HAMFU
HISTORY

INFORMATIONSTECHNIK UND ARMEE

Vorlesungen an der Eidgenössischen Technischen Hochschule in Zürich
im Wintersemester 1996/1997
Leitung:
Untergruppe Führungsunterstützung - Generalstab
Divisionär E. Ebert, Unterstabschef Führungsunterstützung

Vernetzte Welten - Ungeahnte Möglichkeiten und ungeahnte Gefahren ?

Referent: W. Oswald

Diese Vorlesung wurde durch die Stiftung HAMFU digitalisiert und als
PDF Dokument für www.hamfu.ch aufbereitet.

Vernetzte Welten;

Ungeahnte Möglichkeiten! - Ungeahnte Gefahren?

W. Oswald

Inhalt

1 Übersicht

2 Kommunikationsnetze

3 Risiken und Gefahren

4 Schutzmassnahmen und -möglichkeiten

5 Evaluationskriterien für Schutzmassnahmen

6 Schlussbemerkungen

7 Literaturverzeichnis

Adresse des Autors:
GRETACODER Data Systems AG
Althardstrasse 150
8105 Regensdorf

Informationstechnik und Armee
36. Folge 1996/97

5.97 230 U37749/6

1 Übersicht

Weltumspannende Kommunikationsnetze erlauben praktisch mit jedem Computer in Verbindung zu treten. Multimedia-Anwendungen eröffnen neue Kommunikationsformen. Fernsteuerung und Fernüberwachung selbst kompliziertester Technik erlauben, ohne lokales Personal jederzeit über den Status von Netzen und Geräten im Bild zu sein und im Störungsfall schnell und kompetent eingreifen zu können.

Doch wo bleibt die Sicherheit? Allzuoft werden sehr vertrauliche Nachrichten sorglos und ohne Abhörschutz zwischen nicht authentisierten Partnern elektronisch ausgetauscht. Vernetzte Rechner bilden ein ideales Angriffsziel für "Hacker", wie fast tägliche Schlagzeilen immer wieder beweisen.

In diesem Kommunikationsparadies lauern zum Teil unerkannte Gefahren. Moderne kryptografische Methoden erlauben einen weitgehenden Schutz. Die Auswahl der Mittel bedingt Kenntnisse der wichtigsten Fachbegriffe und Evaluationskriterien, die dargelegt werden. Vor allem ist eine Risikoanalyse als erste Aktion einer Reihe von Massnahmen durchzuführen, um sich einen Überblick über die möglichen Schwachstellen im eigenen Netz zu verschaffen.

2 Kommunikationsnetze

Mit der Liberalisierung auf dem Telekommunikationssektor nimmt die Vielfalt der Anbieter und Betreiber von Netzen immer mehr zu. Fast monatlich werden Joint Ventures, neue Beteiligungen oder Fusionen zwischen Netzbetreibern veröffentlicht. Hand in Hand mit dem Wandel der Bedürfnisse werden immer neue Dienste angeboten. So spricht heute fast jedermann von den neuen Übertragungsarten ATM und Frame Relay. Der Telex dagegen ist bei uns praktisch ausgestorben. Private Netzbetreiber konkurrenzieren zunehmend die öffentlichen Anbieter oder positionieren sich entsprechend für einen guten Start nach der Liberalisierung.

Der Bedarf nach Bandbreite steigt weiterhin, sei es wegen der immer grösseren Vernetzung oder Datenmengen. Die Multimedia-Anwendungen werden noch mehr Bedarf an Bandbreite erzeugen.

3 Risiken und Gefahren

Die Risiken und Gefahren lauern überall. Wer hat sich beim Telefonieren nicht auch schon verwählt? Beim Telefon ist dies meistens nicht tragisch, denn die Person am gewählten Ende meldet sich. Aber wie ist es mit einer vertraulichen Faxmeldung? Beim Bedienen eines Faxgerätes ist es recht wahrscheinlich, besonders bei Geräten mit Kurzwahlmöglichkeit, dass man eine falsche Taste drückt und damit die Meldung an einen falschen Empfänger sendet, was sehr unerwünscht sein kann.

Viren! Wenn Sie Dateien auf Disketten erhalten oder via Internet herunterladen; prüfen Sie diese dann jedesmal auf Viren?

Und dann gibt es unter Umständen noch Personen, die Netzwerke gezielt angreifen. Und dies müssen nicht ausschliesslich Hacker sein.

Attacken auf Netzwerke können in zwei Kategorien geteilt werden:

Beim passiven Anzapfen (Abbildung 1) hört der Angreifer nur zu, ohne die Meldung zu modifizieren noch die Kommunikation zu stören. Ein solches Vorgehen ist generell nicht zu entdecken. Dass der Angreifer die Meldungen versteht, kann aber durch Chiffrierung verhindert werden.

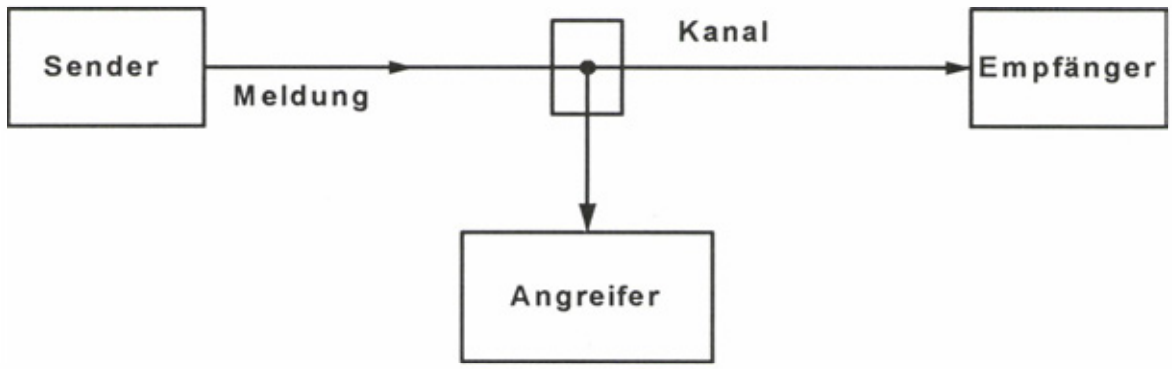

Abbildung 1 Passives Anzapfen

Beim aktiven Anzapfen (Abbildung 2) modifiziert der Angreifer die Meldung oder stört die Kommunikation. Eine Störung kann generell, eine Modifikation unter Umständen entdeckt werden. Verhindert werden kann eine solche Attacke auch nicht durch Chiffrierung, aber eine gezielte Modifikation wird verunmöglicht.

