**Zeitschrift:** Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

**Herausgeber:** Swisscom

**Band:** 79 (2001)

**Heft:** 4

**Rubrik:** News

### Kontrast von LCDs verbessern

Durch eine spezielle Anordnung von verzweigten dreidimensionalen Flüssigkristallen wollen niederländische Forscher der Eindhoven University of Technology die Helligkeit und den Kontrast von LCDs (Liquid Crystal Display) verbessern. Die neuen Moleküle können in einer nur fünf Mikrometer dicken elektro-optischen Zelle so angeordnet werden, dass sie je nach Spannung mehr oder weniger Licht hindurchlassen. Die Transmissionsrate des Lichts lässt sich durch das Brechungsverhalten der Kristalle zwischen 20 und 80% variieren. Ein Display aus diesen Flüssigkristallen leuchtet heller und hat einen höheren Kontrast als die bisher verwendeten Polarisations-LCDs. Bei der heute verwendeten Technik wird die Lichtstärke durch die Polarisierung um bis zu 50% reduziert. Dabei wird polarisiertes Licht je nach Schaltung von den Kristallen hindurchgelassen oder verschluckt. Es erscheinen helle oder dunkle Punkte auf dem Display. Schon geringe Spannungen von 1 bis 1,5 V reichten aus, um die neuen Kristalle zwischen «hell» und «dunkel» zu schalten. Dabei ordneten sich die Moleküle innerhalb von einer halben Millisekunde aus. «Die ersten Ergebnisse sind sehr ermutigend», meint Forscherin Marysia van Boxtel. Dennoch seien noch weitere Forschungen nötig, um die neuen Kristalle für ein marktfähiges Produkt zu nutzen.
Homepage: www.tue.nl

### Erste Siliziumkarbid-Schottky-Dioden

Infineon hat die ersten Schottky-Dioden aus Siliziumkarbid vorgestellt. Solche Dioden ermöglichen deutlich geringere Schaltungsverluste und höhere Schaltfrequenzen als Dioden aus Silizium- oder Galium-Arsenid. Damit lassen sich nach Angaben von Infineon kleinere und kompaktere Schaltnetzteile mit hoher Zuverlässigkeit herstellen, die zusätzlich ohne Kühlkörper oder Lüfter auskommen. Für die Hersteller von Schaltelementen ermöglichen Schottky-Dioden aus Siliziumkarbid (SiC) den Einsatz von kleineren Transistoren oder passiven Bauelementen wie Spulen und Kondensatoren. Dadurch können die Systemkosten für Schaltelemente gesenkt werden. Der Halbleiter hat eine mit Kupfer vergleichbare thermische Leitfähigkeit. Deshalb ist das Material für hochsperrende Leistungsbauelemente geeignet. Diese Materialeigenschaften kommen in geringen Leckströmen, geringem On-Widerstand und hohen Stromdichten zum Tragen. So lassen sich SiC-Dioden mit einer Sperrspannung zwischen 300 und 3500 V realisieren. Infineon wird die SiC-Schottky-Dioden mit Sperrspannungen von 600 V und 300 V in verschiedenen Gehäusen anbieten. Die ersten Muster stehen bereits zur Verfügung. Die Serienfertigung soll im April anlaufen.



CyberKey®

# « Schlüssel zum sicheren Netzwerk »

**Das Thema Sicherheit wird in täglichen Geschäftsabläufen immer zentraler. Mit der Konzentration des Informationsaustauschs auf Datennetzwerken wird das Risiko der Datenkorruption, des Datenverlusts oder eines Angriffs kritisch. Für ein Unternehmen ist der Aufbau des nötigen Sicherheits-Know-how und die Gewährleistung des Betriebs der Infrastruktur sehr komplex, kostspielig und bindet zudem zusätzliche Ressourcen. Nebst Verschlüsselung sind Echtheit und Unverletzlichkeit der Informationen wichtige Bestandteile der Netzwerksicherheit. Diesen Anforderungen gerecht zu werden, ist das Ziel der von Swisscom lancierten CyberKey® Serviceoption.**

CyberKey® wird als so genanntes Site-to-Site VPN (Virtual Private Network), basierend auf dem bereits bestehenden LAN Interconnect Service (Local Area Network), angeboten und stellt so eine Lösung zur Verfügung, die den heutigen Sicherheitsanforderungen vollumfänglich gerecht wird. Dabei werden, vereinfacht gesagt, alle Daten, die das Haus verlassen, verschlüsselt über das WAN (Wide Area Network) zum Zielort transportiert und dort wieder entschlüsselt. CyberKey® erfüllt Sicherheitsanforderungen, indem den Kunden ein sicheres Netzwerk, das von Swisscom kontrolliert und betrieben wird, zur Verfügung gestellt wird.
Swisscom schützt die Kundendaten nicht nur vor der Aussenwelt, sondern auch von Seiten des Service Providers. CyberKey® liefert den Kunden einen Service für Datenverschlüsselung, der rund um die Uhr von Sicherheitsspezialisten überwacht wird.

