

Secure communication with ComSaveBox

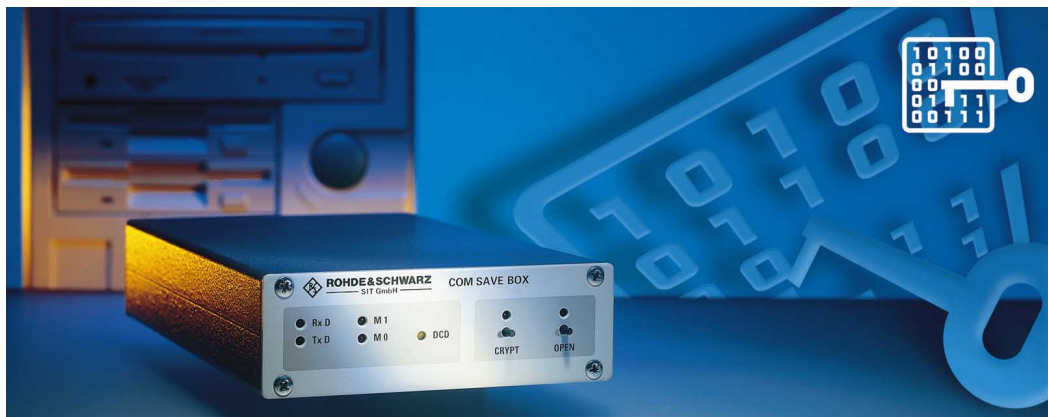


FIG 1
ComSaveBox
encrypts any
modem link online.
Photo 42 801

Serial links are widely used to transmit information. The data are usually transmitted via modems and public telephone networks. But anyone can access these routes, so there are threats to confidentiality and integrity of data. Data can be intercepted, manipulated or retained, for example, without the sender or recipient noticing. Consequently sensitive data have to be suitably protected against such threats. The most efficient method is the use of cryptography, ie transformation of data so that no conclusions can be drawn about their contents. Furthermore, there are special mechanisms to protect transmitted information against unnoticed manipulation.

ComSaveBox security system

The small ComSaveBox (FIG 1) ensures confidentiality of data during their transfer via the serial interface of a data terminal, a PC for example. All data are automatically encrypted before they are sent out and decrypted when received, thus reliably protecting them against unauthorized access. The FEAL-16X algorithm used for encryption has been analyzed worldwide and is generally recognized. It has a code length of 128 bits and is an impenetrable barrier even for modern methods of cryptanalysis. The design and development of such systems was based

on German and European criteria for IT security. ComSaveBox supports an RS-232-C interface with rates from 9600 to 115 200 baud and the usual standard protocol (8 bits, no parity bit, 1 stop bit). The necessary hardware protocol (DTR/DSR or RTS/CTS) is fully transparent.

The unit can be operated in encrypted and in open transmission mode. In encrypted mode the data sent from the data terminal to ComSaveBox are first encrypted and then forwarded to the data transmission equipment. Data received by the transmission equipment and transferred to ComSaveBox are decrypted and then passed to the data terminal. The code used for encryption and decryption is set by the communication partners prior to data transmission or by remote access through a configuration program. The user can choose between a temporary and a permanent code. A permanent code, which remains stored when ComSaveBox is switched off, is recommended for frequently used links, as for example to a company headquarters, and a temporary code for one-time links. ComSaveBox operates with full transparency in the open mode. Data transmission uses the customary software, eg terminal programs for access to mailboxes and connection to other computers and programs for

accessing networks via a modem line (eg asynchronous communication server, NetWare Connect).

Examples of application

File transfer between mailbox and PC

The mailbox of a company stores confidential data, and only authorized persons may access it. Password protection alone is not considered sufficient to prevent unauthorized access. The mailbox is installed on a computer that is fitted with a modem and receives incoming calls. In addition, data should be protected against unauthorized eavesdropping during transmission in the telephone network. To this end, the mailbox computer is fitted with ComSaveBox. All persons who are to have access to the mailbox also have ComSaveBox installed (FIG 2). For mailbox access a code is defined that only authorized persons are informed of. This enables connection to the mailbox and data exchange in encrypted form. Connections in plain text or with the incorrect code are automatically interrupted by ComSaveBox.