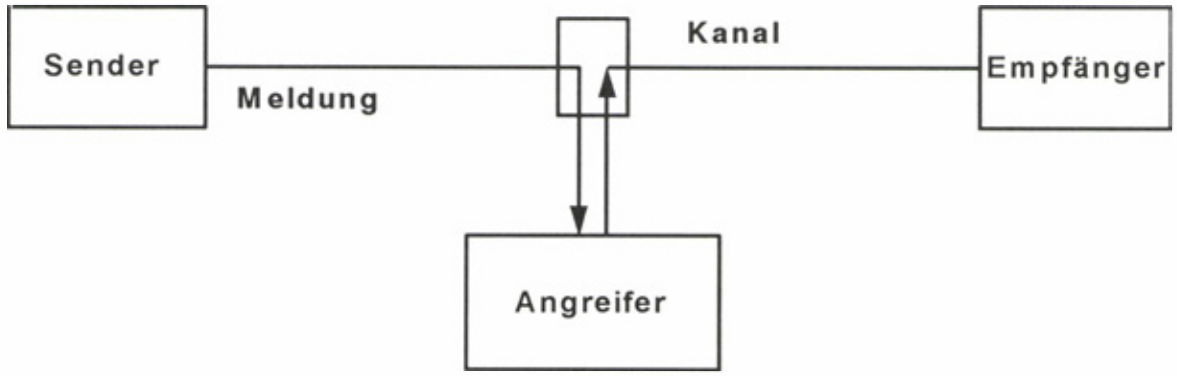

Abbildung 2 Aktives Anzapfen

Dass nicht alle Attacken entdeckt werden, zeigt folgendes Beispiel: Ein Selbstversuch des US-Verteidigungsministeriums hat ergeben, dass von 12'000 Attacken in die eigenen, angeblich gut geschützten Pentagon-Computer einzudringen, sage und schreibe 88% erfolgreich waren. Und nicht nur das: Die Experten mussten zur ihrem Entsetzen feststellen, dass von den über 10'000 gelungenen Attacken lediglich 400 entdeckt wurden, weniger als vier Prozent!

Geräte zur Aufzeichnung von Transaktionen (Sprache oder Daten) sind auf dem freien Markt erhältlich und werden teils bei Banken im Börsengeschäft ganz normal verwendet. Solche Aufzeichnungen werden solange aufbewahrt, bis alles schriftlich bestätigt ist. Die genau gleichen Geräte können aber auch missbräuchlich verwendet werden.

Falls die Datenkommunikation mittels kryptografischer Verfahren geschützt wird, so muss der Angreifer mehr Aufwand betreiben. Klassische kryptologische Attacken sind:

- "Ciphertext-Only" Attacke:
  - Keine Teile des Klartextes sind dem Angreifer bekannt; die generelle Struktur der Daten darf aber bekannt sein.
- "Known Plaintext" Attacke:
  - Teile des Klartextes - und des dazugehörigen Chiffrates - sind bekannt (oft sich wiederholende Information wie Adressen, etc.).
- "Chosen Plaintext" Attacke:
  - Der Angreifer wählt einen freien Klartext und beobachtet das resultierende Chiffrat.

Die schwierigste dieser Attacken ist die "Ciphertext-Only" Attacke.

4 Schutzmassnahmen und -möglichkeiten

Um Schutzmassnahmen und -möglichkeiten sinnvoll treffen zu können, muss zuerst eine Risikoanalyse durchgeführt werden. Vorbeugen ist auch hier besser als heilen, d.h. nicht einen Schadensfall eintreten lassen und dann reagieren und Massnahmen treffen. Nach der Durchführung einer Analyse kann ein Sicherheitskonzept erstellt werden. Dazu sind alle Komponenten der Informationssicherheit (Abbildung 3) zu berücksichtigen.

4.1 Informationssicherheit

Die Informationssicherheit besteht aus folgenden komplementären Komponenten:

- Physikalische Sicherheit
- Personenbezogene Sicherheit
- Prozedurale Sicherheit
- Abstrahlung
- Computer Sicherheit
- Kommunikationssicherheit

Die Kommunikationssicherheit ist *nur eine* Komponente eines umfassenden Sicherheitskonzeptes.

Abbildung 3 Informationssicherheit

Die physikalische Sicherheit kann am einfachsten anhand des Beispieles eines geschlossenen Raumes dargestellt werden. Die abschliessbare Türe, Wände, Decke und Boden eines fensterlosen Zimmers stellen die Sicherheit dar. Fensterlos darum, da sonst vertrauliche Gespräche mittels Laserstrahl mitgehört werden können. Der Strahl tastet die Vibrationen der Fensterscheibe des beobachteten Raumes ab, die durch die Stimmen im Raum angeregt werden.

Personen, welche Daten bearbeiten, stellen praktisch immer das grösste Sicherheitsrisiko dar. Deshalb ist bei der Auswahl der Personen, die zu vertraulichen Daten Zugang haben, grösste Sorgfalt angebracht.

Die prozedurale Sicherheit besteht darin, dass bestimmte Prozeduren durchlaufen werden müssen, bevor der Zugang zu Daten freigegeben wird. Dies kann einerseits für den Zutritt zu Räumen die Verwendung einer Schleuse mit Doppeltüre sein, bei der sich die zweite Türe erst nach dem Schliessen der ersten öffnen lässt. Andererseits ist die Verwendung von Chipkarte und Eintippen einer PIN zum Öffnen einer Türe als Prozedur denkbar.

Alle elektrischen Apparate strahlen elektromagnetischen Wellen ab. Wichtig ist deshalb, dass der Pegel der Abstrahlung entsprechend klein gehalten wird und zwar dort, wo ein Angreifer seine Empfangsapparaturen aufstellen könnte. Die Höhe des Pegels hängt somit vom Sendepegel und den vorhandenen Dämpfungselementen ab. Als klassisches Beispiel wird immer wieder folgendes aufgeführt: Ein Kastenwagen steht auf dem naheliegenden Parkplatz. Im Wagen steht ein Fernsehempfänger mit angeschlossenem Bildschirm, der es erlaubt, die Bildschirminhalte eines abgehörten PCs mitzubetrachten.

