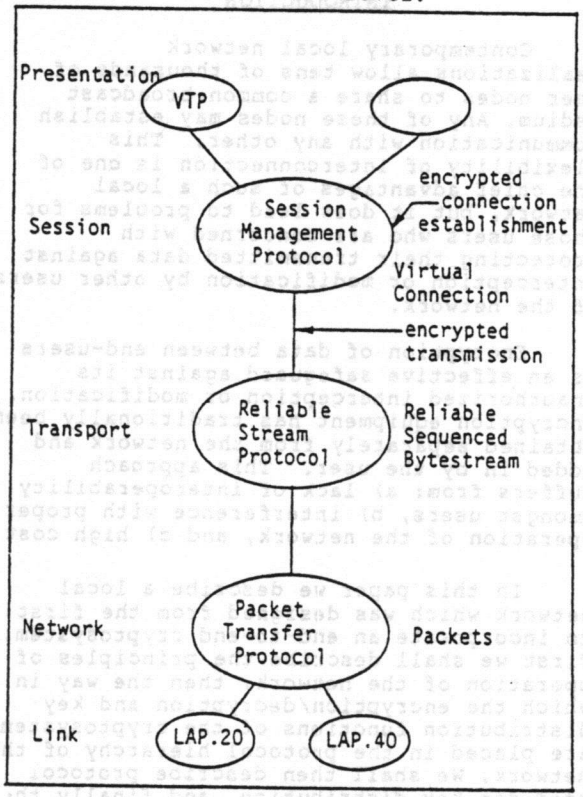

Figure 2: LocalNet protocol hierarchy. Key distribution is a session layer function. Encryption is a transport layer function.

The session layer implements full duplex virtual connections between network users. Fresh working keys are generated for each session and are distributed at the time the session is established. Key distribution is a session layer function.

KEY DISTRIBUTION

Many protocols using public key or secret key schemes have been previously described [9,11,6,7,10]. A secret key scheme was adopted for LocalNet primarily due to the immediate availability of mechanisms for the efficient use of secret keys. The key distribution protocol described here is similar to earlier secret key distribution protocols [9,6] but corrects important theoretical and practical deficiencies as described in [1].

Key generation, maintenance and distribution is accomplished by a specialized PCU referred to as a key distribution center (KDC.) The KDC generates and distributes over the network a session key (SK) to end-users who participate in a private session. The session key is used by the two end-users to encrypt and decrypt the data portions of their packets for the duration of the session in a manner described in the next section. Session keys are not used for more than a single session in order to limit vulnerability to cryptanalytic attack and to minimize the volume of any compromised data.

Each PCU contains a master key (MK) known only to the PCU and the KDC. The KDC encrypts session key distribution messages under the recipient's MK so that an eavesdropper cannot understand the session key distribution message and thereby decrypt the presumed private session. Because very little data is encrypted under the master keys they are changed infrequently by the site security administrator (SA) taking manual action.

Master Key Distribution

The master key is used for each PCU is derived from a pass phrase selected by the SA. The SA inserts the pass phrase and PCU address into the KDC which transforms it into a master key and assigns it to the supplied network address. Next the PCU at the named network address is visited or brought to the KDC location where it is supplied with the same pass phrase. The installation of PCU master keys can be performed infrequently by a single individual per KDC and can be done in a manner which does not impact the PCU user.

The pass phrase translation algorithm samples fifty six bits of the phrase and computes appropriate parity as the eighth bit of each byte. The result is called the pass phrase key. The pass phrase key is used to encrypt a fixed quantity in order to form a master key with good random bit distribution. The resulting master key is screened to ensure it is neither zero (used to designate an unloaded master key) nor one of the crytographically weak keys [5].

Session key distribution by the KDC may best be understood by examining the sequence of actions which occurs when a secure connection is established. A major threat to the distribution of session keys is active wiretapping whereby an intruder alters transmitted messages or replays previously recorded messages. The protocol used by LocalNet incorporates advances in key distribution protocol technology in order to prevent this type of attack. A substantial portion of key distribution protocol message content is devoted to establishing current authentication of the communicants and of the KDC(s).

Session Key Distribution by a Single KDC

In the following discussions A is used to designate the communicant who is initiating the connection and B is the connection recipient. The symbols:

$$\{ I1, I2, \ldots, In \}^{K1}$$

are used to indicate that the message formed by concatenating data items I1 through In is encrypted using K1 for an encryption key. All data items are one or more blocks in length, where each block is eight bytes. Block encryption is used for all protocol messages (1.1-1.4 and 2.1-2.6). A graphic representation of the protocol messages, (1.1-1.4), used in this situation is shown in Figure 3.

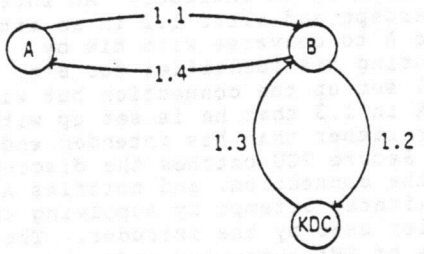

Figure 3: Session key distribution with a single KDC.

