Entwicklungstendenzen in der Datenschutztechnik

Autor(en): **Beth, T.**

Objekttyp: **Article**

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 (Jahr): **77 (1986)**

Heft 1

PDF erstellt am: **11.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-904137

Entwicklungstendenzen in der Datenschutztechnik

Th. Beth

Der Aufsatz zeigt einige Entwicklungstendenzen im Bereich der Datenschutztechnik auf. Er analysiert dazu die Bedürfnisse der Anwender, z.B. der Banken, und anderseits die zur Verfügung stehenden Technologien sowie die darauf basierenden zukünftigen Kommunikationssysteme.

L'article indique quelques tendances de développement en technique de protection des informations et analyse les besoins de leurs utilisateurs, par exemple des banques, et, d'autre part, les technologies disponibles, ainsi que des futurs systèmes de communication, qui y seront basés.

Adresse des Autors
Prof. Dr. *Th. Beth*, Institut für Informatik, Universität Karlsruhe, D-7500 Karlsruhe.

Anwendungen

Wichtige neue kommerzielle und private Anwendungen können durch die Verfügbarkeit von Local Area Networks bzw. Wide Area Networks erschlossen werden. Dies wird grosse Anforderungen an die Bereitsteller dieser Netze stellen, werden sie doch alle möglichen Services wie Mail, Rundruf, Abfrage, Nachrichten, Literatur usw. anzubieten haben. Dazu wird die dedizierte Zuteilung solcher Services in einem Mehrschichtenmodell, entsprechend den Sicherheitsanforderungen und Zugriffsmöglichkeiten, eine in diesem Zusammenhang besonders interessierende zunehmende Rolle spielen. Die vom bankinternen Geldtransfer grosser Bankinstitute bis hin zu den möglicherweise nur täglich einmal erfolgenden Abrechnungen kleinerer Läden reichenden Anwendungen spielen dabei eine besondere Rolle, da sie, je nach Sicherheitsanforderungen, besondere Massnahmen erfordern. Die algorithmischen Lösungen für diese Massnahmen sowie ihre Implementierung in Soft- und Hardware ist Gegenstand dieses Aufsatzes, wobei das Augenmerk vor allem auf technische Entwicklungen im Bereich der VLSI-Technik gerichtet werden soll, welche möglicherweise hochwertige Übertragungsmedien mit allen geforderten Eigenschaften auch für weitere Bevölkerungskreise verspricht. Hier spielt vor allen Dingen eine gemeinsame europäische Entwicklung eine Rolle, denn nur wenn diese Services länderübergreifend angeboten werden, können sie als Markt für die Hersteller ausgewertet und als Medium von den Benutzern sinnvoll eingesetzt werden. Anstehende europäische Aktivitäten sind eine wesentliche Motivation, mit Optimismus an die Beantwortung der hier gestellten Fragen heranzugehen.

Networks

Eine wesentliche Neuerung, deren Einführung innerhalb der nächsten Zukunft in weiten Bereichen zu erwarten ist, betrifft die lokalen Netzwerke (LAN) sowie deren Vermaschung in sogenannten globalen Netzen (WAN). Die technischen Lösungen, die sich anbieten, sind im Moment mannigfaltig und es scheint sich am Markt noch keine Standardlösung durchgesetzt zu haben. Während sich im Bereich der LAN jedoch einige brauchbare Lösungen herauszukristallisieren scheinen, ist die für globale Netzwerke vorgesehene Technologie weder international abgestimmt noch vollständig ausgereift und vor allem weit von einer Standardisierung entfernt. Es wird dennoch davon ausgegangen, dass ein ISDN-Standard schliesslich die Lösung sein wird, so dass für einzelne Übertragungsstrecken eine Bitrate von 64 kbaud zur Verfügung stehen wird, dass aber auch höhere Frequenzen, etwa für die Übertragung von Videosignalen angeboten werden.