Die Computersicherheit ist sehr vielschichtig. Sie kann einerseits das Betriebssystem betreffen, andererseits z. B. das einfache Erstellen von Sicherheitskopien von Dateien, sei es auf eine zweite Speicherplatte, eine Bandstation oder auf Diskette.

Die Kommunikationssicherheit behandelt alle Situationen, wo schützenswerte Daten übertragen werden. So sind Verbindungen zwischen Computern zu schützen. Aber auch Verbindungen zwischen Telefonapparaten und Faxgeräten können schützenswert sein.

Im Falle der hier behandelten Thematik ist primär die *Kommunikationssicherheit* wichtig. Es darf aber nicht vergessen werden, dass diese *nur eine Komponente* eines umfassenden Sicherheitskonzeptes ist.

4.2 Kryptografische Dienste und Prinzipien

Untenstehende Abbildung 4 enthält eine Liste der wichtigsten kryptografischen Dienste.

- **Vertraulichkeit - garantiert Geheimhaltung:**
  - Nur der beabsichtigte Empfänger kann die Meldung lesen und verstehen.
- **Meldungs-Authentisierung - detektiert:**
  - Wenn eine Meldung gefälscht wurde (Daten-Integrität).
  - Wenn eine Meldung nochmals eingespiesen wurde (Wiederhol-Attacke).
- **Partner-Authentisierung - garantiert:**
  - Identifikation des kommunizierenden Gegenübers (Station oder Partner).
  - Daten-Quelle und -Senke sind diejenigen, als die sie sich ausgeben.
- **"Non-Repudiation" (Nicht- Ableugnen, Zurückweisen) - garantiert:**
  - Der Absender kann die Übermittlung der Meldung später nicht abstreiten.
  - Der Empfänger kann den Empfang der Meldung später nicht abstreiten.
  - Die Beweisführung, im Falle eines Streites, ist zu einem späteren Zeitpunkt möglich.

Abbildung 4 Kryptografische Dienste

Ein Grundprinzip der Kryptografie ist dasjenige, dass der Geheimschlüssel der "Schlüssel" zum System sein muss, d.h. die Sicherheit des Systems einzig auf der Geheimhaltung des Chiffrierschlüssels beruht und nicht auf der Geheimhaltung des Chiffrieralgorithmus. Damit wird die sichere Verteilung der Schlüssel (Schlüsselmanagement) entscheidend (Abbildung 5).

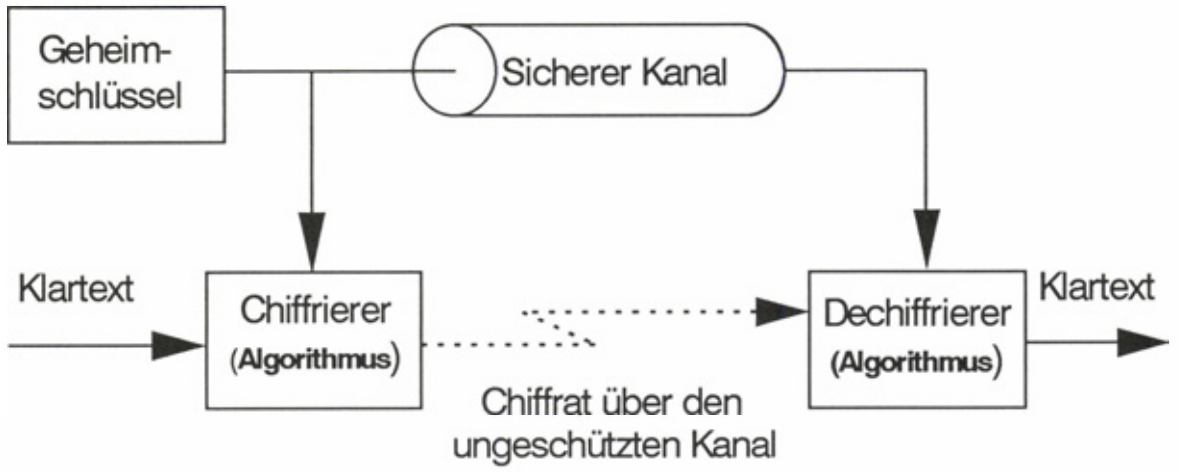

Abbildung 5 Kryptografisches Grundprinzip

4.3 Algorithmen, Schlüsselverteilung und Einbau in ein System

Die Sicherheit ist von vielen Aspekten abhängig. Algorithmen sind einerseits in der Phase der Schlüsselverteilung, andererseits bei der aktuellen Chiffrierung der Daten entscheidend. Ein Algorithmus kann als die komplexe mathematische Funktion bezeichnet werden, nach der die Chiffrierung abläuft. Die Schlüsselverwendung ihrerseits lässt sich in die folgenden Schritte teilen:

- Generierung der Schlüssel (echter Zufallsgenerator?!).
- Verteilung / Transport (Austausch) der Schlüssel auf sichere Art.
- Eingabe und Speicherung der Schlüssel.
- Verwendung der Schlüssel im Gerät.
- Zerstörung der Schlüssel.

Der Einbau solcher Verfahren in ein System ist kritisch. Wie ist der Zugriff zu sensitiven Parametern gesichert? Wird wirklich das (und nur das) gemacht, was behauptet wird, oder gibt es noch versteckte Eigenschaften des Verfahrens?

Damit zeigt sich, dass der Algorithmus nur ein Teil der Sicherheit ist und es noch weitere Teile gibt, die auch wichtig sind.

4.4 Chiffrierverfahren

Die Chiffrierverfahren werden in zwei Kategorien aufgeteilt, in die asymmetrischen (Abbildung 6) und die symmetrischen Verfahren (Abbildung 7).

