AUSGABE 1/02

SWITCHED

T.D.T.®
Transfer Data Test GmbH

Wir laden ein
CeBIT
HANNOVER
13.-20. 3. 2002
Halle 1 Stand 8k4

STIMMEN SIE AB: Wuenschen Sie die SWITCHED in Papierform wie bisher oder nur noch abgespeckt digital? !

Mehr dazu auf Seite 4

Neues T.D.T.-FLAGGSCHIFF ROUTER R1650

Produkt Manager Thomas Maier
skizziert im Editorial und auf Seite 2 TDT-Produkte

Siegfried Vogl
Entwicklungsleiter Technik auf Seite 4 ueber die Ziele der Entwicklungsabteilung

CeBIT 2002 - Einladung
ganz im Zeichen des neuen Routers R1650

Wolfgang Wanner
Neuer Leiter der Doku - mit privaten Einblicken

T.D.T. auf neuen Wegen
Die SPS im Rueckblick

Neuer Pocket-Guide IPSec
und
T.D.T.-Pin
auf der CeBIT kostenlos

QUOWADIS X25

Löst die von T.D.T. entwickelte Routerfamilie die X.25-Datenübertragung ab?

Seit über 18 Jahren hat sich X.25 als Standardprotokoll für die Datenübertragung etabliert. Und selbst nach dieser langen Zeit lässt sich die Technik immer noch empfehlen: Sie ist sicher und erfüllt die gestellten Anforderungen. Doch mit dem Einzug des Internet-Protokolls und den verfügbaren Sicherheitsmechanismen wie IPSec erwächst dem Klassiker eine starke Konkurrenz. Vor allem Kostengründe sprechen für die IP-Technik. *TDT* hat deshalb einen IP-Router mit X.25-Gateway entwickelt, der die bisherigen X.25-Investitionen schützt und die preiswerten Internet-Anschlüsse nutzt.

Es ist schon eine eindrucksvolle Erfolgsgeschichte, die X.25 und der entsprechende Service Datex-P der Deutschen Telekom hingelegt haben. Schon vor zehn Jahren verfügte der Netzbetreiber mit 63 Vermittlungsrechnern über eine gesicherte Flächendeckung in Deutschland. Mit etwa 180 Zugangsknoten an 80 Standorten ist die Technik an jedem Ort in Deutschland präsent. Bereits vor sieben Jahren nutzten die Unternehmen in Deutschland etwa 80.000 Hauptanschlüsse, weitere 20.000 X.25-Nutzer verfügen über feste Nutzerkennungen. Parallel zu dieser Erfolgsstory entwickelte sich die Technik weiter und die Integration von ISDN sorgte für einen weiteren Wachstumsschub. Die Neigung, X.25- und ISDN-Übermittlungen durch die IP-Technik zu ersetzen, steigt jedoch, zumal mit IPSec der so lange gesuchte sichere Übertragungsstandard vorhanden ist. Vor allem Bankautomaten, Reisebüros, Lotto-Terminals, Kreditkartenscanner, Alarmsysteme und Registrierkassen verwenden die paketübermittelnde Technik. Hier werden Zahlenkombinationen hin- und hergesandt, die wenig Bandbreite benötigen. So verwundert es nicht weiter, dass mehr als die Hälfte aller Anwendungen mit Datenraten von 2.400 Bit/s bis 9.600 Bit/s auskommen. Beispielsweise dient der Datendienst beim Polizeinotruf in Bayern und Baden-Württemberg als Ersatz für die Festverbindung. Für das Übermitteln der Datenmeldungen reicht die niedrige Datenrate von 9.600 Bit/s voll aus.

Die Alternativen: Datex-P, Datex-P-ISDN und Internet

Niedrige Bandbreiten für die Übertragung bedeuten aber nicht gleichzeitig, dass langsam kommuniziert wird oder sich der Verbindungsaufbau verzögert. Dies wäre für Kreditkartenterminals oder Kassen nicht zu tolerieren, schon alleine aufgrund der Wartezeiten für den Kunden. Neben der Schnelligkeit ist es vor allem das Kostenargument, das den Ausschlag für die ISDN-Integration von X.25 gibt. Anstatt 240 Euro für einen X.25-Hauptanschluss mit 9.600 Bit/s kostet ein vergleichbarer Datex-P-ISDN-Anschluss lediglich 30,68 Euro pro Monat. Und das summiert sich bei einigen hundert angeschlossenen Endgeräten beziehungsweise Terminals schnell zu stattlichen Summen.

Die Ausgangslage hat sich in den letzten Jahren durch das Internet jedoch erheblich verändert: Einfache Internet-Zugänge via ISDN liefern hier schnelle und sichere Zugänge. Darüber hinaus sorgen preiswerte DSL-Anschlüsse, die nur noch knapp 10 Euro zusätzlich zur ISDN-Grundgebühr kosten, für neue Alternativen. Die damit aufgebaute Festverbindung zum Provider lässt sich nicht nur für die Internet-Kommunikation nutzen, sondern steht vielmehr auch anderen Datenverbindungen offen. Auf diese Weise lassen sich die schon vorhandenen Kommunikationswege für Internet und Sprache zusätzlich nutzen. Für Tausende von angeschlossenen Terminals und den Host-Anschluss lassen sich mit diesen Alternativen insgesamt bis zu 1 Million Euro im Jahr einsparen – sofort und ohne Umstellung der Hardware.

Die Alternative Internet ist sicher und preiswert

Schon immer sorgte das Internet für Diskussionen: Preiswert, aber unsicher. Und dieser Beigeschmack war mit den bisherigen X.25-Anwendungen nicht zu vereinen. Dies hat sich aber geändert. Tunneling-Verfahren und die Einführung von Sicherheitsmechanismen wie IPSec sorgen für ein hohes Maß an Sicherheit. Es liefert ein Layer 3-Tunneling auf der IP-Protokollebene sowie eine persönliche Authentifizierung des Nutzers. Zusätzlich regelt es den Schlüsselaustausch und die Verschlüsselung. Verfahren wie Triple-DES (Data Encryption Standard) mit 168 Bit Schlüssellänge, asymmetrische RSA-Chiffrierung (Rives, Shamir, Adleman) mit 2.048 Bit sowie Blowfish mit Schlüssellängen von 448 Bit lassen sich auf den Übertragungswegen einsetzen.

