Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses

Band: 91 (2000)

Heft: 23

Rubrik: IT-Praxis = Pratique informatique

IT-Praxis
Pratique informatique

Differenziertere Domain-Struktur gefragt

Die Anzahl der Domain-Namen hat die 30-Millionen-Marke überschritten. Zurzeit existieren weltweit 30 272 862 Domain-Registrierungen, die in den letzten zehn Jahren geschaffen wurden. Bis ins Jahr 2002 soll sich die Anzahl mehr als verdoppeln. Dann soll es 75 Millionen Domain-Registrierungen geben. Dieses explosionsartige Wachstum verlangt nach neuen Strukturen.

Laut Tom Barret, CEO von NetNames, wird dieses Wachstum nur verkraftbar sein, wenn neue Endungen (Top Level Domains wie .com usw.) der Öffentlichkeit zugänglich gemacht werden. Die Internetindustrie warte nun also darauf, dass die Firma Internet Corporation for Assigned Names and Numbers (Icann) entsprechende Entscheidungen fällt.

Belgischer Standard für die USA

Die USA ersetzen ihren 30 Jahre alten Verschlüsselungsstandard, Data Encryption Standard (DES), durch den Advanced Encryption Standard (AES). Dem neuen Standard liegt der von den zwei belgischen Kryptografen Vincent Rijman und Joan Daemen entwickelte Algorithmus Rijndael zu Grunde. Die dreijährige Suche nach dem neuen Standard wurde von dem National Institut of Technology (NIST) koordiniert. Die endgültige Entscheidung wird im Frühjahr 2001 bekannt gegeben. AES soll von allen US-Regierungsbehörden eingesetzt werden.

Die Entwickler von Rijndael sehen für ihren Algorithmus kein Geld, da sie ihn als Open Source ins Netz gestellt haben. Das NIST bewertete die insgesamt 15 verschiedenen Kandidaten hinsichtlich Sicherheit, Geschwindigkeit und Verlässlichkeit über ein breites Spektrum an Plattformen, von Smart Cards bis zu Grossrechnern. Alle bewerteten Algorithmen müssen 128-, 196-, 256-Bit-Schlüssel unterstützen. Aus den letzten fünf Kandidaten wurde Rijndael ausgewählt, weil der Algorithmus nach Ansicht von NIST die beste Kombination von Sicherheit, Effizienz, Implementierung und Flexibilität bietet.

ADSL-Rennen geht weiter

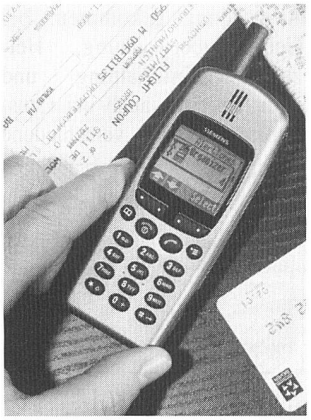
Nach der Lancierung der High-Speed-Anschlüsse ADSL des Westschweizer Unternehmens VTX und der Firma KPNQwest folgt nun auch Econophone mit einem Angebot, das unter dem Label ihrer Muttergesellschaft Viatel-aDSL steht. Econophone bietet zwei verschiedene Varianten an: Eine Flatrate für 145 Fr. pro Monat, die eine Geschwindigkeit von 256 KBit/s aufweist, und das Viatel-aDSL, das eine Geschwindigkeit von 512 KBit/s erreicht und 199 Fr. pro Monat kostet. Als Kunden will Econophone vor allem kleinere und mittlere Firmen gewinnen.

Krypto-Handy

Auf der Orbit/Comdex 2000 hat Siemens den Prototypen eines Handys mit Verschlüsselungstechnologie vorgestellt. Die Topsec-GSM-Verschlüsselungstechnik soll noch in diesem Jahr auf den Markt kommen.

Mobiltelefonate können bisher nur zwischen Handy und der nächstgelegenen Basisstation verschlüsselt werden. Ab der Basisstation werden diese Gespräche ungeschützt über das normale Festnetz – meist per Richtfunk – weitergeleitet. In einigen Ländern ist sogar die Verschlüsselung zwischen Handy und Basisstation nicht aktiviert, wodurch der gesamte Kommunikationsverkehr also ohne weiteres auswertbar ist.

Um die Sprachsignale verschlüsselt übertragen zu können, simuliert das Topsec-GSM eine Datenübertragung. Es



Abhörsicher telefonieren mit dem Handy

nutzt statt des Sprachkanals den Datendienst des GSM. Dieser erlaubt es, die verschlüsselten Inhalte unverändert und transparent von Ende zu Ende zu übertragen. Die Sprachqualität leidet nach Herstellerangaben nicht durch die aufwändige Verschlüsselung.

E-Commerce per Handy

Das Problem des Missbrauchs von Kreditkartennummern im E-Commerce ist allgegenwärtig. Eine einfache, sichere und komfortable Lösung wurde von der Orell Füssli Security Documents AG zusammen mit der Technologiefirma Ininet AG entwickelt. Das System basiert auf Java-Card-Technologie.

Wie bis anhin wird die Ware im Internet bestellt. Die Identifikation und die Kaufbestätigung erfolgt jedoch über das GSM-Netz mit dem Mobiltelefon. Der Käufer kann mit seiner Bestellung verifizieren und bestätigen, ohne seine Kreditkartennummer im Internet bekannt geben zu müssen. Für die Bestellung sind keine zusätzlichen Programme, Browser oder sonstige Geräte wie z. B. Kartenleser notwendig.

Elektromagnetische Verträglichkeit (EMV)

Elektromagnetische Verträglichkeit betrifft heute alle Bereiche der industriellen Ausrüstung, von der Anlagenplanung, Komponentenauswahl, Installation bis zum Serviceeinsatz der Anlagen bzw. Produkte und wird mittlerweile als Standard vorausgesetzt. EMV-Grundkenntnisse wurden somit notwendiges Handwerkzeug für die Mehrzahl der Einkäufer, Anlagenplaner, Installateure und Servicetechniker in allen Bereichen der industriellen Technik. Die Hersteller sind gefordert, sich mit der Gesetzgebung vertraut zu machen, um Grenzwerte einzuhalten und Verstösse zu vermeiden, die empfindliche Strafen nach sich ziehen können.

Der immer grösser werdende Anteil an Elektronikkomponenten und Mikroprozessoren in Systemen und die Einführung der EU-Richtlinien mit der zwingend vorgeschriebenen Anwendung der bestehenden EMV-Gesetze macht die EMV zudem auch im industriellen und privaten Bereich immer mehr zum Thema.

Zu diesem Thema bietet die Firma Lütze AG (info@ luetze.ch) neben ihrem Fachwissen auch das kostenlose *EMV-Kompendium, Antworten für den Praktiker*, zur EMV-konformen Ausführung und Kennzeichnung von Systemen an.