Vorlesungsmodul Datenschutz und Datensicherheit - VorlMod DatSchu -

Matthias Ansorg

18. März 2003 bis 26. März 2005

Zusammenfassung

Studentische Mitschrift zur Vorlesung »Datenschutz und Datensicherheit« bei Prof. Dr. W. Schmitt und Herrn Hajo Köppen (Sommersemester 2003) im Studiengang Informatik an der Fachhochschule Gießen-Friedberg. Dieses Dokument ist identisch zu [1] und [6] gegliedert. Einige Kenntnisse in Rechnernetzen sind für den Teil »Datensicherheit« vorteilhaft.

- **Bezugsquelle:** Die vorliegende studentische Mitschrift steht im Internet zum Download bereit. Downloadquelle: Persönliche Homepage Matthias Ansorg http://matthias.ansorgs.de/InformatikDiplom.
- **Lizenz:** Diese studentische Mitschrift ist public domain, darf also ohne Einschränkungen oder Quellenangabe für jeden beliebigen Zweck benutzt werden, kommerziell und nichtkommerziell; jedoch enthält sie keinerlei Garantien für Richtigkeit oder Eignung oder sonst irgendetwas, weder explizit noch implizit. Das Risiko der Nutzung dieser studentischen Mitschrift liegt allein beim Nutzer selbst. Einschränkend sind außerdem die Urheberrechte der angegebenen Quellen zu beachten.
- **Korrekturen und Feedback:** Fehler zur Verbesserung in zukünftigen Versionen, sonstige Verbesserungsvorschläge und Wünsche bitte dem Autor per e-mail mitteilen: Matthias Ansorg <mailto:matthias@ansorgs.de>.
- **Format:** Die vorliegende studentische Mitschrift wurde mit dem Programm LyX (graphisches Frontend zu LaTeX) unter Linux geschrieben und mit pdfLaTeXals pdf-Datei erstellt. Grafiken wurden mit dem Programm xfig unter Linux erstellt und als pdf-Dateien exportiert.
- **Dozent:** Prof. Dr. W. Schmitt für Datensicherheit, Prof. Dr. Köppen für Datenschutz.
- **Verwendete Quellen:** [3], [4], [1].
- **Klausur:** Die Klausur findet vor den Semesterferien statt. Sie wird zur Hälfte von Prof. Dr. W. Schmitt und zur Hälfte von Herrn Köppen gestellt. Wer die Klausur unvorbereitet schreibt, wird sie aller Wahrscheinlichkeit nach nicht bestehen. Die Veranstaltung ist nicht schwer, man muss sich jedoch mit dem Stoff beschäfigt haben.
  Es gibt kein Buch, nach dem der Teil Datensicherheit der Vorlesung vorbereitet wurde - das Skript [1] ist recht ausführlich und reicht zur Vorbereitung der Klausur aus. In der Klausur werden die wichtigen Dinge aus dem gesamten Skript abgefragt, es bringt also zumindest für eine gute Note wenig, sich nur auf einige Schwerpunkte vorzubereiten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Teil I
Datensicherheit

1 Einführung

1.1 Problemstellung

1.1.1 Datensicherheit und Datensicherung

Datensicherheit Ziele der Datensicherheit für IuK-Systemen:

- die ordnungsgemäße Funktionsfähigkeit des Systems oder des Dienstes sicherstellen
- mißbräuchliche Benutzung, Erkundung und Manipulation eines Systems und seiner Daten verhindern
- Angriffe auf das System oder Systemteile abwehren. Dazu gehören Angriffe mit Viren oder »man in the middle«, aber auch Bombenattentate auf Rechenzentren.

Die zu ergreifenden Maßnahmen sind i.A. technischer, organisatorischer und personeller Art. Datensicherheit ist ein wichtiges Instrument zur Realisierung von Datenschutz. Nach heutigem Kenntnisstand ist eine absolute Datensicherheit unmöglich oder zumindest wirtschaftlich unmöglich. Maßnahmen der Datensicherheit:

technischer Art: Virenscanner, Firewall, Codekarten, ... Diese Maßnahmen reichen i.A. nicht aus!

organisatorischer Art: Abläufe festlegen wie Zutrittskontrolle in Firmen, . . .

personeller Art: Können mit den Maßnahmen organisatorischer Art zusammengefasst werden. Es geht darum, besonders vertrauenswürdige Personen für bestimmte Aufgaben auszuwählen, etwa durch Vorlage eines polizeilichen Führungszeugnisses oder Nachweis ausgeglichener Vermögensverhältnisse.

Datensicherheit wurde durch die Vernetzung aller Rechner zu einem gravierenden Problem. Die Zahl der Straftaten mit IT-Bezug hat in den letzten Jahren sehr wesentlich zugenommen. Das Problem der Datensicherheit in IuK-Systemen kann in zwei Bereiche aufgeteilt werden:

- Datensicherheit in Datenverarbeitungsanlagen einschließlich klassischen Rechnernetzten: »Datensicherheit im EDV-Bereich«
- Datensicherheit in diensteintegrierten Kommunikationssystemen und ihrer Anwendungen. Bestes Beispiel ist das Internet; das erste diensteintegrierte Kommunikationssystem in Deutschland war ISDN, gedacht als Infrastruktur für beliebige Kommunikation.

Datensicherung Datensicherung (Backup) ist ein Mittel der Datensicherheit. In dieser Veranstaltung nicht behandelt.

1.1.2 Datensicherheit im EDV-Bereich

Es gibt mehrere Arten der Computerkriminalität:

Manipulationen Verletzung der Integrität von Daten wie unerlaubte Änderungen des eigenen Kontostands. Gesetze etwa: §303a StGB Datenveränderung, §263a StGB Computerbetrug.

- Missbrächliches Ändern, Einfügen und Löschen von Eingabedaten und gespeicherten Daten.
- Missbrächliches Ändern von Programmen.
- Missbräuchliche Bedienung des Systems

Computerspionage Verletzung der Vertraulichkeit. Gesetze: §202a StGB Ausspähen von Daten.

