Kommunikationssicherheit : Bedürfnisse und Lösungsbeispiele eines Anwenders

Autor(en): **Rimensberger, U.**

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: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-904138

Kommunikationssicherheit: Bedürfnisse und Lösungsbeispiele eines Anwenders

U. Rimensberger

Banken benötigen leistungsfähige Kommunikationsnetze für den Daten- und Telefonieverkehr. Diese Netze müssen gegen Informationsverfälschung oder -verlust sowie unbefugte Kenntnisnahme gesichert werden. Das Referat zeigt Gefährdungen, spezifische Sicherheitsbedürfnisse und Lösungen anhand von privaten Datennetzen, offenen Netzen, Videotex und elektronischem Zahlungsverkehr.

Les banques ont besoin d'un système de communication performant pour les services de données et téléphoniques, dont les réseaux sont à l'abri d'une falsification ou perte d'informations, ainsi que d'un accès par tiers non autorisés. L'auteur indique les mises en danger, les besoins spécifiques de sécurité et des solutions à l'exemple de réseaux de données privés ou publics, vidéotex et opérations électroniques de paiement.

1. Neueste Technologie

Die Technik spielt im Bankgeschäft eine zunehmend bedeutungsvollere Rolle. Ohne den Einsatz des Computers und modernster Kommunikationsmittel wären weder die beachtliche Geschäftsausdehnung noch das damit verbundene gestiegene Verarbeitungsvolumen möglich gewesen.

Abacus ist das integrierte EDV-System der Schweizerischen Bankgesellschaft (SBG), in dem alle Informationen und Geschäftsfälle der Kunden zusammengeführt werden. Das System ist in seinem Grundumfang realisiert und im gesamten schweizerischen Geschäftsstellennetz eingeführt. Ende 1984 waren bereits über 7000 Terminals für die Information und die Büroautomation eingesetzt. Abacus unterstützt in erster Linie den operationellen Bankbetrieb; es ist aber auch die Voraussetzung für alle Formen von *Electronic Banking*, d.h. der elektronischen Dienstleistungen für den Kunden. Die SBG bietet seit Oktober 1984 auch Telebanking-Dienstleistungen über Videotex an und Anfang Juli dieses Jahres hat sie die erste elektronische Bank eröffnet.

Im September wurden drei weitere Dienstleistungen angekündigt: Ubitel, welches z.B. die direkte Kontoabfrage ab Computer mit Sprachausgabe erlaubt, Ubivic als Basis eines SBG-Treasury-Support-Systems und Ubitex, welches die Videotexdienstpalette auf dem Personal-Computer verfügbar macht.

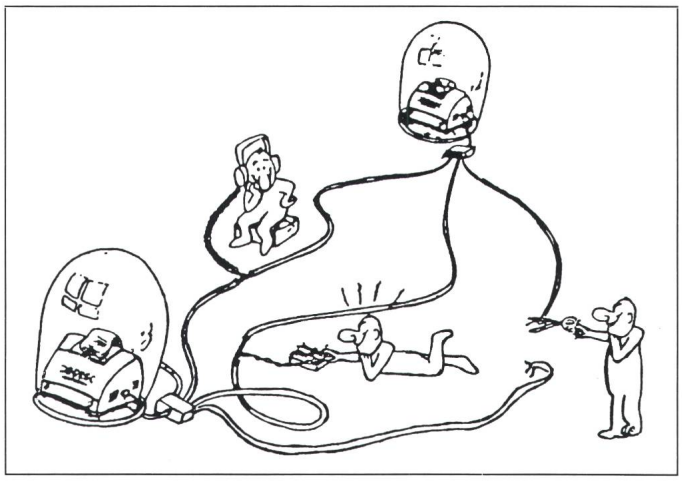
Der Betrieb der grossen On-line-Datennetze einer Bank und erst recht das neue «Electronic-Banking» werden dominiert von zwei Forderungen: Zuverlässigkeit und Sicherheit. Banken waren schon immer sicherheitsbewusst. Ihre Anforderungen gehen weit über die Vorschriften der heutigen Datenschutzgesetze hinaus. So ist es nicht erstaunlich, dass die SBG mehr als 10% ihrer jährlichen EDV-Ausgaben für Sicherheit investiert. So war z.B. das Abacus-Netz von Anfang an vollumfänglich chiffriert.