Neben der Sicherheit der Verbindungen müssen noch weitere Aspekte bei einer Ablösung von X.25 beachtet werden: So benötigt die gewohnte Verfügbarkeit des Dienstes spezielle Kniffe, um die Anwendungen auf dem Laufenden zu halten - und diese Anforderungen erfüllt der neue *TDT*-Router R1650. Ein intelligentes Backup über GPRS, der beim kompletten Ausfall der ISDN-Leitung auf die Luftschnittstelle umschaltet, ist eines der wichtigsten Leistungsmerkmale. Ein sehr günstiger Anbieter für diesen Dienst ist beispielsweise E-Plus, der einen grundgebührfreien GPRS-Datentarif anbietet und pro Kilobyte 2,5 Cent berechnet. Zusätzlich sichert der Router über ein Provider-Switching die Verfügbarkeit der Datenverbindung ab und wählt aus maximal fünf Netzbetreibern einen funktionierenden Zugang aus.

Migration ohne Hardwarewechsel: die richtigen Konzepte für den Umstieg

„Never change a running system" ist eine der Arbeitsgrundlagen aller IT-Experten. Diese Regel wird durch die *TDT*-Lösung weitgehend eingehalten: Die Kommunikationsstrukturen von und zum Host fahren wie bisher X.25-Protokolle und werden hardwareseitig genau so angeschlossen. Auch die Terminals nutzen künftig die bisher gewohnten Protokolle. Darüber hinaus lassen sich mit dieser Lösung weitere Dienste integrieren, die rein auf IP aufsetzen und mit dem Host kommunizieren müssen.

Router R1650

Diese Vorteile setzt der *TDT*-Router 1650 um. Er verfügt über eine X.25-, Ethernet- sowie ISDN-Schnittstelle. Die Neuentwicklung, die auf der CeBIT präsentiert wird, wandelt die Daten der Endgeräte aus den ursprünglichen Formaten (SDLC, Bisync, Async, T3-POS, Visa1, ALC sowie SLIP/PPP IP und IPX) host- beziehungsweise terminalseitig in das X.25-Format und in das passende IP-Paket auf der WAN-Seite. Wie durchdacht das Konzept der niederbayerischen Routerschmiede ist, zeigen die Erweiterungen: Eine zweite Ethernet-Schnittstelle lässt sich ebenso realisieren wie der Backup über GPRS-Mobilfunk. Darüber hinaus ist die Software auf flexible Lösungen ausgerichtet: Die Linux-Plattform erlaubt die Integration von ADSL via PPP over Ethernet genauso wie die weitere Anpassung an IPSec

beziehungsweise IPv6. Als weiteres Feature dient ein IP-X.25-Gateway, das die Umsetzung spezieller Datagramm-Formate erlaubt. Eingebaut ist auch die Sicherheit, die grundlegende Firewall-Funktionen und Netzwerk Adress Translation (NAT) anbietet.

Wichtiges Argument: Kosten sparen im Netz

Um die Kostenvorteile der Internet-Variante aufzuzeigen, soll das unten dargestellte Beispiel dienen, das in der Tabelle übersichtlich zusammengefasst wurde: Zehn Terminals greifen auf eine Zentrale zu. Im Ausbau mit Datex-P verfügt die Zentrale über einen Host-Anschluss mit 64 kBit/s, während die Terminals über Hauptanschlüsse verfügen. Alternativ zu der reinen Datex-P-Variante führen wir hier noch die weitverbreitete und kostengünstigere Datex-P-ISDN-Variante auf. Hier wird der D-Kanal des ISDN für die Datenübermittlung eingesetzt. Um die Berechnungsbeispiele einfach zu halten, gehen wir von einem Datenaufkommen unter einem MByte aus.

Verglichen mit den beiden Varianten wird der reine Internet-Anschluss der ISDN-Leitungen für die Übermittlung genutzt. Deshalb benötigen alle Niederlassungen und die Zentrale einen ISDN-Anschluss. Wir setzen hier die einfachste Variante Internet-Call-by-Call an. Bei Minutenpreisen von 2 Cent und jeweils 10 Minuten Verbindungsdauer pro Tag summieren sich etwa 40 Euro für alle Filialen im Monat auf. Zusammen mit der Zentrale gehen wir von pauschal 80 Euro für die Verbindungskosten aus.

Datenkommunikation effektiv genutzt

Diese Technik lässt sich überall dort einsetzen, wo bisher teure Datenverbindungen für die Verbindung zwischen Terminal und Host eingesetzt werden. Dies ist beispielsweise in Reisebüros der Fall, wo mehrere Mitarbeiter die Buchungssysteme bedienen. Oft sind in diesen Büros Lotterieterminals angeschlossen, um bereits vorhandene Anlagen besser auszunutzen. Für solche Anwender liefert der Router R1650 neben den klassischen X.25-Diensten zusätzlich einen Internet-Zugang.
Alarmsysteme und Geldautomaten nutzen ebenfalls X.25-Techniken. Darüber hinaus verwenden Rechenzentren, Tankstellenbetreiber, Logistik- und Industrieunternehmen die beschriebenen Übertragungsarten. Sie alle profitieren von dem Mehrwert der IP-X.25-Integration und vermeiden dadurch erhebliche Zusatzkosten für weitere Geräte.

Fazit: Die Zeit ist reif für kostensparende Alternativen

Derzeit gilt für IT-Projekte vorrangig ein Ziel: Kostensenkung! Alles, was nicht unmittelbar zu Einsparungen führt, wird auf die lange Bank geschoben. Aus diesem Grund haben Migrationskonzepte für Datenanwendungen Hochkonjunktur. Immerhin lassen sich dadurch riesige Summen an unnötigen Ausgaben reduzieren. Trotz aller Euphorie über die möglichen Einsparungspotentiale darf ein Punkt nicht vernachlässigt werden: Die Sicherheit, die mittlerweile auch im Internet ein hohes Niveau erreicht hat. Hier haben die *TDT*-Entwickler mit dem Router R1650 ganze Arbeit geleistet. Das neue Paradepferd liefert Kostenvorteile, ohne in die funktionierende X.25-Strukturen einzugreifen.
Der Router R1650 ist der richtige Baustein zum richtigen Zeitpunkt, den *TDT* im Rahmen seiner künftigen, umfassenden Routerserie anbietet. Die kostengünstige IP-Datenübermittlung mit höchstem Sicherheitsstandard wie bei X.25 wird für alle Anwender und für alle Anforderungen optimal angeboten.