- Unerlaubte Datenabfrage
- Unerlaubtes Kopieren von Datenbeständen
- Unerlaubtes Kopieren und Ausspionieren von Programmen

Unerlaubte Nutzung von Resourcen

- Unerlaubte Nutzung von Programmen (etwa Software-Piraterie)
- Unerlaubte Überlassung von Rechenkapazität an Dritte
- Unberechtigte Nutzung von Rechenkapazität für eigene Zwecke (evtl. zu Lasten Dritter)

Sabotage Einschränkung der Verfügbarkeit. Gesetze: §303b StGB Computersabotage.

Bei der Planung der Sicherheitsarchitektur verwendet man die Risikoanalyse als wichtiges Instrument. Bestandteile:

Schwachstellenanalyse Jeder Übergang zum öffentlichen Netz ist auch eine Schwachstelle, die beste Firewall ist der Seitenschneider. Allerdings sind manche Schwachstellen notwendig oder wirtschaftlich unvermeidbar, und nicht an jeder Schwachstelle lauert eine Gefahr.

Gefahrenanalyse An welcher der Schwachstellen lauern Gefahren.

1.1.3 Datensicherheit in diensteintegrierten Kommunikationssystemen

Seit etwa 1990 gibt es die Tendenz, diensteintegrierte Netze zu bauen statt ein Netz für jeden Dienst. Im Mobilfunkbereich ist UMTS ein Beispiel. Diese Tendenz verstärkt das Problem der Datensicherheit. Ausspähbare Daten werden aus zwei Sichten in je drei Arten unterteilt:

Netzbetreibersicht

Nutzdaten

Bestandsdaten Dazu gehören auch Daten über softwaredefinierte Teilnehmerverhältnisse: ein Begriff aus dem »Intelligenten Netz« (IN) der Telekom, wo über Software definiert wird, welche Verbindung bei welcher Nummer aufgebaut werden soll, z.B. bei 0800-Nummern, wo eine deutschlandweite Nummer ortsabhängig an verschiedene Kundendienststellen weitergeleitet werden kann.

Verbindungsdaten Verbindungsdaten treten vor allem in den Komponenten des Signalisierungssystems auf; im Internet besteht es aus den unteren Protokollschichten (TCP/IP), in Telefonnetzten aus eigenen Leitungen.

Angreifersicht

Inhaltsdaten

Interessensdaten

Verkehrsdaten

1.2 Schutzziele für IuK-Systeme

Wichtiges Mittel der Authentikation beim Telefonieren ist das Erkennen der Stimme; dieses Mittel ist bei hoher Komprimierung nicht mehr anwendbar, weshalb manche Banken die Authentikation dann nicht mehr durchführen.

1.3 Standardisierung, Regulierung und Zertifizierung

1.4 Literatur

2 Entwurf und Betrieb von sicheren IuK-Systemen

2.1 Sicherheitsprozess

2.2 Schwachstellenanalyse

2.3 Gefahrenanalyse

2.3.1 Gefahrenarten - Grundbedrohungen und Grundwerte der IuK-Sicherheit

2.3.2 Angriffe

Angriffszyklus

Passive Angriffe

Aktive Angriffe

Social Engineering

2.3.3 Ein Fragenkatalog zur Klärung der Sicherheitssituation

2.4 Detaillierte Risikoanalyse

2.5 Grundschutzansatz

2.6 Sicherheitspolitik

2.7 Sicherheitsdienste

2.7.1 Grundsätzliches

2.7.2 Technische Sicherheitsdienste

2.7.3 Organisatorische Sicherheitsdienste

2.8 Sicherheitsmechanismen und -maßnahmen - Übersicht

2.8.1 Sicherheitsmechanismen

2.8.2 Sicherheitsmaßnahmen

2.9 Sicherheitsmanagement

2.9.1 Übersicht

2.9.2 Sicherheitsaudits

2.10 Literatur

2.11 Anhang: Risiko

2.12 Anhang: Intrusion Detection Systeme (IDS)

2.13 Anhang: Computer Emergency Response Team (CERT)

3 Verschlüsselung und digitale Signatur

In diesem Teil werden zwei der angesprochenen Sicherheitsmechanismen ausführlich besprochen: Verschlüsselung und digitale Signatur.

3.1 Verschlüsselung mit geheimen Schlüsseln

3.1.1 Grundbegriffe und Prinzip

Der Nachfolger von DES ist AES. DES hat lange Jahre gut funktioniert, obwohl er veröffentlicht war. Der A-5 Algorithmus der im GSM-Mobilfunk verwendet wird wurde dagegen versucht, geheim zu halten; er ist heute nicht mehr geheim. Das bedeutet jedoch nicht, dass Verschlüsselung mit A-5 unsicher ist! Veröffentlichung von Verschlüsselungsalgorithmen mit anschließender Diskussion ist vorteilhaft, weil Schwachstellen im Algorithmus vor seinem Einsatz erkannt werden können. Von geheimen Algorithmen glaubt man dagegen nur, sie seien sicher, man weiß es jedoch nicht wirklich.

3.1.2 Kryptoanalyse und Sicherheit von Kryptosystemen

Der »brute force«-Angriff besteht darin, den gesamten Schlüsselraum durchzuprobieren. Es gibt also nie absolute Sicherheit, aber praktische Sicherheit.

3.1.3 DES - Data Encryption Standard

Historie und grundlegende Eigenschaften von DES DES hat 56 Bit Schlüssellänge. Das gilt heute als kurz, man verwendet heute mindestens 128 Bit. Den Schlüssel zu raten ist damit fast ausgeschlossen.

Sicherheit von DES

Triple - DES

3.1.4 Betriebsarten für Blockchiffren

3.2 Verschlüsselung mit öffentlichen Schlüsseln

3.2.1 Grundbegriffe und Prinzip

3.2.2 RSA-Algorithmus

3.3 Digitale Signatur

3.3.1 Grundbegriffe und Prinzip

3.3.2 Erzeugung digitaler Signaturen mittels RSA

3.3.3 Urheber- und Empfängernachweis

3.4 Aspekte des Schlüsselmanagements

3.4.1 Aufgaben des Schlüsselmanagements

3.4.2 Authentifizierung öffentlicher Schlüssel mittels MAC - Direktes Vertrauen

3.4.3 Authentifizierung öffentlicher Schlüssel durch dritte Instanzen

Vertrauenswürdige Instanzen und Zertifikate

Zentral verwaltete Zertifikate - Vertrauenshierachien

3.5 Literatur

4 Aufgabensammlung Datensicherheit

Hier wurden alle Aufgaben aus [3], [4] integriert, darüber hinaus selbst erfundene Aufgaben im Stil der Klausuraufgaben zu allem noch nicht abgedeckten wesentlichen Stoff aus dem Skript [1]. Diese somit vollständige Aufgabensammlung eignet sich durch die Frage- und Antwortform gut, um nach dem Lesen des Skriptes den für die Klausur benötigten Stoff auswendig zu lernen.