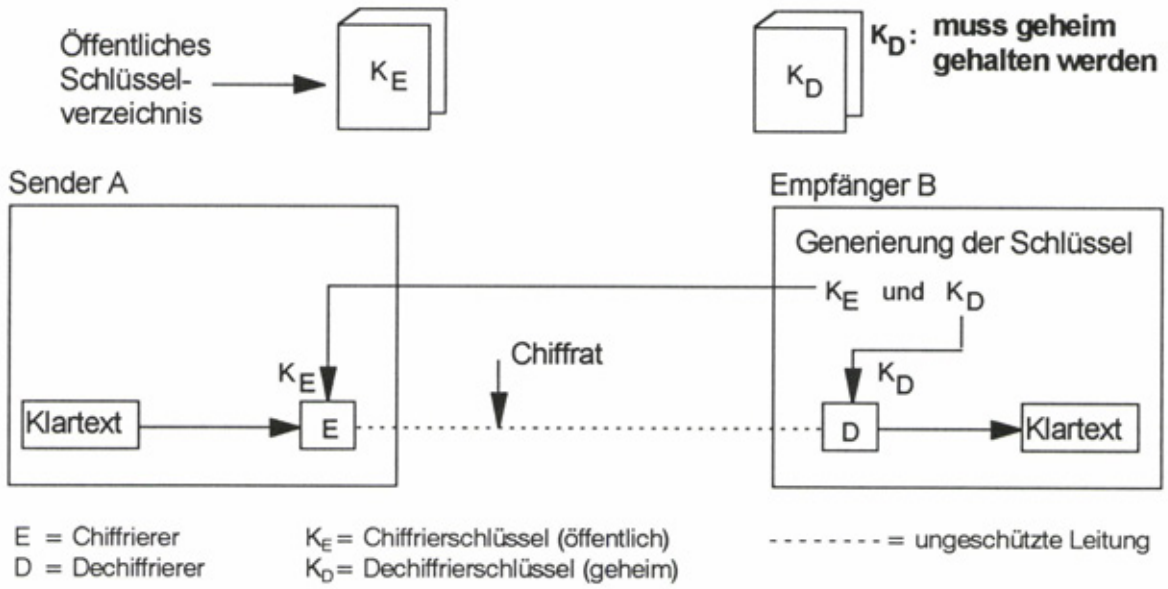

Abbildung 6 Asymmetrische Chiffrierverfahren

Die asymmetrischen Chiffrierverfahren werden auch "Öffentliche Schlüsselverfahren" oder "Public-Key Verfahren" genannt. Sie basieren auf Funktionen, welche in einer Richtung einfach zu berechnen sind. Die Umkehrfunktion dagegen ist bei grossen Zahlen sehr aufwendig und rechenintensiv. Durch entsprechende Wahl der Grösse der Zahlen wird damit einem Angreifer das Berechnen der Ausgangswerte innert nützlicher Frist praktisch verunmöglicht. Bildlich lässt sich dies so erklären: Das Zerschlagen eines rohen Eies ist sehr einfach, das Wiederherstellen des zerschlagenen Eies dagegen praktisch unmöglich. Das RSA Verfahren, benannt nach den Erfindern Rivest, Shamir und Adlemann, basiert auf der Schwierigkeit der Zerlegung einer grossen Zahl in ihre Primfaktoren. Das zweite bekannte Verfahren ist das DH Verfahren, das von W. Diffie und M.E. Hellman erfunden wurde. Es basiert auf der Schwierigkeit der Berechnung von Logarithmen. Diese Verfahren finden vielfach bei der Schlüsselverteilung, zur Authentisierung und für digitale Unterschriften Anwendung.

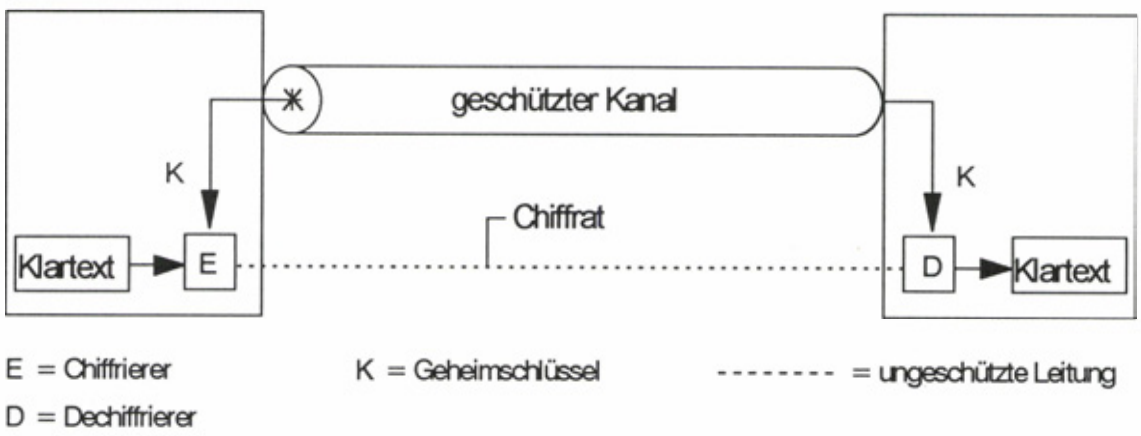

Abbildung 7 Symmetrische Chiffrierverfahren

Dagegen werden die symmetrischen Algorithmen bei der Chiffrierung von Daten und Meldungen angewendet. Dabei gibt es einerseits den normalerweise proprietären "Stream Cipher" (Abbildung 8) oder andererseits den "Block Cipher". Bei den "Block Ciphers" sind u.a. die Algorithmen DES, Triple DES und IDEA allgemein bekannt. Weiter gibt es auch hier proprietäre Algorithmen, wie z.B. den GDS Algorithmus.

Chiffrierverfahren mit "Stream Ciphers" bedingen eine Synchronisation zwischen den Chiffriergeneratoren der beteiligten Chiffriereinrichtungen. Dies ist solange kein Problem, als nach der Startsynchronisierung keine Taktfehler auf der Leitung vorkommen. Sobald aber ein "Bit Slip" auftritt, geraten die Chiffriergeneratoren ausser Takt und ein Resynchronisationsprozedere ist nötig. Dazu muss aber der Synchronisationsverlust zuerst festgestellt werden. Bitfehler auf der Leitung verursachen dagegen einen minimalen Fehler, nämlich die gleiche Anzahl fehlerhafte Klarbit auf der Empfangsseite wie Bitfehler auf der Leitung aufgetreten sind. Wie "Stream Ciphers" im Blockschaltbild aussehen illustriert Abbildung 8.