End-user A decides he would like to open a secure connection with B and issues the secure call command which sends the following message to B:

$$A \rightarrow B: \quad A, \{EMa\}^{MKa} \qquad (1.1)$$

A asks B for a secure connection by sending his claimed identity and an event marker (EMa) unique to this conversation to B. B can either refuse the secure connection or continue the protocol in which case the protocol continues by B sending the following message to the KDC:

$$B \rightarrow KDC: \quad A, \{EMa\}^{MKa}, B, \{EMb\}^{MKb} \qquad (1.2)$$

B requests a session key and various identity assurances from the KDC by sending his claimed identity and his unique event marker, in addition to those of A.

$$KDC \rightarrow B: \quad \{SK,A,EMb\}^{MKb} \quad \{SK,B,EMa\}^{MKa} \qquad (1.3)$$

The KDC generates a unique session key SK by using the DES chip as a random number generator. The KDC maintains a seed in its permanent memory which it increments and encrypts to create the session key. The KDC sends B a message consisting of two similar parts: one intended for B and one to be forwarded by B to A. Note that message (1.3) could be sent to A instead of to B, or to A as well as to B. These alternatives are equivalent in terms of the security they provide; however, the chosen method requires the fewest network connections. To encrypt the message, the KDC retrieves the appropriate end-user master keys and uses them in conjunction with the KDC DES chip.

B can decrypt the first part of (1.3) to learn the session key, his intended end-user A, and his original event marker EMb. A encrypted under B's master key assures B that the KDC understood his request and that that portion of (1.2) was not modified by an intruder. An intruder can intercept and alter 1.2 in an attempt to cause A to converse with him by substituting his identifier for B's. The KDC will set up the connection but will advise A in 1.3 that he is set up with the intruder rather than his intended end-user B. A's Secure PCU catches the discrepancy, breaks the connection, and notifies A of an active wiretap attempt by supplying the identifier used by the intruder. The presence of EMb encrypted under B's master key is assurance that (1.3) was not previously recorded by an intruder and played back. Note that the session key appears only twice, once encrypted under A's master key and once encrypted under B's master key.

$$B \rightarrow A: \quad \{SK, B, EMa\}^{MKa} \qquad (1.4)$$

B forwards to A the portion of (1.3) encrypted with A's master key. A can decrypt (1.4) to learn the session key and to obtain the same assurances enjoyed by B from the same source.

Session Key Distribution by Multiple KDCs

Where networks encompass multiple security communities (for example, accounting and research), each community may wish to implement the level of physical security it feels is necessary for the protection of its own KDC. LocalNet accommodates this situation by supporting multiple KDC's. Secure connections can be made between nodes governed by the same KDC or between nodes governed by separate KDC's through the use of an inter-KDC communications protocol (see Figure 4).

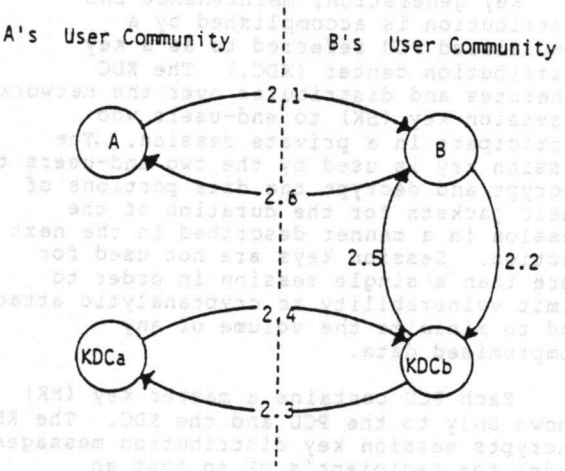

Figure 4: Session key distribution with multiple KDCs.

In this situation, each end-user receives assurance from his own KDC. Here KDCa is the name or location of A's KDC.

$$A \rightarrow B: \quad A, \{EMa\}^{MKa}, KDCa \qquad (2.1)$$

Message (2.1) is modified to include the address of A's KDC.

$$B \rightarrow KDCb: \quad A, \{EMa\}^{MKa}, KDCa, B, \{EMb\}^{MKb} \qquad (2.2)$$

$$KDCb \rightarrow KDCa: A, B, \{EMa\}^{MKa}, \{EMkdcb\}^{MKkdca} \qquad (2.3)$$

When B receives (2.1), he forms (2.2) and sends it to his KDC. KDCb then sends (2.3) to KDCa, requesting that KDCa generate the

session key. EMkdcb is an event marker protecting KDCb from playback attacks. MKkdca is KDCa's communication key which is known to all other KDCs and is used for secure communications between KDCa and all other KDCs.

$$KDCa \rightarrow KDCb: \{SK, B, EMa\}_{MKa}, \{SK, EMkdcb\}_{MKkdca} \quad (2.4)$$

A's KDC generates the session key, encrypts the message eventually destined for A under A's master key, and returns KDCb's event marker.

$$KDCb \rightarrow B: \{SK, A, EMb\}_{MKb} \{SK, B, EMa\}_{MKa} \quad (2.5)$$

$$B \rightarrow A: \{SK, B, EMa\}_{MKa} \quad (2.6)$$

These are identical to 1.3 and 1.4.