Anbindung über Datex-P	
Datex-P 64 k Hostanschluss	613,55 Euro
Datex-P 9600 monatlich	240,30 Euro
Zehn Filialen mit Datex-P 9600	2403,00 Euro
Gesamtkosten pro Monat	3256,85 Euro
Alternative Internet	
ISDN-Grundgebühr	23,84 Euro
Monatliche Grundgebühr (zehn Filialen und eine Zentrale)	238,40 Euro
Verbindungsgebühren Internet-Call-by-call (2 Ct/min) pauschal	80,00 Euro
Ersparnis:	
Monatliches Einsparpotential gegenüber Datex-P	**2914,61 Euro**

Schnell erzielbare Kostensenkung: Schon bei zehn Filialen erzielt die Internet-Alternative monatliche Einsparungen von fast 3.000 Euro pro Monat gegenüber der reinen X.25-Variante

ANSPRUCHSVOLLE LÖSUNGEN - MADE BY T.D.T.

Vorgestellt von Thomas Maier, Leiter Produktmanagement

Flexibilität und Kundenorientierung sind für *TDT* die Grundlagen erfolgreicher Entwicklungsarbeit. Der dynamische Markt forderte in den letzten Jahren die Soft- und Hardwareentwickler zu außergewöhnlichen Leistungen, um die kundenspezifischen Anforderungen mit maßgeschneiderten Produkten erfüllen zu können. Das Resultat kann sich sehen lassen: Die Palette der fertigen Hardware- und Softwaremodule umfasst zunehmend die Datenerfassung und deren gesicherte Übermittlung.
Aus der zwar leistungsfähigen aber reinen „Protokollkonverter-Entwicklung im Hause *TDT* kristallisierte sich eine ISO 9001 zertifizierte R&D Abteilung heraus. Neben der Datenerfassung und der Fernwirktechnik spielt die Umwandlung verschiedener physikalischer Größen in digitale Daten, deren Übertragung und gegebenenfalls die Wiederherstellung, eine tragende Rolle.

Das über 20 Jahre angesammelte Know-how zahlt sich bei den neuen Anforderungen in vielfältiger Weise aus. Spezialisten für die unterschiedlichsten Schnittstellen zur Datenübertragung arbeiten in kleinen Gruppen mit hochspezialisierten Softwareentwicklern zusammen, um die kundenspezifischen Anforderungen in den Geräten und OEM-Modulen zu implementieren.
Aktuelles Beispiel: Die anspruchsvolle Entwicklung einer Anlage zur gemischten Kommunikation für Sprache und Daten in digitaler sowie analoger Form ist abgeschlossen und bei den Kunden im erfolgreichen Feldtest. Das Gesamtsystem besteht aus fünf verschiedenen Komponenten. Um die simultane Kommunikation von Menschen und Maschinen über eine gemeinsame 2-Draht Verbindung lösen zu können, entwickelte *TDT* Elemente zur Sprachkommunikation mit mehreren Freisprechstellen in geschlossenen Räumen und die gleichzeitige Fernsteuerung einer Maschinenanlage. Speziell entwickelte Komponenten ermöglichen den Zugriff von einem zentralen System weltweit über Modem und ISDN Verbindungen. Ein dafür geeignetes Gerät war bisher nicht auf dem Markt verfügbar.
Die „Hausbox“ von *TDT* stellt einen weiteren Meilenstein für die Erfassung und Übermittlung von Daten dar. Mit ihren digitalen und analogen Schnittstellen und der Übertragung der Daten über ISDN oder ein eingebautes Telefonmodem überwacht diese Box z.B. Temperaturen oder Füllstände und kann gleichzeitig bestimmte Schaltzustände (z.B. einer Heizung oder Pumpe) übertragen.
Ein intelligentes Baukastensystem gewährleistet die effektive und vor allem schnelle Entwicklung weiterer kundenspezifischer Funktionen. Innerhalb weniger Tage konnte der OEM TA Phone dem Kunden präsentiert werden. Dieses kleine Gerät erfasst Videodaten einer Kamera über die Ethernetschnittstelle und sendet sie in das ISDN-Netz. Parallel dazu kann der Anwender auf dem zweiten B-Kanal die eingebaute Freisprecheinrichtung benutzen. Der eingebaute parallele, acht datenbit breite, Port lässt die Fernsteuerung von einer Videokamera überwachten Ereignisse zu.

Die wichtigsten Datenübertragungsschnittstellen
und die dazu möglichen Datenübertragungsprotokolle.
Die Einteilung in elektrische Eigenschaften oder die Anpassung auf kundenspezifische Varianten oder Sonderformen ist ohne großen Aufwand möglich. Grundsätzlich kann man sie in synchrone oder asynchrone Schnittstellen einteilen. Entsprechend dieser Klassifizierung gibt es ebenso synchrone oder asynchrone Protokolle bzw. Prozeduren.

	Schnittstellen	TTL	RS 232	X.21/ V.11	V.35/ V.36	RS 485	TTY	DECT	GSM/ GPRS	ISDN S0/ I.430	ISDN Uk0/ Upn	ISDN E1/ T1 S2M	Ethernet 10/100
Asynchrone Protokolle	X.3/ X.28/ X.29	•	•	•	/	•	•	•	•	/	/	/	/
	PPP/ MLPPP	•	•	•	/	•	•	•	•	/	/	/	/
	AMP	•	•	•	/	•	•	•	•	/	/	/	/
	RS 485 Bus	•	/	/	/	•	•	•	•	/	/	/	/
	Async. X.25	•	•	•	/	•	•	•	•	/	/	/	/
Synchrone Protokolle	HDLC/ SDLC	•	•	•	•	/	/	/	/	•	•	•	/
	PPP/ MLPPP	•	•	•	•	/	/	/	/	•	•	•	/
	X.25	•	•	•	•	/	/	/	•	•	•	•	/
	X.75 Ebene 3	•	•	•	•	/	/	/	/	•	•	•	/
	X.31	/	•	•	•	/	/	/	/	•	•	•	/
	Frame Relay	•	•	•	•	/	/	/	/	•	•	•	/
	DSS1	/	/	/	/	/	/	/	/	•	•	•	/
	TCP/IP	•	•	•	•	/	/	/	/	•	•	•	•
	Voice	•	•	•	•	/	/	/	•	•	•	•	/