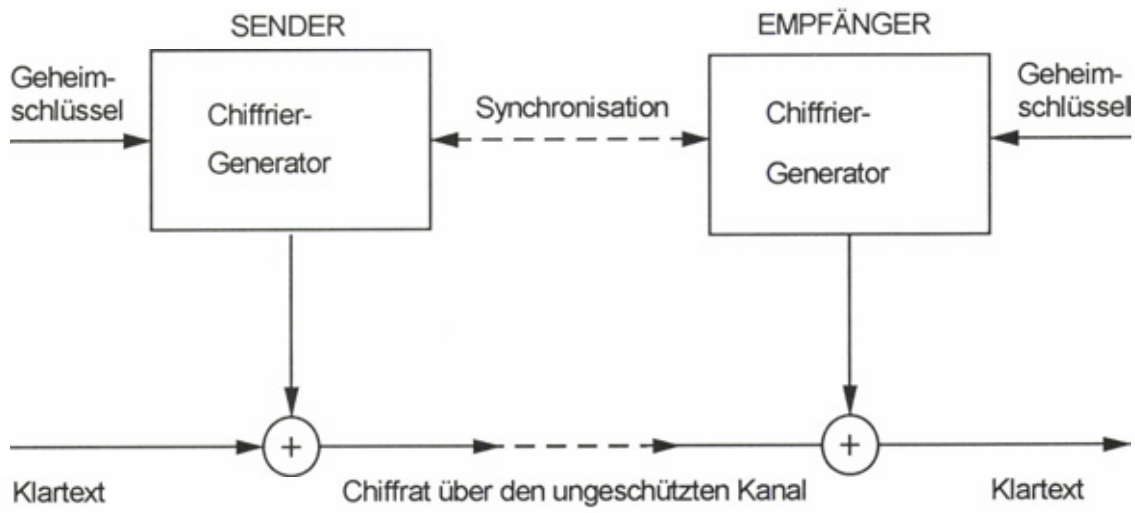

Abbildung 8 "Stream Cipher"

Die Chiffriergeneratoren erzeugen, basierend auf dem Geheimschlüssel und dem Algorithmus einen Bitstrom, der mit dem Klartext bitweise verknüpft wird. Beim Empfänger wird das Chiffrat mit dem Bitstrom des Empfänger Chiffriergenerators verknüpft, was zum ursprünglichen Klartext führt.

Bei den "Block Ciphers" dagegen wird nicht bit- sondern blockorientiert gearbeitet. Dazu hat der Chiffriergenerator je ein Eingangs- und Ausgangsregister. Diese sind je gleich gross und vielfach 64 Bit lang. Die Klardaten werden in Blöcke zu m Bit geteilt und blockweise in das Eingangsregister geladen. Der Block wird dann als ganzes transformiert, d.h. chiffriert. Die komplexe Transformation basiert auf dem Geheimschlüssel und geschieht in mehreren Runden (typisch 16). Pro Runde wird je ein anderer Schlüssel benützt, der mittels "Key Scheduling" vom Geheimschlüssel abgeleitet wird. Das Ausgangsregister enthält das Chiffrat, das über die ungeschützte Leitung gesendet wird. Der Ausgangsblock hat dieselbe Länge wie der Eingangsblock. Blockchiffrierer werden in verschiedenen Betriebsarten verwendet. Die einfachste davon wird ECB-Modus genannt. ECB steht für **E**lectronic **C**ode **B**ook. Früher wurde mit Code Büchern gearbeitet. Darin stand, in welches Chiffrat ein bestimmter Klartext transformiert werden musste. Heute geschieht dies elektronisch. Abbildung 9 zeigt das Prinzip des "Block Cipher" im ECB Modus.

5 - 9

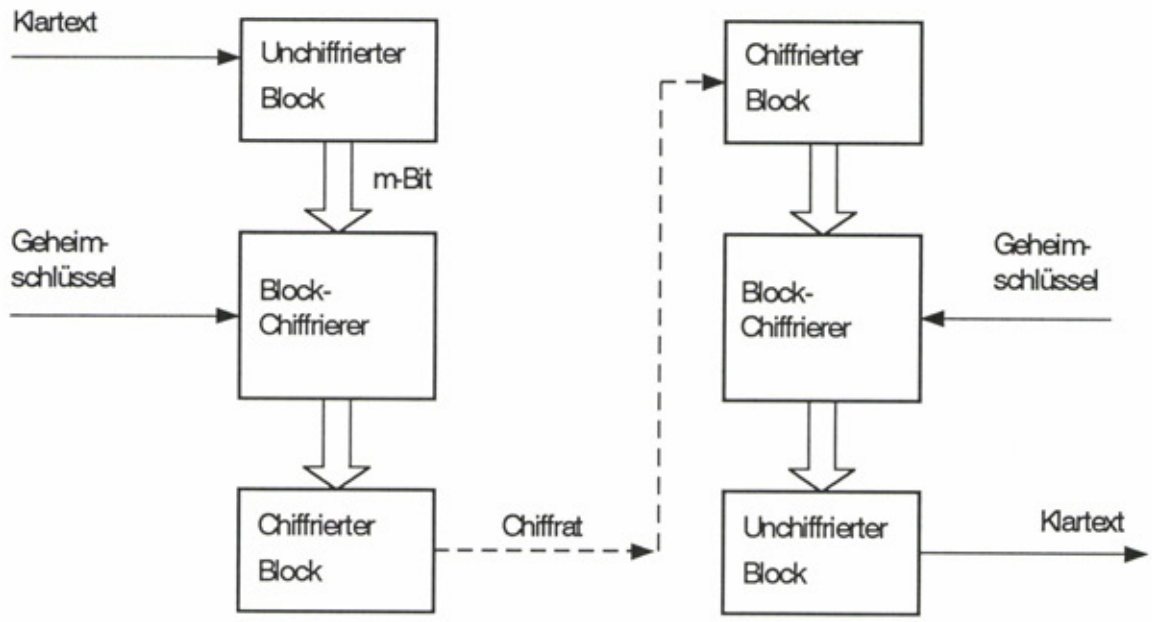

Abbildung 9 "Block Cipher" im ECB Modus (Electronic Code Book)

Eigenschaften des "Block Cipher" im ECB Modus

- Chiffrierte Blöcke sind unabhängig von früher chiffrierten Blöcken, d.h. gleiche Eingangsblöcke - bei gleichem Geheimschlüssel - ergeben gleiche Ausgangsblöcke.
- Das Chiffrat wird bis zu einem Block länger, da der Klartext nicht immer einem vielfachen der Länge des Eingangsregisters entspricht.
- Synchronisationsfehler (Verlust) sind nicht automatisch zu beheben.
- Übertragungsfehler wirken sich auf den ganzen Ausgangsblock aus.
- Verwendung vielfach zur Chiffrierung von PINs, da diese kurz und zufällig sein sollten.