Die Reihenfolge der Aufgaben folgt dem Stoff in [1] und damit auch dem Stoff in diesem Dokument.

4.1 Definition Datensicherheit

Aufgabe Definieren Sie »Datensicherheit« und grenzen sie »Datenschutz« davon ab!

Lösung Datensicherheit ist der Zustand eines IuK-Systems, in dem durch technische, organisatorische und personelle Maßnahmen garantiert ist:

- ordnungsgemäßes Funktionieren des IuK-Systems
- Unmöglichkeit, das IuK-System oder seine Daten missbräuchlich zu benutzen, zu erkunden oder zu manipulieren
- erfolgreiche Abwehr von Attacken zur Zerstörung des Systems

Datensicherheit beugt der Computerkriminalität vor und ist Werkzeug des Datenschutzes. Datenschutz selbst verwirklicht das aus den Grundrechten abgeleitete Persönlichkeitsrecht, über Preisgabe und Verwendung seiner personenbezogenen Daten selbst bestimmen zu dürfen.

4.2 Formen der Computerkriminalität

Aufgabe Nennen Sie die verschiedenen Formen der Computerkriminalität, jeweils mit Beispielen!

Lösung

Manipulationen (Verletzung der Integrität)

- Missbräuchliches Ändern, Einfügen und Löschen von Eingabedaten und gespeicherten Daten.
- Missbräuchliches Ändern von Programmen.
- Missbräuchliche Bedienung des Systems.

Computerspionage (Verletzung der Vertraulichkeit)

- Unerlaubte Datenabfrage

- Unerlaubtes Kopieren von Datenbeständen
- Unerlaubtes Kopieren und Ausspionieren von Programmen

Unerlaubte Nutzung von Resourcen

- Unerlaubte Nutzung von Programmen (Software-Piraterie)
- Unberechtigte Nutzung von Rechenkapazität für eigene Zwecke
- Unberechtigte Überlassung von Rechenkapazität an Dritte

Sabotage (Einschränkung der Verfügbarkeit)

- an der Rechner-Hardware
- an den Datenbeständen
- an den Programmen

4.3 Datensicherheit im EDV-Bereich zur Zeit vernetzter Systeme

Aufgabe Welchen neuen Anforderungen werden von der Einführung vernetzter Systeme an die »Datensicherheit im EDV-Bereich« gestellt?

Lösung

1. Rechner sind nicht mehr nur Großrechner in isolierten Räumen, sondern auch vernetzte PCs, Workstations und Terminals am Arbeitsplatz. Statt durch räumliche Isolation muss Datensicherheit nun durch Software garantiert werden. Beispiele: Passwortschutz, Virenscanner, Firewalls.
2. Datensicherheit darf sich nicht mehr auf einen Rechner beschränken, sondern muss das gesamte Rechnernetz betrachten.
3. Besonders in heterogenen Netzen mit verschiedenen Zuständigkeitsbereichen ist es schwierig, Datensicherheit zu garantieren.

4.4 Datensicherheitsprobleme in diensteintegrierenden Kommunikationssystemen

Aufgabe Nennen sie die Probleme der Datensicherheit in diensteintegrierenden Kommunikationssystemen. Geben Sie jeweils an, ob das Problem Dienstnutzer, Dienstteilnehmer oder Dienstanbieter betrifft.

Lösung Dienstnutzer werden geschädigt, wenn ...

- ... die Diensterbringung vermindert, verzögert oder verändert wird.
- ... eine falsche Identität vorgetäuscht wird (masquerading).
- ... eine Kommunikationsbeziehung unter dem Namen und auf Kosten des Teilnehmers aufgebaut wird, ohne dass dieser es weiß oder billigt.
- ... eine Kommunikationsbeziehung bzw. deren Ergebnis abgestritten wird.

Dienstteilnehmer und Dienstanbieter werden geschädigt, wenn ...

- ... die Diensterbringung vermindert, verzögert oder verändert wird.
- ... ein gebührenpflichtiger Dienst kostenlos genutzt wird.

4.5 Nutzdaten, Bestandsdaten, Verbindungsdaten

Aufgabe Quelle: [4, Aufg. 6a], [3, Aufg. 6a][1]. Alice kommuniziert mit ihrem Freund Bob per E-Mail und Telefon und benutzt Dienste im Internet. Mallory hat die von Alice benutzten Kommunikationssysteme ausgespäht und ihre Kommunikationsaktivitäten abgehört. Ordnen Sie (durch Ankreuzen) in untenstehender Tabelle die von Mallory erspähten Daten (linke Spalte) genau einer der Kategorien Nutzdaten, Bestandsdaten oder Verbindungsdaten zu (technische Sichtweise des Netzbetreibers).

Lösung

Mallory hat u.a. erspäht:	Nutzdaten	Bestandsdaten von Alice	Verbindungsdaten
Die hg-Nr von Alice an der FH Gießen- Friedberg.		×	
Den verschlüsselten Inhalt einer von Alice gesendeten Datei.	×		
Die IP-Adresse des von Alice kontaktierten Web-Servers.			×
Das von Alices PC benutzte Schicht-2- Protokoll zur Einwahl ins Internet.		×	
Einen Sitzungsschlüssel für eine verschlüsselte E-Mail Übertragung			×
Name, Anschrift und Buchungsnummer von Alice in der Datenbank ihres Internet-Diensteanbieters.		×	
Von Alice angewählte Telefonnummern sowie Zeitpunkt und Dauer der von ihr geführten Gespräche.			×
Den Inhalt einer Kommunikation zwischen Alice und Bob.	×		
Das Volumen eines Datentransfers zwischen einem Dateiserver und Alices PC.			×
Die postalische Anschrift von Alice in einer von ihr gesendeten E-Mail.	×		

4.6 Inhaltsdaten, Interessendaten, Verkehrsdaten

Aufgabe Quelle: [4, Aufg. 6b], [3, Aufg. 6b][2]. Alice kommuniziert mit ihrem Freund Bob per E-Mail und Telefon und benutzt Dienste im Internet. Mallory hat die von Alice benutzten Kommunikationssysteme ausgespäht und ihre Kommunikationsaktivitäten abgehört. Ordnen Sie (durch Ankreuzen) in untenstehender Tabelle die von Mallory erspähten Daten (linke Spalte) genau einer dieser Kategorien zu.