Da alle Module bei *TDT* streng nach den ISO-Schichtenmodell entwickelt wurden, können Sie in alle Protokollimplementierungen eingreifen und Anpassungen vornehmen. Darüber hinaus können die Nutzdaten aus nahezu allen Prozeduren entnommen und in andere Protokolle eingesetzt werden. Zumindest aber können die verschiedensten Datenübertragungsprotokolle mittels anderer transportiert oder „getunnelt“ werden.
Die Tabelle zeigt eine Übersicht der gängigsten Protokolle, die in andere transportiert bzw. „getunnelt“ werden können. Sämtliche Nutzdaten und bei Bedarf auch die sie umgebenden Header werden am Endpunkt der Übertragung wiederhergestellt.

	Protokolle	X.3/ X.28/ X.29	PPP/ MLPPP async.	AMP	RS 485 Bus	Async. X.25	HDLC/ SDLC	PPP/ MLPPP sync.	X.25	X.75 Ebene 3	X.31	Frame Relay	DSS1	TCP/IP
Transportprotokoll, Asynchrone Protokolle	PPP/ MLPPP	•	/	•	•	•	•	•	•	•	•	•	•	•
	AMP	•	•	/	•	•	•	•	•	•	•	•	•	•
	RS 485 Bus	•	•	•	•	•	•	•	•	•	•	•	•	•
	Async. X.25	•	•	•	•	•	•	•	•	•	•	•	•	•
Transportprotokoll, Synchrone Protokolle	HDLC/ SDLC	•	•	•	•	•	•	•	•	•	•	•	•	•
	PPP/ MLPPP	•	•	•	•	•	•	•	•	•	•	•	•	•
	X.25	•	•	•	•	•	•	•	•	•	•	•	•	•
	X.75 Ebene 3	•	•	•	•	•	•	•	•	•	•	•	•	•
	X.31	•	•	•	•	•	•	•	•	•	•	•	•	•
	Frame Relay	•	•	•	•	•	•	•	•	•	•	•	•	•
	DSS1	•	/	/	/	/	/	/	/	/	/	/	/	/
	TCP/IP	•	•	•	•	•	•	•	•	•	•	•	•	•

Eine Applikation liefert ihre Daten in dem synchronen X.25-Protokoll. Über ein Gatewaymodul können die Nettodaten auf eine TCP-Session abgebildet werden. Alternativ dazu kann das gesamte X.25 innerhalb des TCP transportiert werden (XOT, X.25 over TCP). Applikationen der Fernwirktechnik oder der Fernsteuerung bzw. Fernabfrage beziehen ihre Informationen in der Regel aus analogen oder digitalen Signalen. Analoge Signale, z.B. Temperatur oder Druck, müssen mit geeigneten Wandlern der Anforderung gemäß zuerst digitalisiert werden. Die daraus resultierenden digitalen Werte werden über geeignete Protokolle übertragen. Die hohe Verfälschungssicherheit wird mittels Prüfsummen und anderen Mechanismen erreicht. Je nach Anwendung werden die Daten am Zielpunkt ausgewertet und weitere Aktionen wie Alarme, SMS oder andere Benachrichtigungen ausgelöst. Varianten der Eingangs- bzw. der Ausgangsbeschaltungen ermöglichen nahezu uneingeschränkte Variationen und Kombinationen der Datenkonvertierung und des Datentransports.

	Applikations Schnittstellen	Parallel I/O	A/D D/A Wandler	4...20mA	0...10 Volt	Voice	Video	Kunden Spez.
Asynchrone Protokolle	X.3/ X.28/ X.29	•	•	•	•	•	•	•
	PPP/ MLPPP	•	•	•	•	•	•	•
	AMP	•	•	•	•	/	•	•
	RS 485 Bus	•	•	•	•	/	•	•
	Async. X.25	•	•	•	•	/	•	•
Synchrone Protokolle	HDLC/ SDLC	•	•	•	•	•	•	•
	PPP/ MLPPP	•	•	•	•	•	•	•
	X.25	•	•	•	•	/	•	•
	X.75 Ebene 3	•	•	•	•	/	•	•
	X.31	•	•	•	•	/	•	•
	Frame Relay	•	•	•	•	•	•	•
	DSS1	•	•	•	•	/	/	•
	TCP/IP	•	•	•	•	•	•	•

Virtual Private Network (VPN)

Teil 2

Lösungen mit IPSec – ein investitionssicheres System zur Realisierung von kostengünstigen, flexiblen Unternehmensnetzen

Safety first, Know-how second

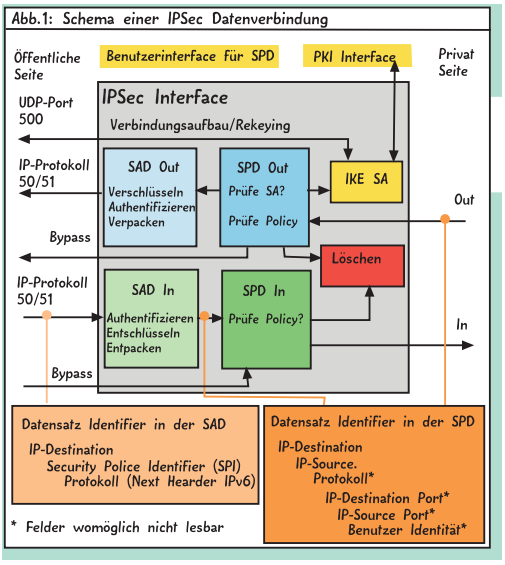
Nachdem im Teil 1 die Kostenvorteile von Virtual Privat Networks und die Sicherheitsaspekte von IPSec aufgezeigt wurden, widmet sich Teil 2 den technische Details von IPSec.