Die als erste erwähnte Eigenschaft des ECB Modus erleichtert Attacken auf den Algorithmus. Sich wiederholende Eingangsblöcke erzeugen immer gleiche Ausgangsblöcke. Dies erlaubt die Anwendung von statistischen Methoden. Dieser Nachteil wurde im Cipher Block Chaining Modus (Abbildung 10) eliminiert.

Eigenschaften des "Block Cipher" im Cipher Block Chaining Modus

- sicherer als ECB Modus, da die statistische Analyse verunmöglicht wird.
- Ausgangsblöcke hängen von den vorhergehenden Ausgangsblöcken ab (wobei Start- und Schlussblocks entfernt werden können).
- benötigt zum Start einen Initialvektor (IV), was zu Schwierigkeiten führen kann.
- Das Chiffrat wird bis zu einem Block länger, da der Klartext nicht immer einem Vielfachen der Länge des Eingangsregisters entspricht.
- Synchronisationsfehler (Verlust) sind nicht automatisch zu beheben.
- Fehlerverschleppung bis zu 2 Blöcken.

5 - 10

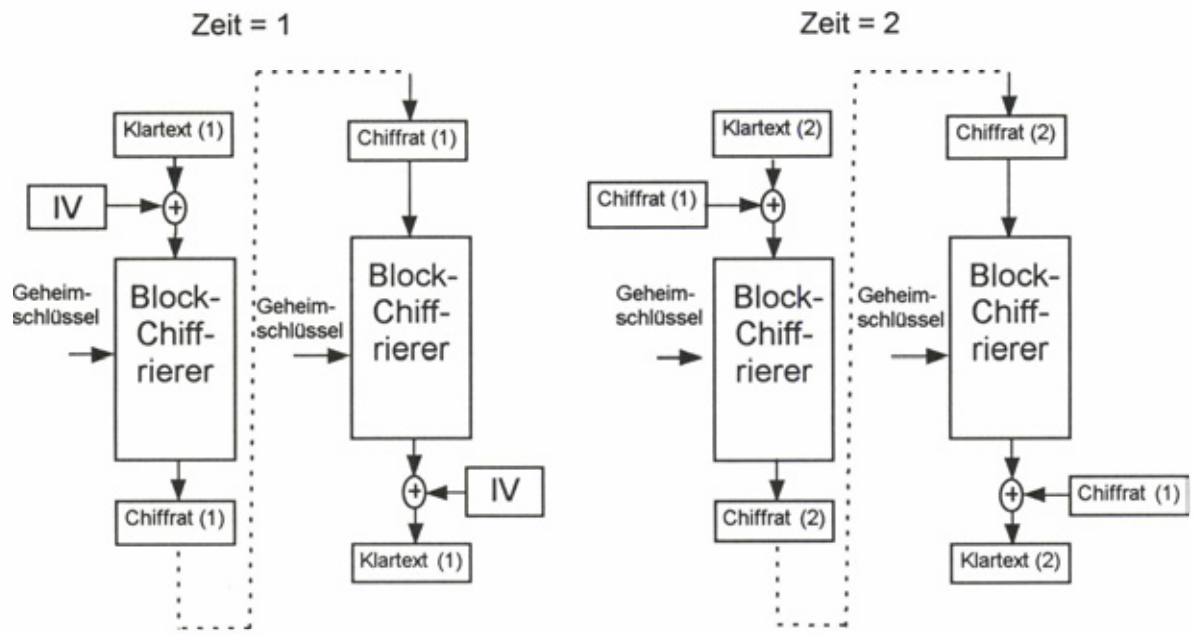

Abbildung 10 "Block Cipher" im CBC-Modus (Cipher Block Chaining)

Es gibt nun noch weitere Modi für "Block Ciphers". So den "Output Feed Back" Modus (OFB-Modus) sowie den "Cipher Feed Back" Modus (CFB-Modus). Der Unterschied besteht darin, dass in der Rückführung entweder der Inhalt des Ausgangsregisters, oder dann derjenige des Chiffrates verwendet wird. Abbildung 11 zeigt den CFB-Modus in allgemeiner Darstellung. In der Praxis beträgt die Anzahl Bit (K) der Rückführung praktisch immer entweder 1, 8 oder 64 Bit. Eine hervorragende Eigenschaft der Anwendung mit 1 Bit Rückführung ist jene, dass bei Bit- und Taktfehlern auf der Leitung die zwei Chiffriergeneratoren nach maximal 64 Bit wieder synchron arbeiten, ohne dass von aussen irgendeine Massnahme wie die Resynchronisierung beim "Stream Cipher" notwendig ist. Diesen Vorteil erkauft man sich mit dem Nachteil der intern notwendigen höheren Taktrate bei gleicher Datengeschwindigkeit auf der Leitung.