[1] Jede dieser Klausuraufgaben enthielt jeweils nur eine halb so lange Tabelle wie die hier abgebildete.
[2] Jede dieser Klausuraufgaben enthielt jeweils nur eine halb so lange Tabelle wie die hier abgebildete.

Lösung

Mallory hat erspäht / erstellt:	Inhaltsdaten	Interessensdaten	Verkehrsdaten
Matrikel-Nr. und Note von Alice in einer an sie gerichteten E-Mail.	×		
Die Themengebiete der von Alice am häufigsten besuchten Webseiten.		×	
Die Häufigkeiten mit der Alice bestimmte IP-Adressen kontaktiert.			×
Ein Einmal-Passwort (TAN) zum Zwecke einer Banküberweisung.	×		
Ein Profil der von Alice beim Online- Shopping gekauften Waren.		×	
Alice besucht häufig die Homepages von Reisebüros.		×	
Datum und Ort für eine Verabredung zwischen Bob und Alice.	×		
Alice hat fünfmal von einem bestimmten Ort (Funkzelle) eine bestimmte Telefonnummer angewählt.			×
Alice bezieht per Internet eine Fachzeitschrift zum Thema Softwaretechnik.		×	
Das Passwort von Alice für den Zugang zum Online-Banking.	×		

4.7 Verkehrsdaten und ihre Erstellung

Aufgabe Nennen Sie Beispiele für Verkehrsdaten und woraus man sie jeweils erhält!

Lösung Allgemein gilt: Verkehrsdaten werden durch Interpretation der Verbindungsdaten und durch Verkehrsflussanalysen gewonnen. Beispiele für Verkehrsdaten und ihre Gewinnung:

Kommunikationsprofil aus Verbindungsdaten, die enthalten, wie lange und wie oft ein Teilnehmer mit wem kommunikziert.

Bewegungsprofile aus Verbindungsdaten von Mobilfunknetzen und Verkehrsleitsystemen, die enthalten, wann und wo sich ein Teilnehmer wie oft aufhält.

Kommunikationsschwerpunkt aus Verbindungsdaten, die zeigen, zwischen welchen Teilnehmern ein besonders reger Informationsaustausch besteht. Zwischen Konzernen kann dies z.B. auf eine Fusion hinweisen.

4.8 Schutzziele für IuK-Systeme

Aufgabe Was konkret wird man schützen, um Datensicherheit in einem IuK-System zu gewährleisten? - Nennen Sie die Schutzziele für IuK-Systeme!

Lösung

1. Vertraulichkeit der Daten (*data confidentiality*).

2. Möglichkeit, die Unversehrtheit der Daten zu erkennen (*data integrity*).
3. Möglichkeit, die Kommunikationspartner und den Datenurprung zu authentifizieren (*authentication*).
4. Verbindlichkeit von Aktivitäten (*non-repudiation*). Bestimmte Aktionen sollen nicht bestreitbar sein; dies geschieht im Wesentlichen durch Nachweis der eigenen Urheberschaft und der Tatsache des Empfangs.
5. Anonymität (*anonymity*). Manchmal wollen Sender oder Empfänger ihre Identität voreinander verbergen oder die Tatsache ihrer Kommunikation vor anderen verbergen.
6. Zugriffs- und Zugangskontrolle zum System (*access control*).
7. Verfügbarkeit (*availability*). Die zeitgerechte und korrekte Ausführung von Funktionen.

4.9 Orange Book und Red Book

Aufgabe Was für Dokumente sind »Orange Book« und »Red Book«? Wie unterscheiden sie sich?

Lösung Beide Dokumente sind sog. »Kriterienwerke«: Standards zur Bewertung der Datensicherheit in IT-Systemen. Weil das Orange Book dabei Rechnernetze ungenügend berücksichtigt, wurde es durch das Red Book ergänzt. Es wendet die im Orange Book formulierten Grundsätze auf Rechnernetze an. Beide Dokumente wurden vom US-amerikanischen Verteidigungsministerium herausgegeben.

4.10 VAT und RAT

Aufgabe Was sind VATs und RATs und wann im Sicherheitsprozess werden sie verwendet?

Lösung VAT: vulnerability assessment tool. RAT: risk assessment tool. Beides sind Softwarewerkzeuge, die einen Angriff auf ein IuK-System simulieren und so Schwachstellen und Gefahren aufdecken können. Sie werden in der Betriebsphase eines Sicherheitssystems im Rahmen des Sicherheitsmanagements bei Sicherheitsaudits verwendet. Dabei will man durch Analyse und Bewertung des Sicherheitssystems seine Schwachstellen erkennen und in folgenden Zyklen des Sicherheitsprozesses beheben.

4.11 Der Sicherheitsprozess

Aufgabe Stellen sie den Sicherheitsprozess grafisch dar und erläutern Sie kurz seine einzelnen Bestandteile.

Lösung Grafische Darstellung des Sicherheitsprozesses in Abbildung 1. Erläuterungen, wobei die Bezeichnungen der Tätigkeiten aus dieser Abbildung übernommen werden:

Schwachstellenanalyse Erkennen, welche Schwachstellen das IuK-System aufweist.

Gefahrenanalyse Erkennen, an welchen Schwachstellen dem IuK-System welche Gefahren durch einen Angriff drohen. Zusammen mit der Schwachstellnanalyse erhält man so qualifiziert Aufschluss über das Ausmaß der möglichen Schäden.