Protokolle

Eine wesentliche Komponente in dieser Entwicklung spielt die Bereitstellung von geeigneten Übertragungsprotokollen, die ein solches Netzwerk in der Anwendung überhaupt erst sinnvoll einsetzbar machen. Die Entwicklung von Protokollen, deren Verifikation und Prüfung ist Gegenstand intensiver Forschungsarbeiten. Auf europäischer Ebene werden gegenwärtig Möglichkeiten diskutiert, um vier sogenannte Testzentren einzurichten, welche die Validierung von Übertragungsprotokollen nach dem ISO/OSI Standard vornehmen können. Hierbei handelt es sich um relativ einfache Protokolle, die schon mit Erfolg eingesetzt werden und somit einen über-

schaubaren Anwendungskreis aufweisen. Für die ins Auge gefasste Vernetzung im nationalen und internationalen Bereich wird die Komplexität sprungartig wachsen, so dass grosse Anstrengungen im Bereich von Theorie und Praxis durch die Bereitstellung von Personalressourcen und Rechnerleistung aufgebracht werden müssen. Hier ist vor allem zu beobachten, dass die festzulegenden Standards evtl. auf wesentlich längere Zeit als geplant und mit wesentlich höheren Kosten anzusetzende Massnahmen implizieren, so dass die Diskussion aus wissenschaftlichen, technologischen und politischen Gründen hochkomplex ist und Fortschritte sich nur langsam abzeichnen.

Übertragungstechnik

Während die Netzwerktechnologie selbst durch die Bereitstellung von Koaxialübertragungsmedien schon weit fortgeschritten ist, lässt im europäischen Bereich die Vernetzung mit optischen Übertragungsstrecken auf sich warten. Die Erklärung für diese Verzögerung, etwa im Vergleich zu Japan, USA und Kanada, ist auf verschiedene wirtschaftliche und politische Faktoren zurückzuführen. Es ist zu hoffen, dass die beteiligten Unternehmen die Behörden durch das Schaffen von Tatsachen zu einem schnelleren Marschtempo veranlassen. Während die Übertragungsmedien selber auf dem Level der Modulation und Codierung durch die Bereitstellung von hochwertigen Modulationsverfahren und Methoden der Vorwärts-Fehlerkorrektur die technischen Voraussetzungen seit langem erfüllen, ist insbesondere die Entwicklung von entsprechend schnellen und zuverlässigen, international akzeptierten kryptographischen Verfahren noch Gegenstand von Forschung und Entwicklung. Es sei auch bemerkt, dass nicht alle kryptographischen Verfahren in allen Ländern gleichermassen eingesetzt werden können, da die wirtschaftlichen und politischen Gegebenheiten des jeweiligen Ursprungslandes des Lieferanten eine wesentliche Rolle bei der Festlegung der Technologie spielen.

Kryptographie

Im Bereich der konventionellen Kryptographie ist durch einige Entwicklungen im Wissenschafts- und Normierungsbereich die Diskussion um die Verwendbarkeit des Data-Encryption-Standards (DES) wieder voll aufgeflammt. Es scheint sich abzuzeichnen, dass für die anstehende Rezertifizierung des Data-Encryption-Standards in Washington D.C. dem Data-Encryption-Standard für gewisse Bereiche die Zulassung nicht wieder erteilen wird, wobei das NBS sich nachhaltig bemüht, die rein kommerziellen Benutzer von der nach wie vor gültigen Zuverlässigkeit des DES zu überzeugen. Dennoch scheint man auch in den USA über die Entwicklung einer neuen Familie von Verschlüsselungsalgorithmen nachzudenken. An dieser Entwicklung sollten europäische Firmen und Wissenschafter unbedingt beteiligt werden. Entsprechende Aktivitäten auf europäischer Ebene beginnen sich abzuzeichnen. Die Entwicklung eines neuen europäischen oder europäisch beeinflussten Sicherheitsstandards ist erklärtes Ziel vieler beteiligter Firmen, Organisationen und Wissenschafter in Forschung und Entwicklung.