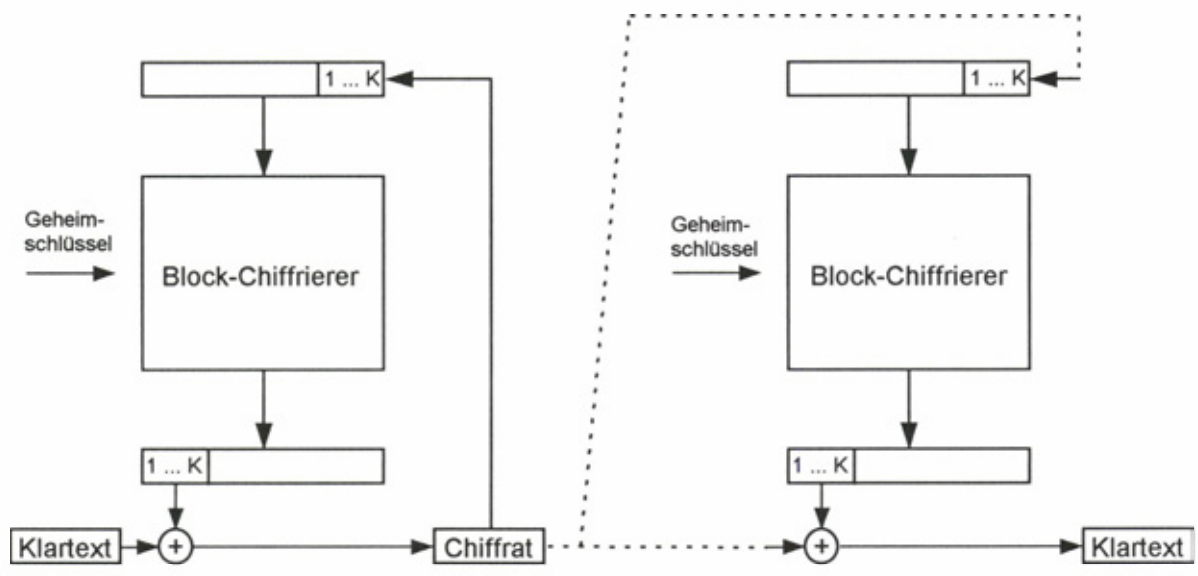

Abbildung 11 "Block Cipher" im CFB Modus (Cipher Feed Back)

Eigenschaften des "Block Cipher" im CFB Modus

- nicht so effizient wie ECB oder CBC (falls K kleiner ist als die Blocklänge).
- Ausgangsblock hängt von den vorhergehenden Ausgangsblöcken ab (wobei Start- und Schlussblocks entfernt werden können).
- Fehlerverschleppung vorhanden.
- automatisch selbstsynchronisierend innert maximal 64 Bit im **1 Bit CFB-Modus** (K=1)

5 Evaluationskriterien für Schutzmassnahmen

5.1 Risikoanalyse

Wie schon eingangs erwähnt, ist am Anfang eines Projektes eine Risikoanalyse unerlässlich. Je besser sie durchgeführt wird, um so einfacher können Entscheide gefällt oder beurteilt werden.

Dazu können folgende Punkte als Richtschnur genommen werden:

- Welche Daten sind schützenswert (evtl. in Kategorien ordnen)?
- Wo sind mögliche Angriffspunkte / Schwachstellen?
- Was sind unsere Erwartungen an eine mögliche Lösung?
- Wie hoch dürfen die Kosten sein?
- Welches Verhältnis der Kosten zu möglichen Verlusten (auch Image!) ist sinnvoll?
- Welche kryptografischen Dienste sind nötig?
- Wie soll das System bei Fehlfunktion reagieren (Stop der Kommunikation!)?

5.2 Fragenkatalog für Lösungsmöglichkeiten

Die nachfolgenden Fragen sind als Hilfe bei einer Evaluation gedacht. Sie decken nicht alle Fälle ab, da Bedürfnisse und Anforderungen immer verschieden sind.

- Wo soll der Schutz eingebettet sein, an welcher Stelle der Kommunikationskette; auf welcher Schicht des OSI Modells ist der Schutz somit gewünscht / sinnvoll?
- Höhe der geforderten kryptografischen Sicherheit / Schlüsselverwaltung?
- Aufwand bei Erstinstallation / Ausfällen / Modifikationen der Netztopologie (zentrales Hilfsmittel zur Steuerung/Verwaltung)?
- Bedienerfreundlichkeit, entspricht diese dem gewünschten Niveau?
- Sind Sicherheits- und technische Funktionen klar getrennt?
- Ist die Lösung immun gegen Wechsel von Computern, Betriebssystemen, Applikationsprogrammen, Protokollen, etc.?
- Hardware oder Software Lösung?
- Notwendigkeit von Anpassungen am Netzwerk wenn Chiffrierlösung zugefügt wird?
- Wie wird die Leistung des Netzes beeinflusst (Durchsatz, Verzögerung)?
- Wie reagiert das System bei Netzausfall und -unterbrüchen / Übertragungsfehlern (Bitverlust oder -wechsel)?
- Wie lange ist der Hersteller schon im Markt; wie ist sein Ruf?
- Kann ich die Komponenten an ausländische Einsatzorte exportieren?

5.3 Einbettung von Schutzmöglichkeiten

Am besten lässt sich dies anhand Abbildung 12 erläutern. Sie zeigt mögliche Punkte, an denen die Chiffriereinrichtungen eingebettet werden können. Dabei ist zu beachten, dass an den Punkten A - C eine in den Kommunikationsgeräten vorhandene Datenkompression nicht verwendet werden kann, da die Chiffrierung vorgängig zur Kompression erfolgt. Ein Chiffrat kann bekanntlich nicht weiter komprimiert werden. Im Gegenteil, es kann sogar eine Verlangsamung bzw. eine Datenexpansion eintreten. Falls dagegen die Daten vor der Chiffrierung komprimiert werden, was an den Punkten D und E der Fall ist, so kann die Kompression genutzt werden.

Punkt A Schutz in der Applikation (OSI Schicht 7)
Punkt B Externes Gerät zwischen Workstation und LAN
Punkt C Externes Gerät zwischen LAN und Kommunikationsgerät (z.B. Router)
Punkt D Schutz im Kommunikationsgerät (z.B. Router)
Punkt E Externes Gerät auf der WAN Seite