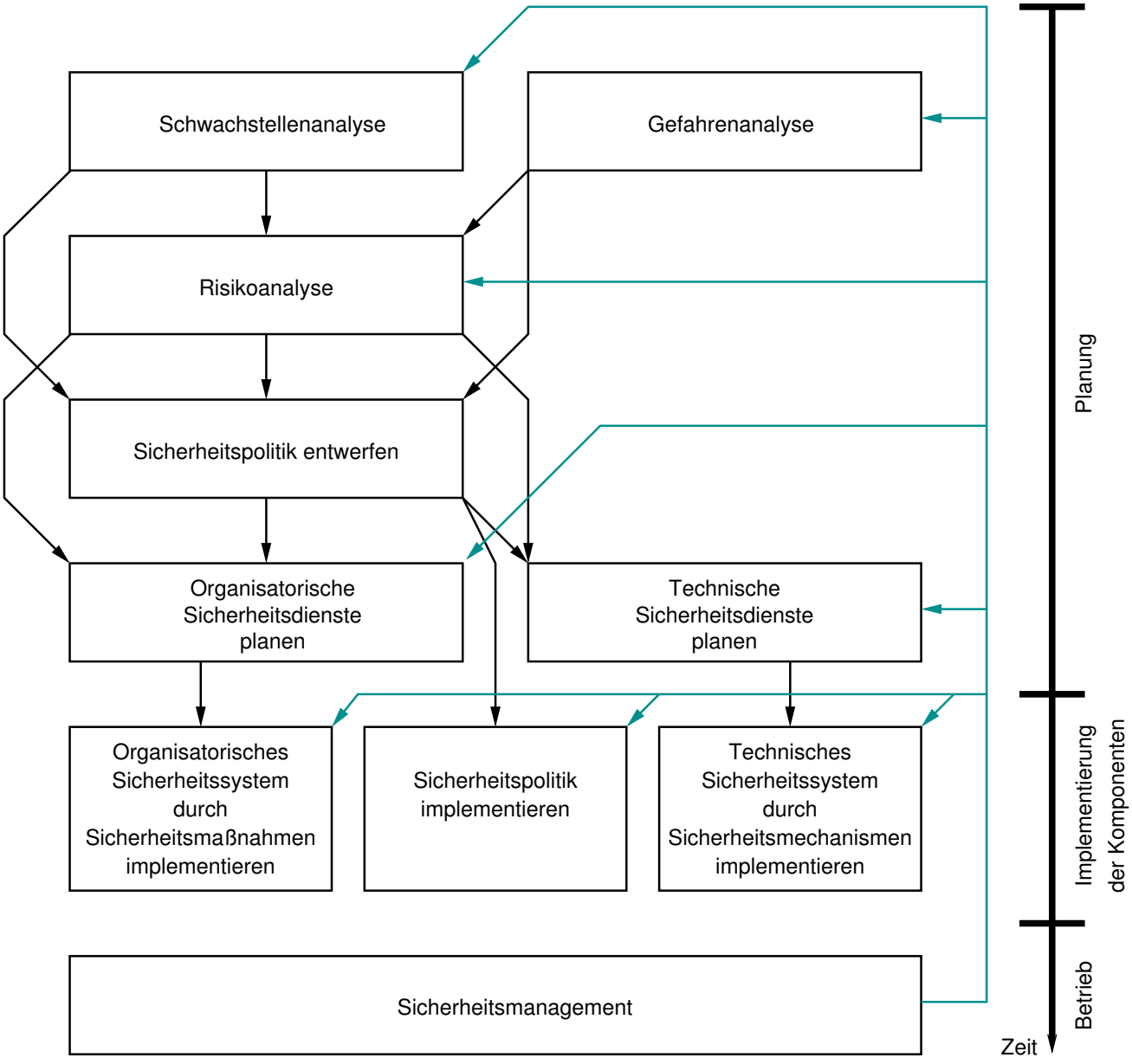

Abbildung 1: Der Sicherheitsprozess

Risikoanalyse Sind die möglichen Schäden »hoch« oder »sehr hoch«, so verwendet man eine detailierte Risikoanalyse, um das Sicherheitsrisiko genau einzuschätzen.

Organisatorische Sicherheitsdienste Implementierungsunabhängige Formulierung des Organisatorischen Sicherheitssystems.

Technische Sicherheitsdienste Implementierungsunabhängige Formulierung des Technischen Sicherheitssystems.

Organisatorisches Sicherheitssystem Bildet zusammen mit dem Technischen Sicherheitssystem das »Sicherheitssystem«.

Technisches Sicherheitssystem Bildet zusammen mit dem Organisatorischen Sicherheitssystem das »Sicherheitssystem«.

Sicherheitspolitik Definition von Regeln und Verfahrensweisen, nach denen die Übermittlung, Verarbeitung und Speicherung von Informationen erfolgen soll.

Sicherheitsmanagement Aufgaben:

- Durchführung und regelmäßige Überprüfung der Sicherheitspolitik.
- Administration von Rechten, IP-Adressen, Schlüsseln, ...
- Betrieb von Einbrucherkennungssystemen.
- Sicherheitsaudits unter Verwendung von VATs und RATs zur Überprüfung und Neubewertung der Sicherheitssituation.
- Analyse und Beachtung von CERT-Warnungen.

4.12 Elemente des Sicherheitsprozesses I

Aufgabe [4, Aufg. 7]. Ordnen Sie die folgenden Begriffe / Aussagen / Fragen genau einem der Gebiete »Schwachstelle«, »Schwachstellenanalyse«, »Angriff«, »Gefahrenanalyse«, »Risikoanalyse«, »Sicherheitspolitik« oder »Sicherheitsmanagement« zu.

Lösung

a)	Passwort geringer Komplexität.	Schwachstelle
b)	Wie hoch ist der mögliche Schaden bei einem Angriff?	Risikoanalyse
c)	Bestandsaufnahme für das zu schützende System.	Schwachstellenanalyse
d)	Trojanisches Pferd.	Angriff
e)	Erzeugen eines Pufferüberlaufs.	Angriff
f)	Durchführung von Sicherheitsaudits.	Sicherheitsmanagement
g)	Definition von Regeln für die Bildung von Passwörtern.	Sicherheitspolitik
h)	Eine in Bezug auf Sicherheit unzureichende Systemkonfiguration.	Schwachstelle
i)	Wie groß ist der materielle Aufwand für einen Angreifer?	Risikoanalyse
j)	Vor welchen aktiven Angriffen muss ein Server geschützt werden?	Gefahrenanalyse

4.13 Elemente des Sicherheitsprozesses II

Aufgabe Quelle: [3, Aufg. 7]. Ordnen Sie die folgenden Begriffe / Aussagen / Fragen genau einem der Gebiete »Schwachstelle / Schwachstellenanalyse«, »Gefahr / Gefahrenanalyse«, »Sicherheitsrisiko / Risikoanalyse«, »Sicherheitspolitik« oder »Sicherheitsmanagement« zu.