2. Sicherheitsbedürfnisse bei der Kommunikation

2.1 Bedrohungsarten

Telekommunikationsnetze erlauben, über Draht in den Sicherheitsbereich einer Bank einzudringen. Spätestens seit dem Film «War Games», in dem Hacker Zugang zu einem Atomwaffencomputer fanden, ist diese Gefährdung auch der breiten Öffentlichkeit bekannt. Grundsätzlich können drei verschiedene Problemkreise unterschieden werden (Fig. 1):

Fig. 1
Bedrohungsarten
Zugriff
Änderung
Unterdrückung



Adresse des Autors
U. Rimensberger, dipl. El.-Ing. ETH, Schweizerische Bankgesellschaft, 8021 Zürich.

- der unerlaubte Zugriff auf Informationen,
- die unerlaubte Änderung von Informationen,
- das unerlaubte Unterdrücken von Informationen.

Attacken, welche nur zur Informationsbeschaffung dienen, werden als *passive*, solche, die Informationen verfälschen oder unterdrücken, als *aktive* Attacken eingestuft. Typisch dabei ist, dass passive Attacken nicht festgestellt, aber relativ leicht vermieden werden können, wo hingegen aktive Attacken schwer vermeidbar, aber leichter festzustellen sind. Kommunikationsnetze müssen gegen beide, d.h. passive und aktive Attacken, geschützt werden.

2.2. Geschlossene Netze

In geschlossenen Netzen, wie z.B. in Bankterminalnetzen, kann man sich einfach mit Chiffriergeräten auf der Linkebene schützen (Leitungschiffrierung), da beide Enden unter Kontrolle des gleichen Benützers sind. Chiffriergeräte gibt es bereits eine Vielzahl auf dem Markt. Ihr Einsatz gibt sicheren Schutz vor passiven und aktiven Attacken auf der Leitung. Das Problem der Autorisierung und der Identifikation des Benützers am entfernten Ende muss aber separat gelöst werden, wobei man annehmen muss, dass das Terminal in einem zutrittsgeschützten Raum steht. Von Chiffriergeräten auf Leitungsebene erwartet der Benützer:
- minimale oder keine Einflüsse auf das bestehende Netz,
- minimale Investitionen,
- Flexibilität für neue Kommunikationslösungen,
- einfaches Key-Management.

Die ursprünglichen Gerätekosten in der Grössenordnung von Fr. 40 000.- im Jahre 1974 haben sich nahezu alle zwei Jahre halbiert. So sind Chiffrierkarten für PCs heute bereits in der Grössenordnung von 2000 Fr. erhältlich. Der Benützer hofft deshalb, dass die Chiffrierung bald einen festen, «gratis» mitgelieferten Bestandteil der Kommunikations-Endgeräte bildet.

2.3 Offene Netze

Über offene Netze kommuniziert die Bank mit einer grossen, unbestimmten Zahl von Drittfirmen und -personen. Früher war das übliche Mittel dazu die Post. Dabei waren, zumindest juristisch, alle Sicherheitsaspekte abgedeckt. Der - eventuell versiegelte - Umschlag sorgte für den Informationsschutz, die Unterschrift für die Authentizität und das öffentliche Unterschriftenregister (Notariat) für die Autorisierung. Neue elektronische Systeme, speziell Zahlungsverkehrssysteme (EFTS = electronic funds transfer system) müssen, um überhaupt eingeführt werden zu können, wesentlich höheren Sicherheitsanforderungen genügen. Kryptologische Systeme sollen dabei gewährleisten, dass
- der Absender den Empfänger identifizieren kann,
- der Absender den Versand beweisen kann (unterschriebene Quittung),
- der Empfänger die Herkunft erkennt,
- der Empfänger sicher sein kann, dass die Meldung unverfälscht ist,
- der Erhalt nachträglich bewiesen werden kann (unterschriebenes Original)
- falls gewünscht, während der Übermittlung Schutz vor Abhorchen besteht.

