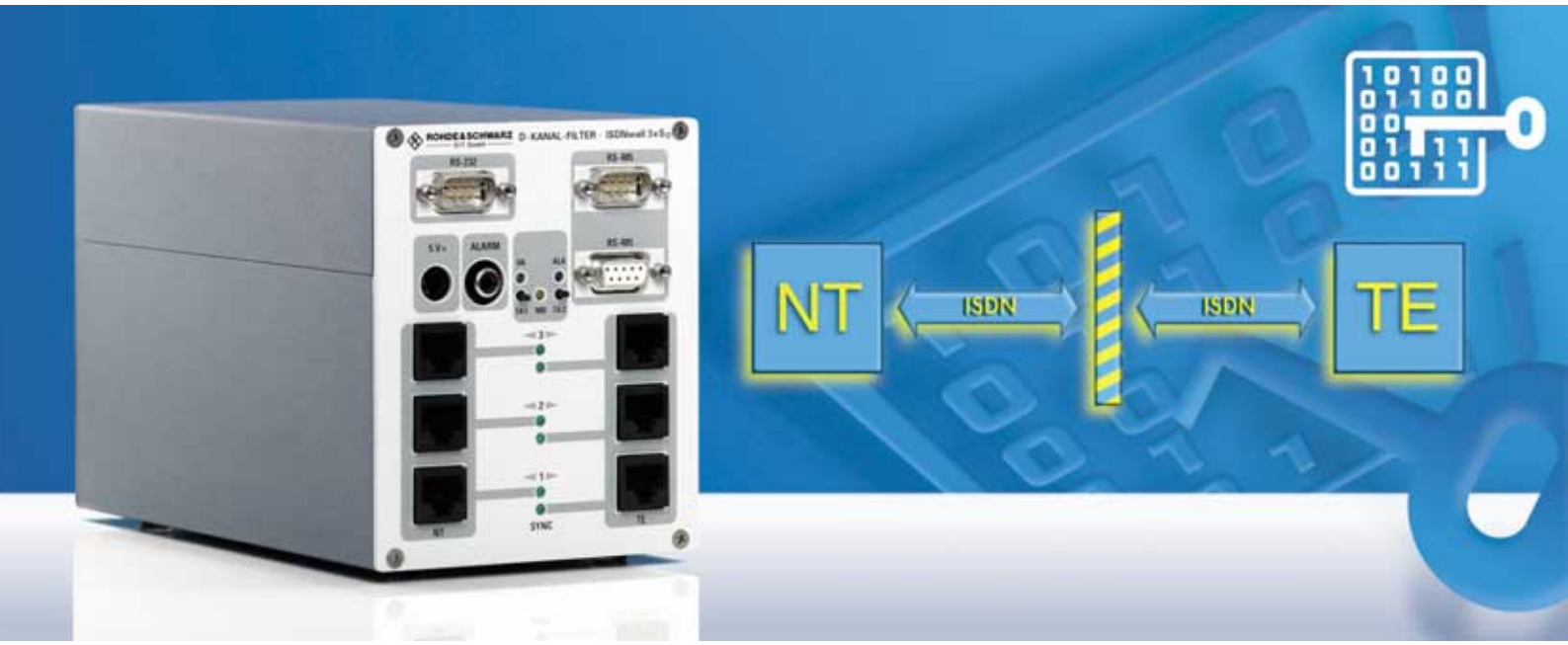


D-Channel Filter ISDNwall

Protection of digital telecommunication systems against manipulations via PSTN

- Firewall for ISDN network
- Intrusion detection
- For interfaces S_0, $3xS_0$ and S_{2M}
- Alarming/alerting and recording of security violations
- High security standards for administration and revision
- Adaptable to changing threat potentials

BSI Bundesamt für Sicherheit in der Informationstechnik

ROHDE&SCHWARZ

Problem

Analog facilities of private telecommunication systems have been rapidly replaced by digital equipment. Especially business companies and authorities can no longer be imagined working without the integrated services digital network (ISDN) and to an increasing extent all corporate communications with external contacts are made via ISDN. Almost unnoticed, this has brought about new security problems for telecommunication systems. While intrusions into the analog system were mainly via physical system components (e.g. network lines), digital systems are vulnerable at the logic level, e.g. to manipulations via the system's own programs or data records.

State-of-the-art digital telecommunication systems often provide hundreds of functions, many of which can be misused. On the one hand, the user of a digital system can profit from a great number of useful and convenient functions but, on the other, a potential intruder has many possibilities for misuse and manipulations. Yet in most cases the users will not be in a position to detect such attacks/misuse.