In einem solchen Algorithmus, der zunächst als Ersatz für konventionelle kryptographische Algorithmen wie DES gedacht ist, sollten auch die Features von Public Key Algorithmen eingebaut werden. Hier bieten sich zwei Verfahren an: das Diffie-Hellman-Verfahren zum öffentlichen Schlüsselaustausch, wobei die dort benutzte Einwegfunktion auch den Einsatz für konventionelle symmetrische Verschlüsselungsverfahren erlaubt, und vor allem das Public Key System nach Rivest, Shamir and Adleman, das sowohl zum Schlüsselaustausch als auch zum Verschlüsseln selber gedacht ist. Zum Stand der Implementierung dieser beiden Verfahren nun einige kurze Daten: Während für das Diffie-Hellman-Verfahren Implementierungen für Bitraten von 64 kbaud mit Single-Chip-Solutions auf etwa 4×4 mm^2 bei 512 bit Sicherheit realisiert werden können, ist die Lage beim RSA-Verfahren etwas unangenehmer. Im Moment werden mehrere Implementierungen diskutiert. Es sind zwei Lösungen in Single-Chip-Form angekündigt, ferner wurde kürzlich eine Gate-Array-Lösung mit 16 Einzelchips angekündigt. Eine Lösung auf einer einzelnen Europakarte wird ebenfalls entwickelt. Alle diese Lösungen bieten Geschwindigkeiten an, die sich im Bereich von 10 bis 50 kbaud bewegen. Unsere eigene Lösung auf Europakarte, die mit konventioneller Signalverarbeitungshardware läuft, würde Geschwindigkeiten bis zu 64 kbaud erlauben. Der wesentliche Faktor, der diese Entwicklung behindert, ist der Preis. Die Single-Chip-Solutions haben etwa die Ausmasse von Hochleistungsmikrocomputern, etwa des Typs 68 000. Die Europakartenlösung, die am Institut für Informatik der Universität Karlsruhe gegenwärtig vorangetrieben wird, ist dichtbesetzt mit Signalverarbeitungs-Hardware, so dass der Einsatz nur in Systemen gerechtfertigt ist, bei denen der Preis für eine relativ teure Verschlüsselungseinheit vernachlässigbar ist.

Akzeptanz und Verfügbarkeit

Diese Überlegung führt zum nächsten wesentlichen Punkt: Eine sinnvolle Arbeit im Bereich Datenschutz und Datensicherheit ist nur dann gewährleistet, wenn eine breite Anwendung den Einsatz in allen Komponenten und bei allen Teilnehmern eines Systems ermöglicht. Dieses setzt voraus, dass ein Sicherheitsbedürfnis überhaupt besteht, und alle Teilnehmer Sicherheitsmodule benutzen dürfen. Gegenwärtig ist auf dem Markt eine gewisse Zurückhaltung gegenüber dem aus Sicherheitsforderungen entstehenden Investitionsbedarf zu beobachten. Es sollte aber dringend klargemacht werden, dass bei der zu erwartenden Verbreitung von Kommunikationsnetzen eine Datensicherheitseinrichtung ein ganz gewöhnliches Bauteil, wie etwa ein elektrischer Zähler oder ein Briefkasten, sein wird. Bei den Netzen, an denen viele Tausende oder gar Millionen Benutzer teilnehmen werden, ist die Frage der *Identifikation* und *Authentifikation* wesentlich. Ohne hinreichend erforschte Methoden auf diesem Gebiet wird ein weltweites System, das hohen Sicherheitsanforderungen genügen muss, nicht zu implementieren sein. Ein Schritt in diese Richtung ist die Bereitstellung einer persönlichen Identitätskarte im Kreditkartenformat, auf der alle wesentlichen Informationen gespeichert sind. Hierzu bietet sich die sogenannte *Smart-Card* oder der *Intelligent Token* an. Dies ist eine Karte, auf der ein Mikroprozessorchip mit entsprechendem Memory untergebracht ist. Ohne kryptographische Massnahmen ist diese Karte nicht sinnvoll einzusetzen. Gegenwärtig zeichnen sich erste technologisch brauchbare Lösungen am Markt ab, aber dennoch bleibt die Kryptographie ein Stiefkind. So bieten einige Hersteller zwar eine software-