Beim Zahlungsverkehrssystem, z.B. beim SIC (Swiss Interbank Clearing) gilt es, höchsten Sicherheitsanforderungen zu genügen, werden doch täglich über 100 Milliarden Franken «übermittelt».

Beim Videotex sind exakt die gleichen Anforderungen zu stellen, sobald der Kunde von seinem Terminal aus Geschäfte abwickelt, z.B. eine Zahlung veranlassen oder auch nur eine Reise buchen will. Wichtig ist hier eine einfach zu handhabende und billige Lösung (z.B. Chip Card), wobei ein Standard noch fehlt.

3. Lösungsbeispiele

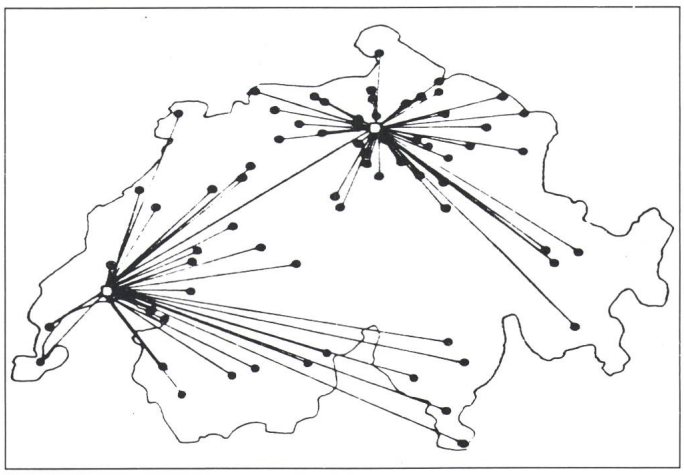
Chiffrierlösungen dürfen nicht punktuell realisiert werden - einmal mit höchster Sicherheit, einmal nicht -, sondern müssen auf ein ganzheitliches Sicherheitskonzept abgestützt sein. Ausgehend von den Gefährdungsanalysen muss ein Gesamtkonzept festgelegt und auf höchster Ebene abgesegnet werden. Jedes einzelne Kommunikationsprojekt hat sich dann ausnahmslos an diese Standards zu halten.

Das On-line-Datennetz *Abacus* mit über 30 Sperry Hosts und fast 400 Nixdorf-Niederlassungs-Computern bestand bis vor kurzem aus über 500 einzelnen Datenmietleitungen. Alle wurden mit Hardware-Chiffriergeräten ausgerüstet. Die gewählten Chiffriergeräte konnten nicht nur im stream cipher mode arbeiten, sondern auch auf der Prozedurebene (message encryption). So war es möglich, punktuell Strecken mittels Paketvermittlung zu realisieren, ohne die Geräte zu ersetzen. Seit diesem Jahr wird das gesamte Netz auf digitale Leitungen mit 65 kbit/s umgestellt. Wieder konnten die gleichen Chiffriergeräte weiterverwendet werden (Fig. 2).

Die SBG-*Rechenzentren* werden mit Hyperchannels direkt verbunden. Dabei wurde erstmals in der Schweiz eine Mietleitung von 2 Mbit/s realisiert, welche die Standorte Zürich und Lausanne verbindet. Auch diese Verbindung wurde chiffriert, wobei auf militärische Geräte zurückgegriffen werden musste.

Ubitel ist eine neue Dienstleistung, dank welcher der Kunde über ein kleines Taschenterminal und irgendeinen Telefonapparat z.B. den Stand seines Kontos abfragen und mittels Computer-Sprachausgabe die Antwort erhalten kann (Fig. 3). Sogar in dieses kleinste Gerät wurde eine Chiffrierung eingebaut.