3. IPSec im Detail, Bausteine und Verfahren

Mit Security Policy Database und der Security-Association Database wird ein Modell nach [6] beschrieben wie sich ein IPSec Interface nach außen verhalten muss. Die detaillierte Ausführung ist herstellerabhängig. Damit kann ein Benutzerinterface für die SPD und SAD alles sein, von einem Texteditor bis zu einer menügesteuerten Browserapplikation. IKE dient zum Verbindungsaufbau und zur Authentifizierung des Netz-werkdevices. Die Protokoll Authentification Header (AH) und Encapsulating Payload dienen zur sicheren Datenübertragung mit unterschiedlichen Sicherheitsansprüchen und werden nachfolgend beschrieben.

3.1 Security Policy Database (SPD)

In der SPD werden Sicherheitsrichtlinien hinterlegt. Ein SPD-Eintrag ist ein Filterkriterium, das auf den gesamten IP-Verkehr anzuwenden ist. Zur Definition des Filters werden die Felder IP-Destination- und IP-Source-Adresse, Source*- und Destination-Port* und Protokoll* (oder Next Header bei IPv6) verwendet. Die mit * gekennzeichneten Felder können unter Umständen verschlüsselt und damit nicht lesbar sein. Für alle Felder sind



Wildcards zulässig. Natürlich können IP-Netzadressen oder Hostadressen konfiguriert werden. Die detaillierte Umsetzung der Benutzerschnittstelle bleibt dem Hersteller überlassen [7]. Die Richtlinien, oder besser die Filterkriterien, bestimmen ob IP-Datagramme weitergeleitet, verworfen oder durch ein IPSec Verfahren zu behandeln sind. Ist IPSec gefordert, dann zeigt der Eintrag auf einen Datensatz in der Security-Assosiation Datenbank (SAD). Dort sind die anzuwendenden IPSec-Verfahren genau beschrieben. Ist kein Eintrag in der SAD vorhanden kann mit dem Internet Key Exchange Protokoll (IKE) ein dynamischer SA Datensatz erstellt werden. IKE regelt den dynamischen Verbindungsaufbau und die gegenseitige Authentifizierung der Kommunikationspartner. Daten von der öffentlichen Seite werden zuerst authentifiziert und entschlüsselt, gegebenenfalls entpackt (siehe Abb. 1). Danach erfolgt eine Prüfung, ob das Vorgehen mit den in SPD hinterlegten Richtlinien übereinstimmt. Erst bei einer Übereinstimmung wird das Datagramm auf der privaten Seite weitertransportiert. Bei zu versendenden Daten ist es umgekehrt, der SPD-Eintrag verweist auf den Eintrag in der Security Association Database. Existiert kein Eintrag, dann wird mit IKE ein Eintrag in die SAD generiert, andernfalls wird das IP-Datagramm gelöscht. Ein SPD-Eintrag kann auf mehrere SAD-Einträge verweisen, damit ist ein Verschachteln der IPSec-Verfahren möglich.

3.2 Security Association Database (SAD)

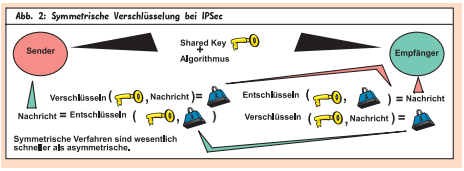
In dieser Datenbank werden alle nötigen Informationen für eine IPSec-Verbindung gespeichert. Jedes eingehende Datagramm wird laut SA-Eintrag überprüft, entschlüsselt, ggf. entpackt. Stimmt das/die Verfahren für das Datagramm mit einem Eintrag in der SPD überein, wird es weitergeleitet. In der umgekehrten Richtung verweist ein SPD-Eintrag auf eine oder mehrere SA. Die Datagramme werden laut SA verschlüsselt und gegebenenfalls eingepackt bevor sie über das öffentliche Netz transportiert werden. Für Tunnel Mode SA müssen natürlich die Adressen für den Outer-IP-Header gespeichert sein. Die Headerkonstruktion für die IPSec Protokolle AH und ESP sind in [7], [8], [9] beschrieben. Folgende Angaben werden in einer SA für die Bearbeitung der Datagramme laut [7] vorgeschrieben:

- Authentifizierungs-Algorithmus und Schlüssel für AH
- Verschlüsselungs-Algorithmus und Schlüssel für ESP
- Authentifizierungs-Algorithmus für ESP
- Lebenszeit der SA (Datenmenge in Kilobytes und Zeit in Sekunden, das zuerst erreichte Kriterium löst aus).
- Replay-Schutz (nur in Verbindung mit IKE)
- Encapsulation Mode, Tunnel oder Transport

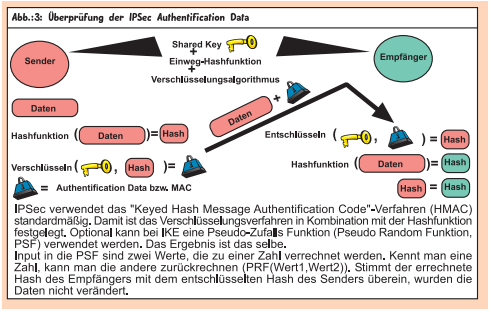
Weitere Details sind in der „Internet IP Security Domain of Interpretation for ISAKMP“ (DOI) [3] festgelegt. Eine SA ist immer für eine Transportrichtung zuständig (siehe Abb.1). Damit sind mindestens zwei SA für eine bidirektionale Kommunikation notwendig. Die Datenfelder für die eindeutige Zuordnung der SA sind IP-Destination-Adresse, Security Parameter Index (SPI) und das Protokoll AH oder ESP. Die SPD-Einträge werden in Transport- und Tunnel-Mode unterteilt. Ein automatischer Verbindungsaufbau, Replay-Schutz und Perfect Forward Secrecy ist nur mit IKE möglich. Ein rechtzeitiges Etablieren einer neuer SA durch IKE (inkl. Schlüssel) verhindert ein Überlaufen der Packet-Counter.

3.3 Verfahren für die Verschlüsselung, Integritäts- und Authentizitätsprüfung von IPSec Datagrammen

Bei IPSec werden zur Verschlüsselung des Datenstroms symmetrische Verschlüsselungsverfahren angewendet. Diese Verfahren sind schneller als asymmetrische Verfahren.