Lösung

a)	Denial of Service Angriff.	Gefahr / Gefahrenanalyse
b)	Sicherheitsaudit.	Sicherheitsmanagement
c)	Definition von Regeln für die Vergabe von Zugriffsrechten.	Sicherheitspolitik
d)	Computer Viren	Gefahr / Gefahrenanalyse
e)	Ausgeschiedene Mitarbeiter verfügen noch über Zugriffsrechte.	Schwachstelle / Schwachstellenanalyse
f)	Betrieb eines Einbruchserkennungssystems.	Sicherheitsmanagement
g)	Welche Kosten und welchen Nutzen hat ein potentieller Angreifer?	Sicherheitsrisiko / Risikoanalyse
h)	Social Engineering.	Gefahr / Gefahrenanalyse
i)	Unzureichende Kontrolle von Sicherheitsmaßnahmen.	Schwachstelle / Schwachstellenanalyse
j)	Penetrationstest.	Sicherheitsmanagement

4.14 Phasen der Schwachstellenanalyse

Aufgabe Nennen Sie die Phasen der Schwachstellenanalyse und beschreiben Sie kurz die Aufgabe jeder Phase.

Lösung

1. **Bestandsaufnahme.** Alle vorhandenen und geplanten IuK-Systeme werden systematisch erfasst, inkl. zugehöriger Organisation und zugehörigem Personal. Neben der technischen Infrastruktur werden also u.a. die Dienste und Anwendungen auf diesen IuK-Systemen, die bisherigen Sicherheitsmaßnahmen, -mechanismen und Schutzeinrichtungen, die geschäftsrelevanten Strukturen und die sicherheitsrelevanten Strukturen erfasst.

2. **Schwachstellen identifizieren.** Mögliche Angriffspunkte und mangelnden Schutz vor zufälligen Gefahren entdecken, in den Bereichen:

   - Konzeption und Organisation
   - Personal
   - Technik

3. **Schwachstellen minimieren (Systemhärtung).** Änderungen in drei Bereichen am System und seiner Konfiguration, um seine Sicherheit zu erhöhen:

   - Beschränken des Systems auf seine tatsächliche Anwendung durch Deaktivieren (Ports, ...) und Deinstallieren (Programme, ...) von Komponenten.
   - Aktivieren und Konfigurieren der systemeigenen Sicherheitsmechanismen entsprechend eigener Sicherheitspolitik.

- Aktualisieren des Systems durch Updates, Patches und Service Packs.

4. **Protokollierung.** Ergebnis der Schwachstellenanalyse in einem Protokoll festhalten.

4.15 Systemhärtung

Aufgabe Quelle: [4, Aufg. 9a]. Erläutern Sie den Begriff Systemhärtung und die damit verbundenen Maßnahmen.

Lösung Systemhärtung meint Änderungen in drei Bereichen am System und seiner Konfiguration, um seine Sicherheit zu erhöhen:

- Beschränken des Systems auf seine tatsächliche Anwendung durch Deaktivieren (Ports, ...) und Deinstallieren (Programme, ...) von Komponenten.
- Aktivieren und Konfigurieren der systemeigenen Sicherheitsmechanismen entsprechend eigener Sicherheitspolitik.
- Aktualisieren des Systems durch Updates, Patches und Service Packs.

Der durch solche Maßnahmen gegenüber der Standardkonfiguration erhöhte Stand von Sicherheit heißt »Discretionary Security«. Die Standardkonfiguration vieler Programme ist unsicher, um in vielen Anwendungen zu funktionieren.

4.16 Zufällige Gefahren

Aufgabe Nennen Sie die drei Kategorien zufälliger Gefahren und jeweils einige Beispiele!

Lösung

Höhere Gewalt

- Feuer
- Wasser
- Unwetter
- Krieg

Menschliches Versagen

- Fehlbedienungen
- Unwissenheit
- Nichtbeachtung oder Fehlinterpretation von Regeln
- leichte und grobe Fahrlässigkeit

Technisches Versagen

- konstruktive Schwachstellen behindern oder verhindern die Systemfunktion
- Veschleiß
- Übermittlungsfehler durch Rauschen, Übersprechen, Fehlverbindungen, ...

4.17 Aussagen vervollständigen

Aufgabe Quelle: [4, Aufg. 8a], [3, Aufg. 8a], selbst entwickelte Fragen. Vervollständigen Sie die folgenden Aussagen im Zusammenhang mit IuK-Sicherheit.

Lösung

1. Ein MAC ermöglicht die Entdeckung von Angriffen auf die *Integrität* von Daten.
2. Die Grundbedrohungen für IuK-Systeme sind:
   (a) *unbefugter Informationsgewinn (interception - Angriff auf die Vertraulichkeit)*
   (b) *unbefugte Veränderung von Information (modification - Angriff auf die Integrität)*
   (c) *unbefugte Beeinträchtigung der Funktionalität (interruption - Angriff auf die Verfügbarkeit)*
3. Die Grundwerte der IuK-Sicherheit sind:
   (a) *C - confidentiality: Vertraulichkeit*
   (b) *I - integrity: Integrität*
   (c) *A - availability: Verfügbarkeit*
4. Das Orange Book ist ein Standard für *die Bewertung der Datensicherheit in IT-Systemen.*
5. Verschlüsselung schützt vor *Verletzung der Vertraulichkeit von Daten.*
6. Bei einem Angriff mit ausgewähltem Klartext (Chosen-Plaintext-Attack) hat Mallory Zugang zu f_k, *dem mit dem Schlüssel k parametrisierten Verschlüsselungsalgorithmus* f.

4.18 Angriffszyklus

Aufgabe Nennen und beschreiben Sie die Phasen des Angriffszylus!

Lösung

1. **Zielsystem ausspähen.** Informationen erwerben über:
   - Softwarekonfiguration
   - Softwareversionen
   - Systemzustand
   - IP-Adressen
2. **Schwachstellen identifizieren.** Dazu werden die ausgespähten Daten verwendet.
3. **Angriff ausführen.** Beim Angriff werden die identifizierten Schwachstellen ausgenutzt. Ziel ist eine Möglichkeit zur Aneignung von Rechten.
4. **Rechte aneignen.** Mit neuen Rechten ist eine tiefergehende Ausspähung möglich: ein neuer Zyklus beginnt.