mässige Implementierung des Data-Encryption-Standard auf einem 8-bit-Prozessor an, neben der Tatsache aber, dass diese Lösung nicht dem vorgeschlagenen ISO-Standard entspricht und dass dies der von allen beteiligten Ländern geübten Zurückhaltung beim Verkauf von DES-Hardware widerspricht, hat diese Lösung vor allem den Nachteil, dass es sich um ein symmetrisches Chiffrierverfahren handelt, das zu Authentifizierungszwecken bekanntermassen nicht benutzt werden kann und ausserdem mit 1,5 kbyte im jeweiligen EEPROM sehr viel Speicherplatz wegnimmt. Offen ist in diesem Bereich die Bereitstellung einer Single-Chip-Lösung für kryptographische Prozessor- und Memorybausteine, - hierbei handelt es sich aus kryptographischer Sicht um eine Minimalforderung, die gegenwärtig noch von keinem Hersteller realisiert werden kann. Die Algorithmen-Entwicklungsgruppe an der Universität Karlsruhe denkt im Moment darüber nach, wie dieses Problem durch die Bereitstellung geeigneter Krypto-Hardware bewältigt werden kann. Auch hier sind Fortschritte nur dann zu erzielen, wenn die internationalen Standardisierungsmassnahmen Fortschritte verzeichnen können. Es ist zu hoffen, dass bei den europäischen Gesprächen, die in den nächsten Monaten stattfinden, auch diese Frage angeschnitten wird.

Ausblicke

Schliesslich sei noch ein Ausblick auf neue Technologien erlaubt. Neben der optischen Verarbeitung, die nach neusten Mitteilungen gute Fortschritte macht, scheint es, dass in kurzer Zeit neue Architekturen für digitale Verarbeitung den Markt bestimmen werden. Beispielhaft sei an die Wafer-Scale-Integration des selbstorganisierenden fehlertoleranten Typs erinnert, die im Moment von einer Gruppe englischer Wissenschaftler propagiert wird. Es handelt sich hierbei um eine Technologie, die Wafer bereitstellen kann, auf denen bis zu 300 und mehr korrekt funktionierende Chips in einem Pipeline-Netzwerk miteinander verbunden sind. Diese Architektur bietet sich an, um sowohl schnelle RSA-Operationen als auch Protokolle für komplizierte Netzwerke zu implementieren. Die zu erwartenden Rechengeschwindigkeiten liegen mit Sicherheit jenseits von 20 MBaud, so dass selbst für optische Netzwerke die nötige Technologie bereitstehen wird.

Die Entwicklung dieser neuen Technologien sollte unter Beteiligung der Industrie mit höchster Geschwindigkeit vorangetrieben werden. Es zeichnet sich ab, dass hier zum ersten Mal europäische Firmen die Führung in einem besonderen Technologiebereich übernehmen könnten. Es wäre schade, wenn diese Chancen vergeben würden.

Literatur

[1] *T. Beth:* Implementations of fast public key algorithms. Proceedings of the Online Conference, London, October 16...18, 1985.

[2] *T. Beth:* Cryptography. Proceedings of the Workshop Burg Feuerstein, Germany, March 29... April 2, 1982. - Lecture note in computer science, vol. 149 - Berlin/Heidelberg, Springer-Verlag, 1983.

[3] *T. Beth* u.a.: Kryptographie. Stuttgart, Teubner-Verlag, 1983.