Access to Novell network via modem

Company employees are to be able to access the inhouse Novell network from their homes. For this a connect server

with a modem and NetWare Connect software are installed. The NetWare password used as the sole means of protection is not regarded as sufficient to prevent unauthorized access. In addition to the password, data are to be protected by encryption during transmission in the telephone network. The connect server is fitted with ComSaveBox. All persons who are to have access to the network will also have ComSaveBox installed at their end and a code is arranged with them. Links with differently set operating modes (eg one ComSaveBox set to "Crypt", the other to "Open") or with an incorrect code are automatically interrupted by ComSaveBox.

Transmission via RS-232-C interface without modem signals

The data collected by a telemetry station are to be transmitted by radio to a

stored even with ComSaveBox switched off. In this case no further configuration of the telemetry unit is required, ie a PC is not needed at the site. With the configured ComSaveBox installed at the telemetry station, an encrypted link can be set up when needed by means of the "Crypt" key on the ComSaveBox at the central station. When the link is no longer required, the encrypted link is cleared down by pressing the "Crypt" key again. Of course, open links are possible any time using the "Open" key.

Use of ISDN modem

Users who frequently have to transmit large amounts of data cost-effectively will recognize the benefits of ISDN. ISDN modems present a number of advantages over plug-in PC cards, so their fields of application are constantly expanding. Installation, identification,

pose. ComSaveBox is inserted between the PC and the ISDN modem and initialized (setting of code and mode). If the called station has the same configuration, transmission is possible with a terminal program (eg Telix from ELSA). Transmission rates of up to 115 200 baud can be achieved with two B channels (channel trunking).

Frank Bergmann; Klaus Hesse

REFERENCES

- [1] Krieghoff, H.; Sörgel, D.: SIT – Security in Information Technology. News from Rohde & Schwarz (1997) No. 153, pp 41–43
- [2] Bergmann, F.: Security for modem links with ComSaveBox. News from Rohde & Schwarz (1997) No. 155, p 39

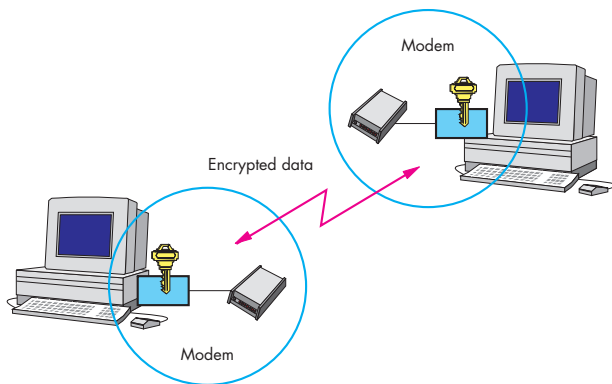


FIG 2
ComSaveBox encryption unit is inserted between data terminal (here PC) and data transmission equipment (here modem).

central station. The radio equipment has an RS-232-C interface to send digital information, and this is to be encrypted against unauthorized access during transmission. ComSaveBox is inserted into the link between the data collection unit and the radio equipment of the station, and another one is required at the central station. Here the RS-232-C mode is set for the two boxes and also the code for the unit of the telemetry station, ie when a permanent code is to be used, which remains

available resources (interrupts) and problems with CAPI drivers make the use of plug-in PC cards less desirable. What is more, ISDN modems can easily be taken to another operating site, also in connection with laptops. The transmitted data are to be protected against unauthorized access. ComSaveBox is most suitable for this application, especially with its high communication speed of 115 kbaud. An ISDN modem (eg MicroLink ISDN/Tlpro from ELSA) is required for this pur-

Reader service card 161/09