Realisierung einer Verschlüsselungstechnik für Daten im ISDN B-Kanal

Diplomarbeit

Technische Fachhochschule Berlin

Fachbereich 13 - Technische Informatik

Wintersemester 1997/1998

Boris Floricic

Betreuer: Prof. Dr. rer. nat. C. Kordecki

Gutachter: Prof. Dr. Ing. Buchholz

Vorsitzender: Prof. Bormann

Formale Anlage

Hiermit versichere ich, daß ich die vorliegende Diplomarbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Berlin, den 06 Januar 1998

.....

Unterschrifft (Boris Floricic)

Aufgabenblatt

Die Privatsphäre eines jeden wird durch die zunehmende Vernetzung der Rechenanlagen im Internet und die zunehmende Auswertbarkeit von Daten und Fakten bedroht. Multiplexen von Signalströmen in einem Kabel erlaubt mit einfachster Technik eine Vielzahl von Signalquellen zu beobachten und ggf. auch zu sabotieren. Um die Sicherheit im Datenverkehr zwischen Rechnern zu verbessern werden Zugangskontrollen durch Passworte, Fingerprints durch digitale Signatur bei der Datenübertragung und Speicherung eingerichtet.

Das größte Übertragungsaufkommen, das Telefongespräch, ist bis heute aber ohne jeglichen Schutz, egal ob über öffentliche Leitungen oder über das Internet telefoniert wird. Es ist daher die Aufgabe dieser Diplomarbeit ein Konzept zu entwerfen, bei den die Sprachübertragung beim telefonieren gegen Manipulationen jeglicher Art so geschützt wird, daß die beteiligten Telefoniepartner eine Manipulation erkennen können und eine Interpretation der Nutzdaten einem Dritten erschwert wird.

Die Arbeit wird in zwei Teile aufgespalten und als getrennte Diplomarbeiten vergeben:

1. Die Analyse des ISDN Signalisierungakanals (D-Kanal),

   Dokumentation der erforderlichen und der optionalen Signalisierungen,

   a) Telefon,

   b) Fax,

   c) Daten

   Erkennung und Implementierung der erforderlichen Handshakesignale auf einem µP- Kern. Darstellung unerwünschter Signalisierungen.

   Test und Monitoring des Signalverhaltens am S0 Bus,

   Zustandsdarstellung des D-Kanals am Telefon-Display.

2. Analyse und Entwurf eines Datenschutzkonzeptes,

   Begründung und Dokumentation des gewählten Schutzmechanismus

   Entwurf eines ISDN-Telefons mit Integration der gewählten Verschlüsselungstechnik (die Echtzeiteigenschaft eines Telefongesprächs ist zu berücksichtigen)

   Erstellung einer Leiterplatte zur Diplomarbeit auf der die Verschlüsselung und das Verhalten des Telefons bei unterschiedlichen Betriebsarten in einem Versuchsaufbau demonstriert werden kann.