4.19 Tempest-Angriff

Aufgabe Was ist ein Tempest-Angriff?

Lösung Mit hochempfindlichen Empfängern werden elektromagnetische, akustische oder optische Signale von Rechnersystemen und Peripherie aufgezeichnet und dann analysiert. Das können Bildschirminhalte, Tastaturanschläge usw. sein. Ein Tempest-Angriff ist ein passiver, d.h. nur lesender Angriff.

4.20 Computervirus

Aufgabe Quelle: [4, Aufg. 8c]. Was ist ein Computervirus?

Lösung Ein nur in Wirtsprogrammen lauffähiges Programmstück folgender Funktionalität:

Infektionsfunktion Mindestens ein weiteres Programm mit einer evtl. modifizierten Kopie ihrer selbst infizieren.

Schadensfunktion Schaden herbeiführen durch Ausführung eigener Anweisungen vor denen des Wirtsprogramms.

Nach der Art des Wirtsprogramms unterscheidet man:

Boot-Viren in Boot-Code

Datei-Viren in gewöhnlichen Programmen

Makro-Viren in selbstdefinierbaren Makros von Anwendungsprogrammen

Script-Viren in interpretierten Scripten

4.21 Trojanisches Pferd

Aufgabe Was ist ein Trojanisches Pferd?

Lösung Ein scheinbar harmloses Programm mit verdeckter Schadensfunktion, die die Rechte des gutgläubigen Benutzers ausnutzt.

4.22 Grundschutzansatz

Aufgabe Definieren Sie »Grundschutzansatz« und diskutieren Sie seine Vor- und Nachteile«!

Lösung Das »IT-Grundschutzhandbuch« des Bundesamts für Sicherheit in der Informationstechnik (BSI) enthält den »Grundschutzansatz« als Bausteine für ein Standard-Sicherheitssystem.
Vorteile

- Oft ist bereits durch diese Standard-Schutzmaßnahmen ausreichende Datensicherheit gegeben.
- Gute Basissicherung bei höheren Sicherheitsanforderungen.
- Pragmatischer de-facto Standard der Datensicherheit in vielen Unternehmen und Behörden Deutschlands.

- Effektiver IT-Grundschutz kann durch lizensierte IT-Grundschutz-Auditoren zertifiziert werden.
- Nichtkommerzieller Träger, daher kostenfreie Anwendung und langfristige Wartung sicher.

Nachteile

- Dieser nationale Ansatz ist in internationalen IT-Verbünden schwierig anzuwenden.
- Diesem nationalen Alleingang ist eine analoge internationale Übereinkunft vorzuziehen bzw. hinzuzufügen.
- Mängel im IT-Grundschutzhandbuch kompromittieren alle anwendenden Systeme gleichermaßen.

4.23 Grundsatz der Sicherheitspolitik

Aufgabe Was sollte der Grundsatz einer jeden Sicherheitspolitik sein? Warum?

Lösung »Alles, was nicht explizit erlaubt ist, ist verboten«. Sicherheitsbeauftragte müssen beim Konfigurieren des Systems alles Erlaubte explizit erlauben und werden dabei stets die möglichen Folgen ihres Handelns überdenken (Warnmechanismus).

4.24 Fragen an eine Sicherheitspolitik

Aufgabe Nennen Sie aus folgenden Bereichen Fragen, die eine Sicherheitspolitik zu beantworten hat: Zugriffskontrolle und Umgang mit Daten; Implementierung des Sicherheitssystems; Protokollierung, Auswertung, Alarme; Organisation und Durchsetzung der Sicherheitspolitik.

Lösung

- Zugriffskontrolle und Umgang mit Daten
  1. Wie werden Passwörter ausgewählt, gewechselt, aufbewahrt, . . . ?
  2. Wer darf auf welche Daten wie zugreifen?
  3. An wen dürfen welche Daten übermittelt werden?
  4. Bei welchen empfangenen Daten ist ihr Ursprung zu überprüfen?
  5. Welcher Datenaustausch muss rechtsgültig sein?
- Implementierung des Sicherheitssystems
  1. Welche Sicherheitsdienste werden wann benötigt?
  2. Wodurch werden die Sicherheitsdienste implementiert?
  3. An welcher Stelle im System (z.B. in welcher OSI-Schicht) werden die Sicherheitsdienste implementiert?
- Protokollierung, Auswertung, Alarme
  1. Welche Ereignisse werden protokolliert?
  2. Nach welcher Strategie werden Protokolle ausgewertet?

3. Wie lange werden Protokolle aufbewahrt?
4. Welche Ereignisse lösen Alarme aus?
5. An wen werden Alarme gemeldet?
6. Was ist bei Alarmen zu tun?

- Organisation und Durchsetzung der Sicherheitspolitik

1. Mit welchen (organisatorischen und technischen) Maßnahmen wird für die Einhaltung der Sicherheitspolitik gesorgt?
2. Wie werden die technischen und organisatorischen Sicherheitsdienste im laufenden Betrieb überwacht?
3. Wer trägt die Verantwortung für die Sicherheitspolitik?
4. Wie und wann wird die Sicherheitspolitik weiterentwickelt?

4.25 Rechtlicher Rahmen der Sicherheitspolitik

Aufgabe Nennen Sie rechtliche Einflussfaktoren auf die Sicherheitspolitik!

Lösung

- Grundgesetz (GG)
- Bundesdatenschutzgesetz (BDSG)
- Informations- und Kommunikationsdienstegesetz (IuKDG). Es enthält das Signaturgesetz und Bestimmungen zum Schutz von Verbindungs- und Abrechnungsdaten.
- bilaterale Absprachen und Verträge zwischen Unternehmen und Kunden

4.26 NTCB und SMIB

Aufgabe Was sind NTCB und SMIB und wofür werden sie verwendet?

Lösung Die *network trusted computing base* (NTCB) ist der im Red Book vorgeschlagene sichere Ort, um die Regeln der Sicherheitspolitik und die Sicherheitsparameter eines Sicherheitsbereichs zu speichern: eine sichere Datenbank im Netzwerk, nur über festgelegte Schnittstellen zugänglich. Zusammen mit den o.g. Daten wird sie im OSI Security Management als *security management information base* (SMIB) bezeichnet. Sie unterstützt die Teilsysteme als Datenbank bei der Durchsetzung ihrer lokalen Sicherheitspolitik. Benutzer können hier also jederzeit die für sie relevanten Regeln der Sicherheitspolitik nachschlagen.