Fig. 2
Kommunikationsnetz der SBG in der Schweiz



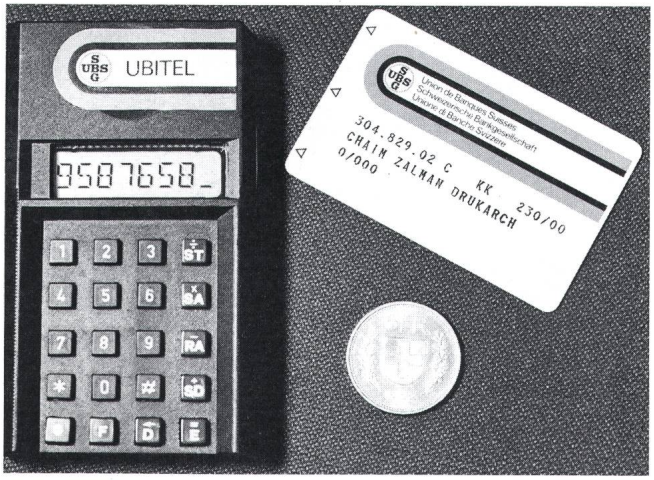


Fig. 3
Ubitel
Zur Kommunikation zwischen Bankkunde und -konto

4. Neue Herausforderungen

4.1 ISDN

Das Fernmeldegeheimnis, nur durch gesetzliche Massnahmen sichergestellt, genügt den Anforderungen der Benützer bereits heute nicht mehr. Allerdings ist die sichere Chiffrierung von analoger Sprache äusserst aufwendig. Mit IDN, dem integrierten digitalen Netz, wird die Chiffrierung aber realisierbar. Die Benützer erwarten deshalb, dass im ISDN auch gesicherte Dienste auf der Ebene «End to End» angeboten werden. Dabei muss der Chiffrierprozess im Endgerät ablaufen, aber das Netz muss eine zentrale, öffentliche Notariatsfunktion anbieten. So wird eine gesicherte Übermittlung über ein offenes Netz – praktisch jeder mit jedem – möglich. Entsprechende Standards müssen dringend festgelegt werden. Diverse Gremien wie ANSI, ISO, NBS, IEEE sind bereits aktiv.

4.2 LAN

Local Area Networks verursachen ein neues, häufig unterschätztes Problem. Innerhalb eines Gebäudes werden z. B. in der Bank verschiedene Sicherheitszonen definiert. So ist z. B. der Computerraum eine andere Sicherheitszone als eine Schalterhalle. Bisherige Punkt-Punkt-Datenleitungen konnten innerhalb einer Sicherheitszone verlegt werden. LANs erschliessen jedoch das ganze Haus, d. h. aber auch, dass alle Informationen überall angezapft werden können. Also müssen auch auf einem LAN die Übermittlungen chiffriert werden. Wir Benützer erwarten, dass diese Chiffrierung Bestandteil der LAN-Interface-Boxen wird und die Kosten nur unwesentlich erhöht.

5. Schlussbemerkungen

Zum Schluss noch zwei Gedanken. Der erste Punkt betrifft Standards. Um eine grosse Verbreitung der Chiffrierung, speziell in offenen Netzen, zu erreichen, setzt man bei der SBG stark auf die kommenden Standards. Diese bieten die Chance der Vereinheitlichung und damit kostengünstiger Produkte; sie bergen aber auch eine Gefahr. Es besteht nämlich bei diesen internationalen Gremien das Risiko, dass man sich auf den kleinsten gemeinsamen Nenner einigt, d. h. auf der tiefsten Sicherheitsstufe. Somit ist die Chance gross, dass sich weltweit Mathematiker an die Analyse des Systems setzen und mit einiger Wahrscheinlichkeit das System auch knacken können.

Der andere Punkt betrifft die Implementation der Chiffrierung. Um eine End-to-End Chiffrierung sicherzustellen, darf die Chiffrierung nicht mehr als Black Box auf Leitungsstufen eingesetzt werden, sondern sie muss bis zur Applikation hinauf reichen. Das heisst konkret: was der Benützer braucht, sind nicht mehr Chiffrierboxen, sondern in die Architektur eingebettete Gesamtlösungen.