CRYPTOGRAPHIC ALGORITHM

A stream cipher is used for the encryption and decryption of the data portion of packets. In brief, DES is used to provide a keystream which is applied by modulo-two addition synchronously at both ends of the connection. Further details of its generation and application are in this section.

The method of keystream generation is illustrated in Figure 5. DES is keyed with the SK and with an initial vector (IV). SK and IV form the session key which is distributed by the protocol described in the previous section. The keystream is generated by encrypting the sequence IV, IV+1, IV+2, ... under SK. This scheme is certain to generate a maximum length sequence, as shown in Figure 5a. It was chosen over a feedback or autokey scheme because either of those may generate a short sequence in one of the ways shown in Figure 5b.

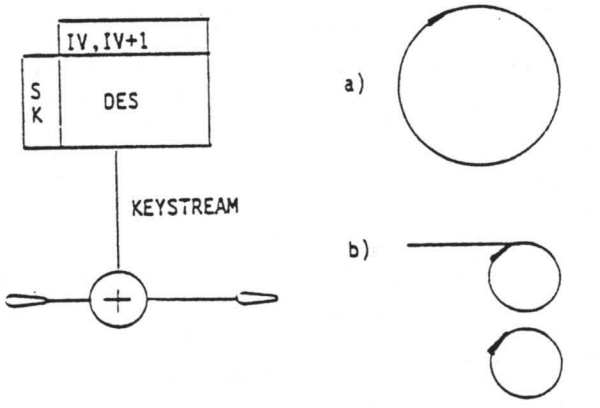

Figure 5: DES is used to generate a keystream. a) illustrates the maximum cycle. b) shows shorter cycles which may arise from feedback schemes.

Recall that the transport layer of protocol provides a stream of bytes which is guaranteed to be free from errors and in proper sequence. These guarantees are relied upon for proper operation of the encryption scheme which, by itself, offers no resynchronization.

In practice two keystreams are generated for each session, one for each direction of transmission. These are keyed separately and operate independently.

Any given PCU is idle much of the time and the speed of most network components is high compared to the speed of the DES device. This leads to a bursty demand for keystream which could not be satisfied in real time without degrading network performance. The scheme used here allows keystreams to be precomputed and then cached until they are needed. Careful exploitation of this property allows LocalNet to use a single moderate speed DES device to service sixteen full duplex encrypted connections (thirty two keystreams) through a PCU.

REFERENCES

[1] Bauer, R.K., T.A. Berson, and R.J. Feiertag, "A key distribution protocol using event markers," Sytek Report TR-81060, Sytek, Inc., Sunnyvale, CA (1981).

[2] Biba, K.J., "LocalNet(tm): a digital communications network for broadband coaxial cable," Proc. IEEE CompCon, (Feb. 1981), pp. 59-63.

[3] Bux, W., "Local area subnetworks: a performance comparison," in West, A. and Janson, P., eds., Local networks for computer communications, North Holland Publishing Co. (1981), pp. 157-180.

[4] Clark, D.D., K.T. Pogran and D. P. Reed, "An introduction to local area networks," Proc. IEEE, Vol. 66, (1978), pp. 1497-1517.

[5] Davies, D.W., private communication, (1981).

[6] Denning, D.E. and M.S. Sacco, "Timestamps in key distribution protocols," CACM, Vol. 24, (Aug. 1981), pp. 533-536.

[7] Merkle, R.C., "Protocols for public key cryptosystems," Proc. 1980 Symp. on Security and Privacy, IEEE, p. 122.

[8] Metcalfe, R.W. and D.R. Boggs, "Ethernet: distributed packet switching for local computer networks," CACM, Vol. 19, (1976), pp. 395-404.

[9] Needham, R.M. and M.D. Schroeder, "Using encryption for authentication in large networks of computers," CACM, Vol. 21, (Dec. 1978), pp. 993-999.

[10] Popek, G.J. and C.S. Kline, "Encryption and secure computer networks," ACM Computing Surveys, Vol. 11, (Dec. 1979), pp.331-355.

[11] Price, W.L., and Davies, D.W., "Issues in the design of a key distribution centre," Report DNACS 43/81, National Physical Laboratory, Teddington, Middlesex England, (April 1981).

[12] Tobagi, F.A. and V.B. Hunt, "Performance analysis of carrier sense multiple access with collision detection," Technical Report 173, Computer Systems Laboratory, Stanford University, Stanford, CA, (1979).