### Vorteile von CyberKey®

CyberKey® bietet eine Reihe von Vorteilen, wie beispielsweise:
- Betrieb einer eigenen Public Key Infrastructure (PKI) inklusive allen nötigen baulichen Massnahmen.
- Proaktive Überwachung rund um die Uhr.
- Garantierte Leistungen durch Service Level Agreements.
- Anwendung von standardisierten Verschlüsselungs- und Authentifizierungsverfahren.
- Hohe Performance dank Hardware basierender Verschlüsselung.
- Skalierbare, stabile und bereits erprobte Lösung.
- Attraktives Pricing (Economy of Scale).
- Schweizweite Verfügbarkeit. 4

Info: Tel. 0800 800 900 oder Homepage: www.swisscom.com/business-solutions

SPHINX Personal Firewall

# « Schutz vor Angriffen aus dem internen Netz »

**Die Personal Firewall SPHINX ist eine Software-Lösung, die Desktop-PCs und Notebooks in lokalen und externen Netzen schützt. Mit diesem Programm verfügen Einzelrechner auch in unsicheren Netzen über flexible Abwehrmöglichkeiten gegen Hacker-Angriffe. Ohne eine Änderung der Sicherheits-Policy können Administratoren SPHINX einfach installieren und konfigurieren. SPHINX wird direkt auf dem Rechner installiert und sichert das Betriebssystem auf den unteren Netzwerkschichten ab.**

Die Firewall-Software verwendet einen NDIS (Network Device Interface Specification)-Treiber, der unterhalb der Netzwerkschicht des OSI (Open System Interconnection)-Schichtenmodells arbeitet. Auf dieser Vermittlungsschicht werden Datenpakete gesendet und empfangen. Direkt bei der Datenübermittlung kontrolliert SPHINX alle eintreffenden Informationen und filtert unautorisierte Datenpakete heraus. Dadurch sichert SPHINX Desktop-Rechner und Notebooks in Local Area Networks (LAN) und Wide Area Networks (WAN). Durch die Kombination verschiedener effektiver Abwehrmechanismen verhindert SPHINX, dass Angreifer in ein Computer-Netzwerk eindringen und unautorisiert auf den PC zugreifen. Mit der Personal Firewall können Administratoren Schutzfunktionen einer BIGfire+ auf dem Einzelrechner installieren. Angeschlossen über ISDN (Integrated Services Digital Network), Modem oder Netzwerkkarte verfügen Anwender auch im Home Office über eine gesicherte Anbindung mit BIGfire+ an ein öffentliches Netzwerk wie zum Beispiel das Internet. Nach individuellen Regeln sperrt SPHINX einzelne Dienste, beschränkt den Datenverkehr auf autorisierte Übertragungsprotokolle wie HTTP (Hyper Text Transfer Protocol). Während des Rechnerbetriebs lassen sich Datenpakete wie zum Beispiel Internet/Intranet (IP), Netware (IPX) and NetBEUI (NetBios Enhanced Interface) herausfiltern oder der gesamte Datenverkehr blockieren. Die Sicherheitsfunktionen der Personal Firewall wehren Angriffe ab, die gegen die Software gerichtet sind. SPHINX unterstützt in Zukunft die Management-Software BALI (Biodata Application Link Interface), über die Administratoren neue Konfigurationen, Sicherheits-Policies oder Software-Versionen zentral einrichten. Alle Biodata-Produkte lassen sich mit BALI verwalten. Die Personal Firewall unterstützt die Betriebssysteme Windows 98/NT/2000, sodass Anwender auch weiterhin die gewohnte Arbeitsumgebung verwenden können. Bereits die Grundversion von SPHINX wehrt Angriffsmethoden wie IP-Spoofing ab, bei denen Hacker eine vertrauenswürdige IP-Adresse vortäuschen, um in fremde Netzwerke einzudringen. ICMP (Internet Control Message Protocol)-Blocking unterbindet PINGs (Packet Internet Groper) und andere Anwendungen, die feststellen, ob eine bestimmte IP-Adresse zugänglich ist. Der integrierte SYN Flood Defender verhindert, dass der Rechner durch eine systematische Bombardierung mit Anfragen lahmgelegt wird.