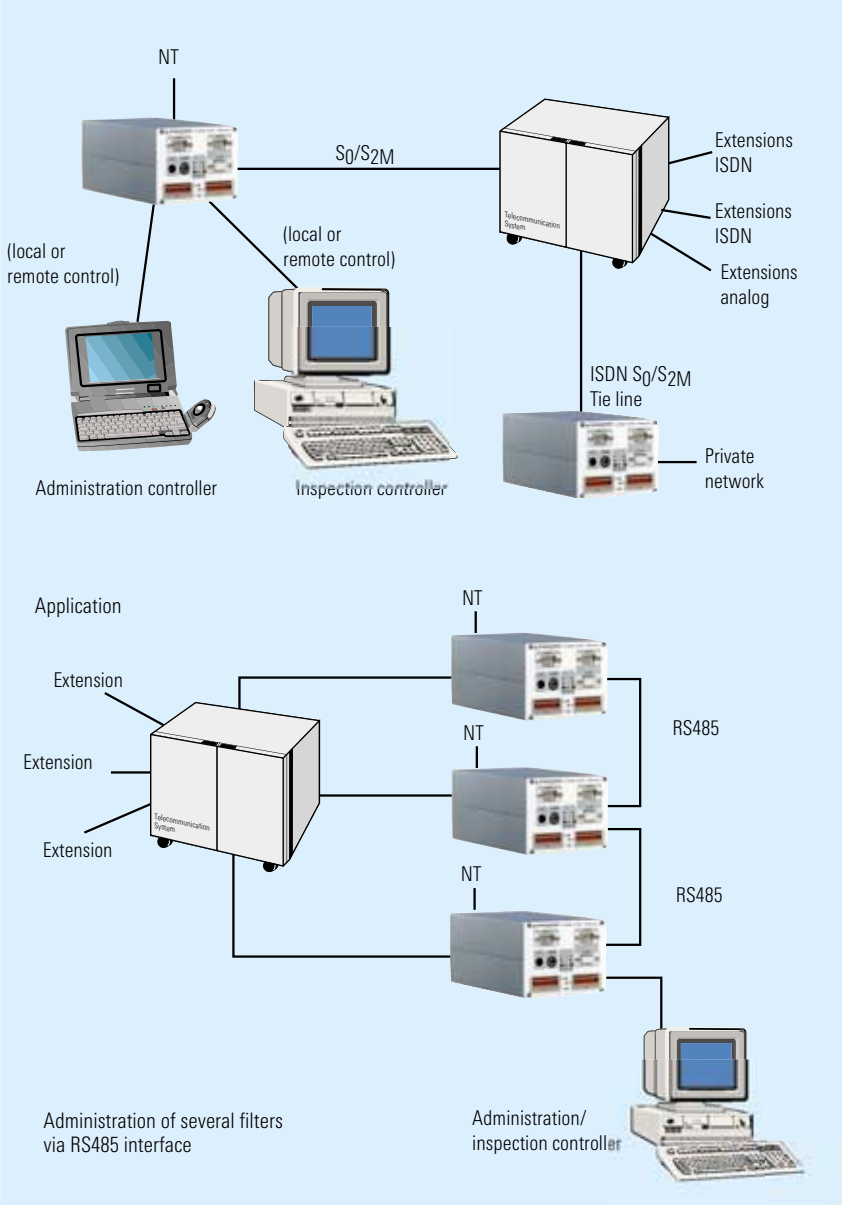
Another aspect is that digital telecommunication systems are often not configured or managed by their users. This means that the user does not know the actual configuration of his system.

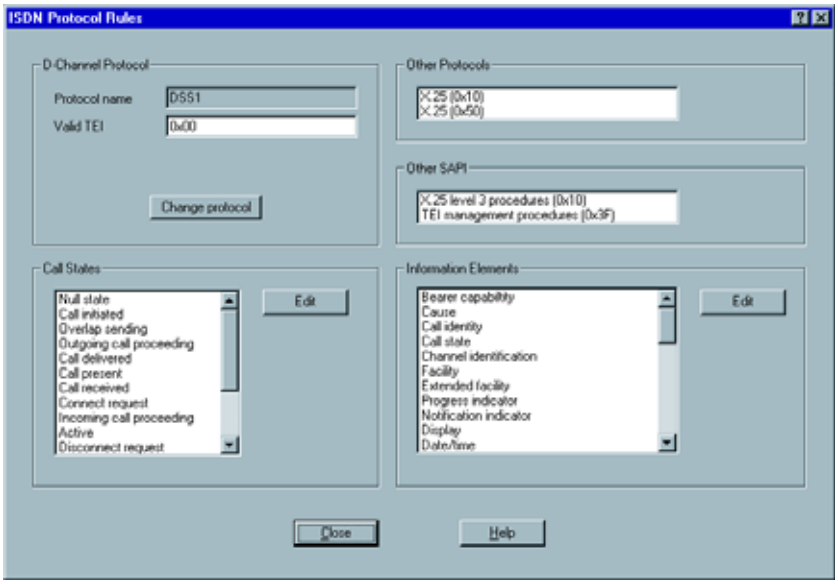
The following examples demonstrate the harm that can be done by the misuse of functions:

- The handsfree facility may be activated from the telephone set but also from the PSTN permitting eavesdropping.
- Remote servicing is mostly carried out via special call numbers. Since, in practice, the associated passwords are very rarely changed, access to the administration level and so reconfiguration of the system is relatively easy.
- Direct dialling from exchange to exchange allows worldwide calls to be made from an external telephone set at the expense of the owner/user of the telecommunication system.
- Concealed information transfer via D-channel makes it possible to activate programs previously implanted in the telecommunication system (Trojan horses), their aim being to empower the attacker with control.

An important target here is the unconcealed transmission via the ISDN's D-channel. With the appropriate know-how and suitable technology, elements of the control protocol can be used to cause damage in telecommunication systems (activation of programs in the telecommunication system, manipulation of the internal sequence control of the telecommunication system, access to the administration level).

Examples of integration and administration of the D-channel filter

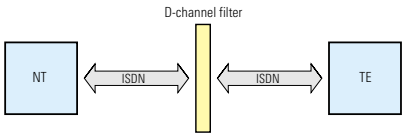




Dialog box ISDN-specific filter rules

Solution

With the aid of a special D-channel filter, unauthorized control information can be filtered out and the associated threats eliminated by suitable actions, e.g. by clearing down the link.



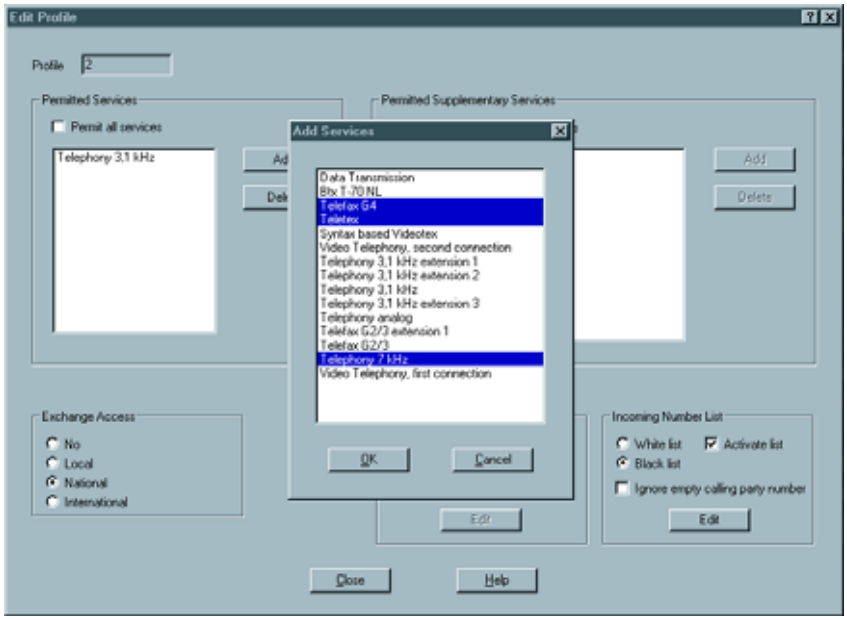
Based on an order from the German Information Security Agency (BSI), Rohde & Schwarz SIT GmbH developed a D-channel filter (ISDNwall) for protecting digital telecommunication systems against manipulations via the PSTN.

ISDNwall cuts down on performance features and services of specific extension numbers, thus normally preventing misuse and eliminating threats. This is to avoid the unauthorized use of services and performance features and the deliberate sabotage from outside.
ISDNwall simulates the telecommunication system to be protected and uses the switching procedures of the standard D-channel protocol regarding call numbers (extensions), services (voice, data transmission, fax, voice mail) and the assignment of services and performance features to individual extensions.

D-Channel Filter ISDNwall is fitted between the exchange connection and the telecommunication system. With regard to signalling in the ISDN, the filter acts as a terminal equipment (TE) for the exchange line and as a network termination (NT) for the telecommunication system. The great variety of functions ensures ISDN basic access (S_0) and primary rate access (S_{2M}) to DSS1 protocol. Adaptation of ISDNwall to other protocols is possible.

The B channels with the useful information are transparently looped through but there is no direct physical connection between the NT and TE sides of the D-channel filter. In case of unidentified, incomplete or unexpected protocol elements or sequences, ISDNwall reacts in conformance with the DSS1 protocol. Unauthorized attempts to use features and services are countered by ISDNwall with a link cleardown. The same reaction is caused by the violation of ISDN-specific filter rules. Such incidences are registered – directly when occurring – in an internal record.