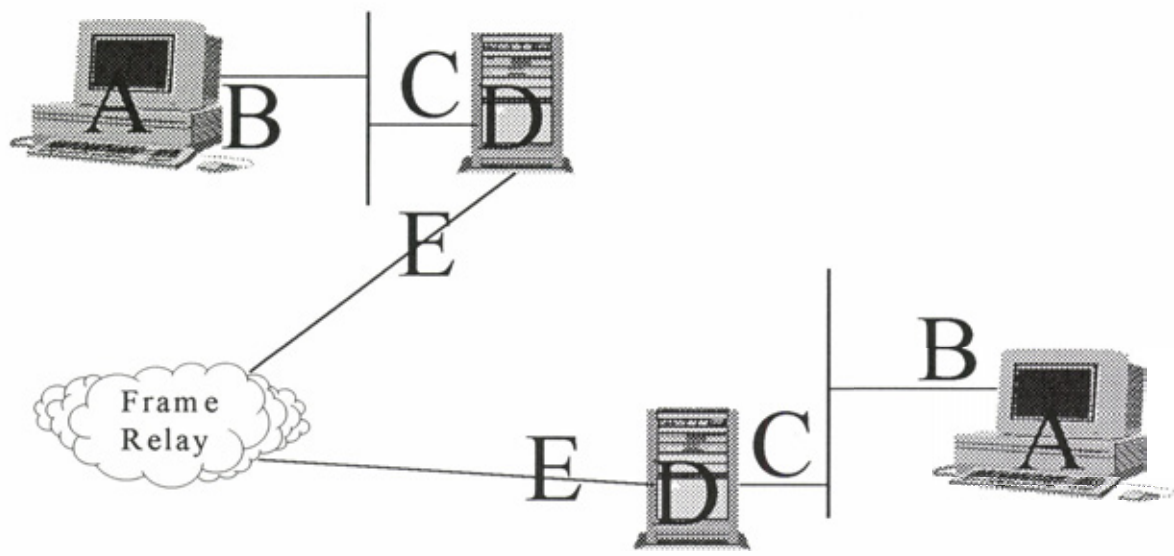

Abbildung 12 Einbettung von Schutzmöglichkeiten

Die Frage der OSI Schicht muss auch gestellt werden. Für die Schichten 1, 2, 3 und 7 gibt es handelsübliche Lösungen. Bei den anderen Schichten muss man unter Umständen eine neue Variante in Betracht ziehen.

5.4 Kryptografische Sicherheit / Schlüsselverwaltung

Der Entscheid bezüglich der geforderten kryptografischen Sicherheit / Schlüsselverwaltung bereitet oft Schwierigkeiten. Dies darum, weil vielfach Fachkenntnisse fehlen.

Der schwierigste und aufwendigste Ansatz zum Brechen eines Algorithmus ist derjenige der "Brute Force Attack", sofern der Algorithmus derart aufgebaut ist, dass keine Attacke

wirkungsvoller ist als das Durchprobieren aller möglichen Schlüssel. Im Falle der DES ähnlichen Algorithmen ist diese Bedingung erfüllt. Bruce Schneier hat Überlegungen angestellt, wie lange das Probieren dauert, unter der Annahme von verschieden hohen zur Verfügung stehenden Budgets [1]. Abbildung 13 zeigt einen Auszug aus seinen Resultaten.

Schätzung der durchschnittlich benötigten Zeit für eine "Brute Force Attack" bei DES ähnlichen Algorithmen; Stand der Rechenleistung im Jahre 1995 *)

	Schlüssellänge in Bit					
Kosten	**40**	**56**	**64**	**80**	**112**	**128**
US$100k	2 s	35 h	1 y	70'000 y	10^{14} y	10^{19} y
US$1M	0.2 s	3.5 h	37 d	7'000 y	10^{13}y	10^{18} y
US$10M	0.02 s	21 min	4 d	700 y	10^{12}y	10^{17} y
US$100M	0.002 s	2 min	9 h	70 y	10^{11}y	10^{16} y

*) = gemäss "Applied Cryptography" von Bruce Schneier

Abbildung 13 "Brute Force Attack": Schlüssellänge versus Aufwand und Zeit

Der Aufwand zum Brechen der Schlüssel mittels der "Brute Force Attack" in Abbildung 13 gilt für DES ähnliche, symmetrische Algorithmen. Für asymmetrische Verfahren, wie sie in öffentlichen Verfahren verwendet werden, gelten für die Schlüssellängen bei gleichem Aufwand in Bezug auf Kosten und Zeit grössere Werte. Entsprechende Vergleichsangaben von Bruce Schneier [1] sind in Abbildung 14 enthalten.

Ähnliche Stärken bei "Brute Force Attack" *)

Symmetrische Schlüssellänge (DES ähnlich)	"Public-Key" Schlüssellänge (RSA System)
56 Bit	384 Bit
64 Bit	512 Bit
80 Bit	768 Bit
112 Bit	1792 Bit
128 Bit	2304 Bit

*) = gemäss "Applied Cryptography" von Bruce Schneier

Abbildung 14 Vergleichbare Schlüssellängen für DES und RSA Algorithmen

5.5 Kosten des Schutzes im Verhältnis zu den Kosten der Datenerstellung

Kosten des Schutzes im Verhältnis der Kosten zum Erstellen der Daten am Beispiel einer 2 Mbit/s Frame Relay Chiffrierung:

- Kosten der Chiffriergeräte zirka CHF 24'000.- pro Paar
- Abschreibung in 5 Jahren: CHF 400.- pro Monat
- Übertragung von 65 GBytes/Monat bei 10 % Kapazitätsauslastung (dies entspricht zirka 16 Mio. gedruckten A4 Seiten)
- Kosten zum Schutz eines 100 Seiten Dokumentes: 0.25 Rappen
- Kosten zum Erstellen eines 100 Seiten Dokumentes: CHF 25'000 bis 2.5 Mio.
- Relative Kosten des Schutzes: $10^{-7}...10^{-9}$

Abbildung 15 Verhältnis der Kosten: Datenerstellung versus Kommunikationsschutz

Die relativen Kosten des Schutzes sind also sehr klein. Die Kosten eines Verlustes an Geschäftsaufträgen oder an Image sind darin noch nicht eingerechnet. Sie können beträchtlich sein, sind aber auch schwierig zu schätzen.

6 Schlussbemerkungen

Lösungen zum Schutz von Daten sind im Markt erhältlich, decken aber nie das ganze Spektrum an womöglich benötigten Komponenten ab. Zu Beginn ist immer eine Risikoanalyse durchzuführen und dann ein Sicherheitskonzept zu erstellen. Dabei werden vorteilhafterweise Schwerpunkte gesetzt um Kosten zu sparen. Die nun notwendige Evaluation ist schwierig, aber nötig und erfordert Zeit und Geld. Lieferanten von Chiffrierlösungen können dabei Hilfe bieten. Eine Beschaffung von Chiffrierlösungen ohne seriöse Risikoanalyse, Sicherheitskonzept und Evaluation kann sehr rasch in Fehlinvestitionen ausarten.

7 Literaturverzeichnis

[1] Bruce Schneier "Applied Cryptography", second edition, Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 1996