### Virtual Private Networks (VPN)

Die Personal Firewall lässt sich auf eine leistungsstärkere Sicherheitslösung mit VPN-Funktionen ausbauen. Virtuelle private Netze ermöglichen es, in getrennten Netzwerken Informationen sicher auszutauschen. Anwender können mit SPHINX über einen verschlüsselten virtuellen Tunnel zu einer lokalen oder externen Firewall BIGfire+ kommunizieren. Auf diese Weise verbergen sie ihre Identität und schützen Inhalt und Integrität der Daten. Gleichzeitig nutzen sie kostengünstige Kommunikationsnetze wie das Internet zur gesicherten Kommunikation. VPNs lassen sich auch nur für eine Richtung aufbauen, um Zugang zu bestimmten Web-Inhalten zu erhalten, aber einen externen Zugriff auf den Rechner zu verhindern. Die Personal Firewall SPHINX bietet selektive Netzwerkverschlüsselung auf Applikations- oder Protokoll-Ebene. Das reduziert das Datenaufkommen, denn nur die gewählten Protokolle werden bei dieser Funktion verschlüsselt.

### Remote Management und SNMP-Funktionalität

In der Vollversion unterstützt SPHINX Remote Management und SNMP (Simple Network Management Protocol). Der komplette Datenverkehr des Einzel-PCs kann von SPHINX geloggt, diese Logging-Information dann lokal oder auf einem zentralen Syslog-Server gespeichert werden. Als Ergänzung zu anderen Authentifizierungs-Mechanismen kann SPHINX Datenpakete über die Adressen der Netzwerkkarten identifizieren. SPHINX nutzt die Rechengeschwindigkeit moderner Computer optimal und minimiert den Verwaltungsaufwand für den Betrieb mehrerer Rechner. Damit steht eine effiziente Lösung auch für die Bewältigung grosser Datenaufkommen zur Verfügung. Zusätzliche Firewall-Module, die den Datenverkehr überwachen, analysieren und die Bandbreiten-Geschwindigkeit zuordnen, sind nicht nötig. Die Personal Firewall führt Applikationen aus, die einen hohen Datendurchsatz erfordern. In Netzwerken, die durch eine zentrale Firewall abgesichert werden, lassen sich mit SPHINX verschiedene Funktionen auf Desktop-Ebene durchführen. SPHINX erweitert den Schutz, den eine zentrale Firewall bietet und wehrt Angriffe aus dem lokalen Netzwerk auf den Einzel-PC ab. Die Software sichert dadurch bestehende Investitionen und senkt die Total Costs of Ownership (TCO). Unabhängig von Ort und Netzwerkstruktur bietet SPHINX zusätzliche Sicherheit vor Hackerangriffen – ein wichtiger Vorteil für Anwender, die mobil Informationen über öffentliche Netze austauschen.

### Versionen für professionelle Anwender sowie für Remote- und Heim-Anwender

Für professionelle Anwender in mittleren und grossen Unternehmen steht eine Netzwerkversion der Firewall zur Verfü-

gung, die auf jedem Computer in einem Netzwerk installiert wird. Administratoren können diese Rechner in internen (Local Area Network) und externen Netzen (Wide Area Network) von einer zentralen Stelle aus überwachen. Die Version für Remote-Anwender wird auf Notebooks oder Rechnern installiert, die aus der Ferne eine gesicherte Verbindung zu einem Unternehmensnetz benötigen. In internen und externen Netzwerken kann ein Administrator im Unternehmen diese Software zentral einsetzen. Beide Softwareversionen, für Netzwerke und Remote-Anwender, verfügen über VPN- und IPSEC-Funktionalität. Heim-Anwender sichern mit ihrer Firewall-Version einzelne Rechner, die über Modem eine Internet-Verbindung aufbauen. Über die benutzerfreundliche grafische Oberfläche richten Anwender alle Funktionen für die eigenen Sicherheits-Bedürfnisse ein. Die Heim-Anwender-Software lässt sich vom Internet herunterladen und ist im Fachhandel erhältlich.