In addition to the recording of any attempt of intrusion, an optical alarm and an acoustic interval alarm are output. The optical signal remains on until it is explicitly reset by the administrator.



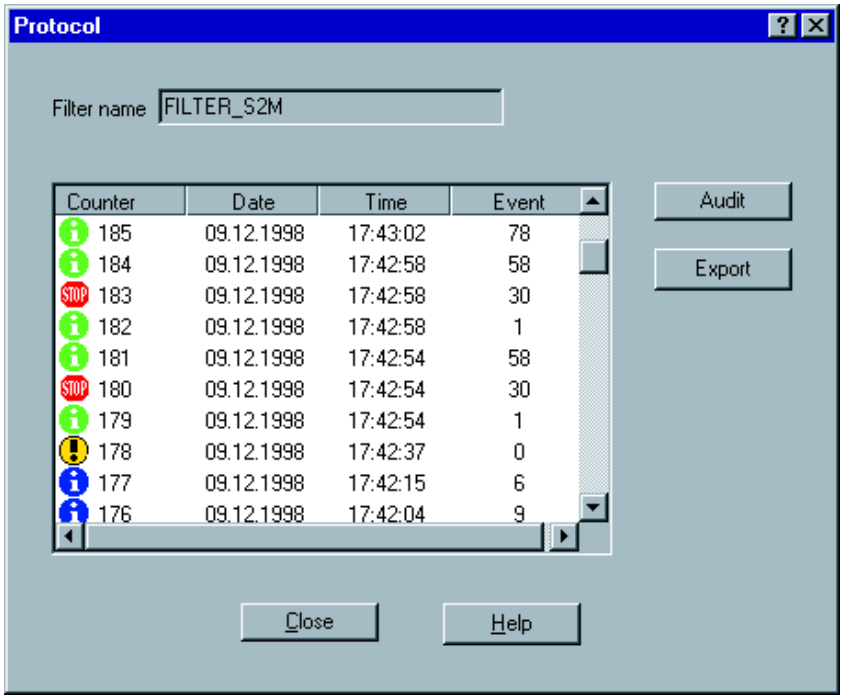
Dialog box Edit Profile

ISDNwall is equipped with two serial interfaces (RS-232-C, RS485) which can be used for local administration and inspection. Central management for remote administration, inspection and alarming/alerting can be integrated as an option. Administration and inspection are performed via a protected and encrypted line. The protocol used meets the requirements to E3/high of ITSEC.

The following variants of the D-channel filter are available:

- with one S_0 interface for multiple access interfaces
- with one S_0 interface for basic access interfaces
- with 3 S_0 interfaces for basic access interfaces
- with S_{2M} interface for access interfaces (primary rate access interface)

ISDNwall is supplied as an external unit. Administration and recording software, a basic configuration of the filter (on request customized) and manuals for installation and operation are provided with the filter.



Recorded events

Specifications

Controller	CPU 80486
ISDN inputs/outputs	S_0 devices: 1 or 3 basic access interfaces S_0 S_{2M} devices: 1 primary rate access interface S_{2M}
Serial interfaces	RS-232-C, RS485
ISDN protocols	DSS1, adaptation to other protocols possible
Approvals	CE0681X
Evaluation	user software developed to E3/high of ITSEC and submitted for certification
Number of extensions	filter parameters for up to 9999 extensions (optionally more) in up to 256 user profiles can be implemented

General data

Operating temperature range	+5 °C to +45 °C
Power supply	
AC	220 V to 240 V ±10%, 47 Hz to 53 Hz (12 VA)
DC	5 V, 2A
Floating output	alarm line connection
Dimensions (W x H x D)	
S_0 and S_{2M}	105 mm x 85 mm x 205 mm
$3xS_0$	105 mm x 115 mm x 205 mm
Weight	
S_0 and S_{2M}	1.5 kg
$3xS_0$	2.0 kg

Certified Quality System
ISO 9001
REG. NO CERT-01 100 025007

Ordering information

Designation	Order number
ISDNwall S_0	3534.3558
ISDNwall 3x S_0	3534.3858
ISDNwall S_{2M}	3534.3612
ISDNwall for multiple access interface	3534.3206

Equipment supplied

Filter unit
Power supply with cable, cable for connection to RS-232-C interface, CD-ROM with administration and inspection software in German and English, user manual, installation manual
Instruction for use:
A PC/laptop with Windows9x or NT is neccessary for administration and inspection. The connection of ISDNwall to an UPS is recommended.

ROHDE&SCHWARZ
ROHDE & SCHWARZ SIT GmbH · Agastr. 3 · 12489 Berlin · Germany
Telephone (+4930) 65884-223 · Fax (+4930) 65884-184 · e-mail: contact@sit.rohde-schwarz.com · www.sit.rohde-schwarz.com

Printed in Germany 0201/0902 (Bi bb)