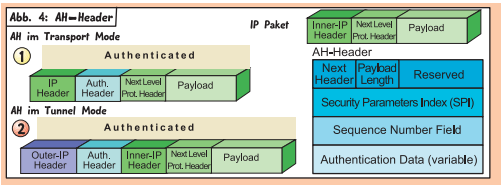
Auch das Integrity Check Value (ICV) wird symmetrisch verschlüsselt. Auf beiden Seiten sind die nötigen Schlüssel und Algorithmen in den SA hinterlegt. Für die Integritätsprüfung wird ein Hash über die Daten berechnet. Eine Hash-Funktion liefert einen Wert gleicher Länge unabhängig von der Länge der Eingangsdaten. Der Hash der Daten ist so eindeutig wie ein Fingerabdruck. Die Daten können daraus nicht rekonstruiert werden. Der Empfänger überprüft den entschlüsselten Hash mit dem berechneten Hash der empfangenen Daten. Stimmen die Hashwerte überein, wurden die Daten nicht verändert. Gleichzeitig ist durch die



erfolgreiche Überprüfung die gegenseitige Authentizität der Partner gegeben, da die Schlüssel nur den Kommunikationspartnern bekannt sind.

3.4 Authentification Header

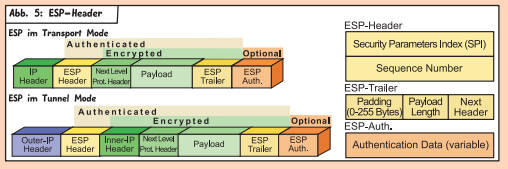
Mit dem AH-Header wird der Gegenstelle ein SPI und ein Packet-Counter für den Replay-Schutz übermittelt. Zur Sicherstellung der Integrität und Authentizität der Partner wird ein Hash über die Daten gebildet. Dieser Hash wird zusätzlich mit einem symmetrischen Verfahren verschlüsselt und als „Authentification Data“ übermittelt. Die Gegenstelle überprüft die Daten mit den durch die SA definierten Verfahren (referenziert durch SPI, Dest.-IP, Protokoll bzw. Next Header in IPv6). Die Protokollnummer für AH ist 51. Mit AH wird der IP-Header und auch der Outer-IP-Header im Tunnel Mode in die Hashberechnung mit einbezogen. Damit ist eine Änderung des IP-Headers nicht möglich. Network



Address-Translation-Verfahren ändern den IP-Header. Eine AH-Verbindung zur Gegenstelle kann nicht durch ein NAT Interface aufgebaut werden. Details zur NAT-Problematik werden in „IPSec und NAT“ erläutert. Das AH-Verfahren verschlüsselt nicht. Für Dateien die keiner Geheimhaltung unterliegen, z.B. Binärdateien, Gesetzestexte usw., reicht AH aus. Denn mit AH wird garantiert, dass die Daten von der richtigen Institution kommen und nicht verändert wurden.

3.5 Encapsulating Security Payload

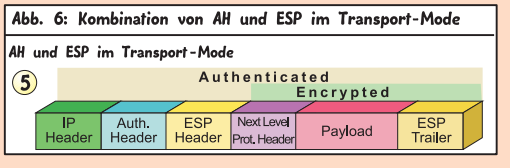
Bei diesem IPSec-Verfahren werden ein ESP-Header, ein Trailer und optional ESP-Authentification-Daten zum ursprünglichen IP-Datenpaket hinzugefügt. Im Feld „Next Header“ wird die



Protokollnummer des verschlüsselten IP-Datagramms laut [10] eingetragen. Die Felder Padding und Payload werden für Verschlüsselungsverfahren benötigt, welche nur feste Blockgrößen verarbeiten können. Im ESP-Header ist unverschlüsselt der SPI und die Sequenznummer eingetragen. Im IP- bzw. Outer-IP-Header wird die Protokollnummer 50 für ESP eingetragen. Das Next Header-Feld im ESP-Trailer ist verschlüsselt und kann nicht ausgewertet werden. Das Datagramm wird überprüft und entschlüsselt. ESP benutzt symmetrische Verschlüsselungsverfahren. Bei ESP wird zur Datenintegritätsprüfung der IP-Header nicht mit einbezogen. Damit kann ESP-Datenverkehr durch ein NAT-Interface übertragen werden.

3.6 Kombination von SA

AH und ESP können beliebig kombiniert werden. Im Transport Mode werden die AH- und ESP-Header hinter dem orginal IP-Header eingesetzt. Im Tunnel-Mode vor dem original IP-Header (Inner-IP) und nach dem äußeren IP-Header (Outer-IP). Die in Abb. 4, 5, 6 dargestellten Kombinationen sind nach [7] für



Hostimplementierungen zwingend. Für Gateways ist nur Tunnel Mode vorgeschrieben. Über einen Tunnel zwischen zwei Gateways können natürlich auch IPSec Daten transportiert werden. Damit ist eine IPSec-Verbindung zwischen zwei Hosts auf beiden Seiten des Gateways im privaten LAN möglich. Nicht jede Kombination ist sinnvoll. Manche Kombinationen sind uneffektiv, z.B. ESP mit Authentifizierung in einem AH-Tunnel.

3.7 Internet Key Exchange Protocol (IKE)

Das IKE-Protokoll, früher als ISAKMP/Oakley bekannt dient zum automatischen Aufbau von IPSec-Verbindungen. Die Verfahren zur Authentifizierung und Verschlüsselung werden nach den zugrundeliegenden Sicherheitsrichtlinien in der SPD mit der Gegenstelle über den UDP-Port 500 ausgehandelt. Nach der Authentifizierung steht ein sicherer Verbindungskanal zur Verfügung. Über diese Verbindung werden die SA für die IPSec-Datenverbindung ausgetauscht. Details zu IKE werden in „Automatische Verteilung von Sicherheitsvereinbarungen und Schlüssel mit IKE“ diskutiert.