Die OEM-Version von SPHINX sichert einzelne Rechner, die via Modem mit dem Internet verbunden sind. Anwender verwalten die verschiedenen Funktionen der Software, die beim Neukauf eines Rechners vorinstalliert ist. SPHINX bietet effiziente und umfangreiche Sicherheitsfunktionen wie beispielsweise Firewall-Filter auf der Desktop-Ebene, Verschlüsselung, Authentifizierung, virtuelle Tunnel und Logging. Administratoren können während des Rechnerbetriebs Sicherheits-Funktionen verändern: So lassen sich Filter-Regeln ändern und den Authentifizierungs- sowie den Tunnel-Modus starten und beenden. Ebenso lässt sich der Verschlüsselungsmodus starten oder beenden und die Schlüssel können gewechselt werden. Auf diese Weise optimieren und kontrollieren Sicherheitsadministratoren Computernetzwerke. SPHINX ist in den Sprachen Deutsch, Englisch, Französisch, Japanisch, Mandarin und Koreanisch erhältlich. 9.4

**Info:**
Siemens Schweiz AG
IC Enterprise Networks
Information Security
Postfach
CH-8047 Zürich
Tel. 01 495 63 30
Fax 01 495 63 31

## Modularer xDSL-Funktions-Tester

Der AM 500e von Ameritec ist ein modular aufgebauter, batteriebetriebener Tester zur analogen und digitalen Prüfung und Qualifizierung von Kupferadernpaaren und zum Testen der Performance bei Modemverbindungen. Die im verwendeten Spektrum benötigten Frequenzen können damit auf Dämpfung überprüft werden. Ausserdem werden in der Modem-Simulation für CO und USER die Übertragungsraten für Upstream und Downstream festgestellt. Damit ist der AM 500e für die verschiedensten Übertragungssysteme einsetzbar, einschliesslich der Basisbandbreite für POTS-Schnittstellen und Schnittstellen für ISDN, HDSL und ADSL-Anwendungen.

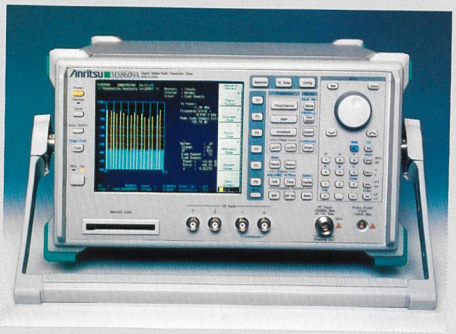

*AM 500e von Ameritec.*

GIGACOMP AG
Gewerbezone Lätti
CH-3053 Münchenbuchsee
Tel. 031 868 44 55
Fax 031 868 44 50
E-Mail: info@gigacomp.ch
Homepage: www.gigacomp.ch

## Digital Mobile Radio Transmitter Tester

Der Digital Mobile Transmitter Tester MS8609A von Anritsu ist, wie der MS8608A, speziell auf Anwendungen für die dritte Mobilfunkgeneration (3GPP) entwickelt worden. Deckte der MS8608A bisher den Frequenzbereich bis 7,8 GHz ab, so erlaubt nun der MS8609A die Untersuchung von Frequenzspektren bis 13 GHz und erfüllt somit die 3GPP-Spezifikation zur Untersuchung von Spurious Emissions. Ebenfalls ist jetzt für beide Geräte eine GSM/Edge Analyse Option verfügbar. Die Geräte sind in der Lage, breitbandige digitale Signale mit höchster Präzision und Genauigkeit zu analysieren. Sie sind nicht nur für die Entwicklung, sondern auch für die Fertigung von Komponenten und Systemen für Basisstationen und Mobilfunktelefone der dritten Generation einschliesslich W-CDMA geeignet. Der standardmässig eingebaute Spektrumanalysator verfügt über Auflösebandbreiten bis 20 MHz und kann Signale bis zu 20 Mbit/s verarbeiten. Die Geräte können wegen des grossen Dynamikbereichs sowohl zur Untersuchung von Basisstationsverstärkern als auch für ACP-Messungen von W-CDMA-Signalen benutzt werden. Der eingebaute Leistungsmesser mit Sensor verfügt über eine Genauigkeit von ± 0,4 dB. Mit der eingebauten W-CDMA-Software können Modulationsanalysen und Code-Domain-Untersuchungen gemäss den 3GPP-Spezifikationen auf HF-Ebene als auch auf Basisbandebene (I, Q) durchgeführt werden. Ebenso sind ACP-Messungen gemäss den 3GPP-Spezifikationen für den HF-Eingang möglich.

GIGACOMP AG
Gewerbezone Lätti
CH-3053 Münchenbuchsee
Tel. 031 868 44 55
Fax 031 868 44 50
E-Mail: info@gigacomp.ch
Homepage: www.gigacomp.ch




*Das grosse TFT Farbdisplay ermöglicht ein ermüdungsfreies Arbeiten und ein einfaches Ablesen der Einstellungen und Messkurven.*