Literatur:

[1] Infonetics Research, “Virtual private Networks“, 1997

[2] W. Townsley, A. Valencia, “Layer Two Tunneling Protocol L2TP”, RFC 2661, Aug. 1999

[3] D. Piper, “The Internet IP Security Domain of Interpretation for ISAKMP”, RFC 2407, Nov.1998

[4] M. Baer, R. Charlet, W. Hardaker, “IPsec Policy Configuration MIB”, Draft, Juli 2001

[5] Man Li, David Arneson, Nortel Networks, “IPSec Policy Information Base”, Draft, Juli 2001

[6] L.A. Sanchez, H. Orman, “A Roadmap for IPSec Policy Management”, Draft, Nov. 2000

[7] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, Nov. 1998

[8] S. Kent, R. Atkinson, “IP Encapsulating Security Payload (ESP)”, RFC 2406, Nov. 1998

[9] S. Kent, R. Atkinson, “IP Authentication Header”, RFC 2402, Nov. 1998

[10] J. Reynolds, J. Postel, “ASSIGNED NUMBERS”, RFC 1700, October 1994

[11] Bernard Aboba, “IPSec-NAT Compatibility Requirements”, Draft, June 2001

[12] T. Kivinen, M. Stenberg, “Negotiation of NAT-Traversal in the IKE”,

Nachwuchs im Hause Pickhardt

Stolz zeigten Sabine und Michael Pickhardt der *TDT*-Belegschaft ihren Sprössling Luca im *TDT*-Gebäude. Dabei gingen die Meinungen der Mitarbeiterinnen und Mitarbeiter bei einer gemütlichen Feier auseinander, ob der kleine Luca mehr der Mama oder mehr dem Vater ähnlich sieht. Einig waren sich jedoch alle, dass der Junge schon von klein auf neben der elterlichen Erziehung auch schon erste Team-Erfahrung im Hause *TDT* sammeln muss.

Siegfried Vogl - Leiter der Entwicklung

Das *TDT*-Urgestein realisierte mit seinem Team innerhalb kürzester Zeit ehrgeizige Ziele: Die Entwicklung der neuen *TDT*-Routerfamilie mit konsequenter Ausrichtung in Richtung VPN und IPSec. Dies schließt nahtlos an die bisherige *TDT*-Philosphie an, Projekte akribisch zu planen und zu systematisieren. Unter diesen Voraussetzungen kann sich ein hochdynamisches Team nicht nur schnell, sondern auch mit dem entsprechenden Weitblick mit absehbaren Kundenanforderungen auseinander setzen und ein verlässlicher Partner sein. Das Ziel ist somit schon gegeben: Statt Ad hoc-Entwicklungen zu betreiben, konzentriert sich die *TDT*-Entwicklung schon im Vorfeld auf künftige Anforderungen, wie die Migration neuer Software in vorhandene Technik und baut somit stabile Partnerschaften auf.

Das klare Bekenntnis zur gezielten Nachwuchsförderung zeigt schon erstaunliche Früchte. Informatik-Studenten als Praktikanten und freie Mitarbeiter wird nicht nur Wissen unter Federführung erfahrener *TDT*-Entwickler vermittelt. Es kommt auch erstaunliches Feed-back zurück. Die Einbindung der jungen Entwickler in das produktive *TDT*-Team ist im wahrsten Sinne des Wortes nur noch eine formale Angelegenheit.

Editorial

Sie, als aufmerksame Begleiter von SWITCHED, haben es schon seit längerer Zeit bemerkt. *TDT* entwickelt sich parallel der IT-Innovationen und setzt verstärkt auf das Internet. Das oberste *TDT*-Prinzip wird dabei noch konsequenter als bisher durchgesetzt: Ob X.25, ISDN-Dienste oder Internet, wir suchen permanent den Draht zu unseren Kunden, um die aus dem Boden schießenden IT-Entwicklungen auf ihre Anforderungen prüfen zu können. Jede neue Innovation erfordert Spezialisten für Hard- und Software, so zum Beispiel bei IPSec. Dieser Prozess muss permanent koordiniert werden, um zukunftsweisende und plattformübergreifende Systeme in zum Teil vorhandene Systeme implementieren zu können. Damit dieses Ziel auf direktem Wege erreicht wird, hat *TDT* die Entwicklungsabteilung neu strukturiert, bzw. die Stelle des Produktmanagers eingeführt. Ihm kommt eine zentrale Bedeutung zu: Die Bedürfnisse des Marktes erkennen, die Umsetzbarkeit neuer Technologien prüfen und die Koordination zwischen Entwicklung, Technik und Vertrieb leiten. Flexibilität, verknüpft mit strategischem Weitblick, ist dabei die Messlatte für neue Produkte. Die Feuertaufe können Sie auf der CeBIT erleben: Den neuen *TDT*-Router R1650.

Auf ein Wiedersehen und auf Ihre Meinung freut sich
Thomas Maier - Leiter Produktmanagement

Einladung zur CeBIT 2002

„The same procedure as every year." Kann die CeBIT die hohen Erwartungen erfüllen?

Die doch etwas unter die Räder gekommene EDV- und IT-Branche hofft auf die CeBIT als Initialzündung für neue Investitionsschübe. Die Führungsetagen aller Global Player und die Riege der mittelständischen Unternehmen wissen nur zu gut, dass die Wachstumseuphorie innerhalb eines Jahres erheblich nachgelassen hat. Die Einkäufer ordern nicht jede neue Entwicklung, nur weil sie leistungsfähiger, schneller oder bequemer zu bedienen ist. Investitionen und Kosten werden sehr wohl gegeneinander mit spitzem Bleistift aufgerechnet. Oder in den Worten des Finanzministers Hans Eichel ausgedrückt: Die Etats für Telekommunikation sind in den Unternehmen auf Kante genäht. Da macht es schon Sinn, nach der Rentabilität der neuen Leistungen zu fragen. Darauf kommt *TDT* auf der CeBIT gerne bei der Vorstellung des neuen Routerkonzeptes zu sprechen: Kostenreduzierung durch Minimieren der Übertragungskosten und Migration vorhandener Technik. Dass die „Erfinder" des DCC's auch im Bereich TCP/IP für Furore sorgen werden ist gewiss. Das neue Routerflaggschiff R1650 wird modular aufgebaut, damit unsere Kunden einen auf ihre Bedürfnisse ausgerichteten Router ordern können. Dass neben allen üblichen Features VPN und IPSec standardmäßig integriert sind, lässt auch Internet-Skeptiker aufhorchen. Diese Maxime gilt natürlich auch für alle weiteren *TDT*-Innovationen mit Migrationsoptionen. In welchen Geräten neue Features eingebaut worden sind, erläutern wir Ihnen gerne in Halle 1 Stand 8k4 - und die echte bayerische Brotzeit ist in dieser Einladung natürlich eingeschlossen.

Herzlichst

Michael Pickhardt *Jürgen Büttner*

Wolfgang Wanner leitet die T.D.T.-Doku-Abteilung

Er bringt exakt die Voraussetzungen mit, die für diese Stelle so wichtig sind, so einhellig die Meinung seiner Kollegen über Wolfgang Wanner. Der Weg seit 1994 im Hause *TDT* prägten sein Verständnis für die Fragen und Probleme der Anwender. Praktische Erfahrungen bei den hauseigenen Qualitätstests und die langjährige Position für alle Hardwarekonfigurationen des kompletten *TDT*-Hausnetzes und der dazugehörigen Software sind die besten Voraussetzungen, komplexe Aufgabengebiete einfach beschreiben zu können. In diesem Sinne wird Wolfgang Wanner verantwortlich die *TDT*-Doku-Abteilung leiten. Besonderen Wert legt der Hobbykoch dabei auf den optimalen Mix der verschiedenen Informationsträger wie Papier, CD-ROM und Internet und auf die durchgängige Visualisierung der Themen in allen Medienbereichen.

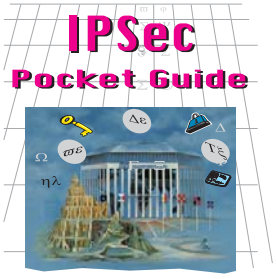
Wolfgang Wanner an seinem Arbeitsplatz. Zu seinem Aufgabenbereich gehört auch der Aufbau und Pflege des TDT-Internetauftrittes.

Meine Nr. 1

Essen	Gebratene Ente
Film	Don Camillo und Pepone
Hobby	Hund, Zigarren, Technik allgemein
Farbe	Blau
Schauspieler	Steve McQueen
Song	Take me home Country roads (J. Denver)
Getränk	Adlkofener Südbach-Qualitätsbohrung

Der neue IP-Pocket-Guide ist ab sofort verfügbar

Viele haben darauf gewartet - auf den neuen, kompetenten Begleiter im Taschenformat. Der laminierte IPSec-Pocket-Guide setzt die Reihe der erfolgreichen *TDT*-Reihe fort und kann ab sofort gegen die Schutzgebühr von 3 Euro bei *TDT* angefordert werden. Auf der CeBIT erhalten Sie ihn kostenlos - **ebenso senden wir ihn allen, die auf unsere Fragen zur Switched antworten, kostenlos zu.**



Erste Erfahrungen auf der SPS waren sehr positiv

Der Trend ist irreversibel: Automatisierungs- und Maschinensteuerungen werden immer mehr weltweit vernetzt und benötigen so zuverlässige Datenverbindungen. Hat bis vor kurzem die Branche hier noch auf ISDN und herkömmliche Netze gesetzt, so ist die Datenübertragung über IP ein hoch beachtetes Thema auf der SPS in Nürnberg gewesen. Die vielen aufschlussreichen Gespräche bestätigten die ausgezeichneten Perspektiven für das *TDT*-Engagement in diesem Bereich.

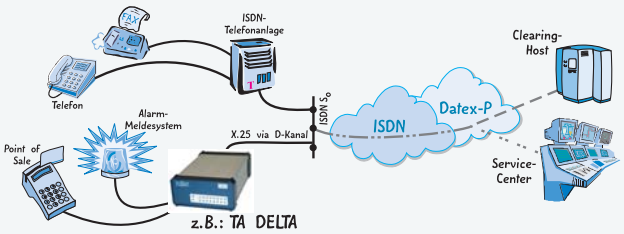
Nicht vergessen:

Bestimmen Sie, in welcher Form die Switched künftig erscheinen soll. Bitte unbedingt antworten!

ISDN goes Datex-P

Datex-P ISDN Access - Zugang zum Datex-P via ISDN D-Kanal

Interaktive Anwendungen erfordern meist Verbindungen über längere Zeit, auch wenn das zu übertragende Datenvolumen relativ klein ist. Mit dem Datex-P ISDN Access fallen durch den Zugang zum Datex-P Datennetz unter Verwendung des ISDN D-Kanals die zeitabhängigen Übermittlungsgebühren des Telefonnetzes weg. Dieser Kanal ist bei jedem ISDN-Anschluss verfügbar und wird ausschließlich für die Signalisierung verwendet (Verbindungsaufbau etc.). Mit einer Kapazität von 16 Kbit/s ist der ISDN D-Kanal bei weitem nicht ausgelastet und bietet sich für eine zusätzliche Nutzung zur Übertragung von Daten (max. 9,6 Kbit/s) geradezu an. Datex-P ISDN Access kann bei allen neuen und bestehenden ISDN Basisanschlüssen (EURO-ISDN) freigeschaltet werden.



Zusammenarbeit mit I•T•E•N•O•S

Der *TDT*-Service

Ob ISDN oder Datex-P ISDN Access, wir übernehmen für Sie die Anmeldung und das Ausfüllen aller erforderlichen Formulare und leiten diese an I.T.E.N.O.S. weiter. I.T.E.N.O.S. betreibt „im Auftrag der Deutschen Telekom" exklusiv diese Dienste.

Eine Auswahl möglicher Anwendungen:

Handel
EC.Cash, Sicherheit, Warendispositionen, Bestandsabfragen u.v.m.

Tankstellen
EC-Cash, Füllstände, Messen, Steuern u.v.m.

Sicherheit
Feuer, Wasser, Gas, Überfall (bis VdS-Klasse C zertifiziert)

Fernwirken
Ablesen von Zählern/Füllständen, Steuern und Messen

SoHo
Anbindung von Außendienstmitarbeitern

IMPRESSUM

Herausgeber	T.D.T. Transfer Data Test GmbH Siemensstraße 18 84051 Essenbach Tel. +49 (0) 8703 9 29-00 Fax +49 (0) 8703 9 29-201 E-Mail info@tdt.de http://www.tdt.de
Verantwortlich für den Inhalt	Michael Pickhardt, Geschäftsführer und Jürgen Büttner, Vertriebsleiter
Gesamtproduktion	Werbeagentur J. Wimmer Ulmenstraße 21 84051 Essenbach Tel. +49 (0) 87 03 9 13 60 Fax +49 (0) 87 03 9 13 61
Auflage	12.000 Exemplare
Ausgabe 1/2002	Auf Umweltpapier gedruckt