4.27 Warum Sicherheitsdienste?

Aufgabe Warum definiert man Sicherheitsdienste, statt den Gefahren direkt durch ein Sicherheitssystem zu begegnen?

Lösung Die Vorteile sind:

1. Entkopplung von Funktion und Realisierung der Sicherheitsvorkehrungen (Abstraktionsprinzip).

2. Das Sicherheitssystem kann dem technischen Fortschritt einfach angepasst werden. Es muss ja nur die Implementierung (Sicherheitssystem), nicht aber das Konzept (Sicherheitsdienste) geändert werden!

3. Die Sicherheitsmechanismen können problemlos in offene Kommunikationssysteme nach ISO 7498 eingebunden werden.

4. Sicherheitsdienste können als Module in einem vollständigen standardisierten Satz bereitgestellt werden (Modularitätsprinzip). Mit diesen Modulen kann man dann eine gestufte (»hierarchische«) Sicherheitsarchitektur realisieren.

4.28 Technische Sicherheitsdienste

Aufgabe Beschreiben Sie die in ISO 7498-2 (»Referenzmodell für offene Systeme - Sicherheitsarchitektur«) genannten Technischen Sicherheitsdienste, zusätzlich noch »Verfügbarkeit« und »Anonymität«.

Lösung

1. Authentifikation (*authentication*)

   (a) Authentifikation auf Partnerebene (*peer entity authentication*)
   Beide Kommunikationspartner beweisen ihre Identität, entweder durch Besitztum, Wissen oder Merkmale. So weiß der Benutzer, dass es sein System ist (z.B. kein manipulierter Kartenleser) und das System weiß, dass es ein berechtigter Benutzer ist. Auch können alle Aktionen ihren Urhebern zugeordnet werden. Neben dieser zweiseitigen gibt es auch die weniger sichere einseitige Authentifikation.

   (b) Authentifikation des Datenursprungs (*authentication of data origin*)
   Soll verhindern, dass sich ein Dritter in eine auf Partnerebene authentifizierte Verbindung einschaltet und unter der Identität eines der Partner Daten versendet und empfängt (*masquerading*). Datenursprung kann durch digitale Signatur authentifiziert werden.

2. Zugriffskontrolle (*access control*)
   Schützt das IuK-System vor unerlaubtem Zugriff auf seine Resourcen. Realisiert von Betriebssystemen und sonstiger Verwaltungssoftware, ausgehend von authentifizierten Benutzern. Man unterscheidet benutzerbestimmte und systembestimmte Zugriffskontrolle.

3. Vertraulichkeit von Daten (*data confidentiality*)
   Schützt Daten vor passiven Angriffen: vor unberechtigter Einsicht Dritter.

4. Integrität von Daten (*data integrity*)
   Schützt Daten vor aktiven Angriffen: Verfälschung, Erweiterung, Reduzierung, Reihenfolgeänderung, ... Oft enthalten im Dienst »Authentifikation des Datenursprungs«.

5. Nichtbestreitbarkeit bestimmter Aktivitäten (*non-repudiation*)
   Notwendig für rechtsgültigen Informationsaustausch. Mit dem Urhebernachweis kann der Empfänger beweisen: eine Nachricht wurde von einem bestimmten Absender erzeugt. Mit dem Emfängernachweis kann der Absender beweisen: eine Nachricht wurde von einem bestimmten Empfänger empfangen.

6. Protokollierung (*auditing*)
   Um Angriffe und Missbrauch zu beweisen und um Schwachstellen zu erkennen.

7. Verfügbarkeit (*availability*)
   Garantiert eine unterbrechungsfreien, zeitgerechten und korrekten Betrieb des IuK-Systems.

8. Anonymität (*anonymity*)
   Gegenteil der Authentifikation: Schützt Kommunikationspartner davor, ihre Identität voreinander oder die Tatsache ihrer Kommunikation vor anderen preiszugeben.

4.29 Authentikation auf Partnerebene

Aufgabe Quelle: [3, Aufg. 9a]. Erläutern Sie den Sicherheitsdienst Authentikation auf Partnerebene Mit welchen Mitteln / Sicherheitsmechanismen kann dieser Sicherheitsdienst prinzipiell realisiert werden und welche Ziele sollen mit diesem Dienst erreicht werden?

Lösung Bei Authentifikation auf Partnerebene (*peer entity authentication*) beweisen beide Kommunikationspartner ihrem Kommunikationspartner ihre Identität. Dieser Dienst kann prinzipiell realisiert werden durch:

- Mechanismen gegen die Verletzung der Vertraulichkeit
- Authentifikationsmechanismen
  - Authentifikation durch Besitztum (etwa durch einen maschinenlesbaren Ausweis)
  - Authentifikation durch Wissen (durch Kenntnis einer geheimen Information, etwa eines Passworts oder von Punkten in einer Grafik.
  - Authentifikation durch Merkmale (etwa durch biometrische Merkmale)
- Digitale Signatur
- Beglaubigung

Durch die zweiseitige Authentifikation verfolgt man vor allen drei Ziele:

- Das System soll berechtigte Benutzer erkennen und somit unberechtigte Benutzer ausgrenzen können.
- Der Benutzer soll »sein« System erkennen können und manipulierte Systemteile (etwa Kartenleser) ausgrenzen können.
- Alle Aktionen sollen ihren Urhebern zugeordnet werden können.

Neben dieser zweiseitigen gibt es auch die weniger sichere einseitige Authentifikation.

4.30 Organisatorische Sicherheitsdienste

Aufgabe Nennen und beschreiben Sie die organisatorischen Sicherheitsdienste!

Lösung Organisatorische Sicherheitsdienste sind nicht standardisiert. Die folgende Einteilung richtet sich nach [10].

1. Zugangskontrolle
   Regeln des Zugangs zu Rechnerräumen, Verteilzentren, Vermittlungs- und Übertragungseinrichtungen und Endgeräten. Benutzerrechte festlegen und kontrollieren.

2. Protokollierung
   Systematisches und regelmäßiges Auswerten der Protokolle. Prüfen, wer wann wozu Zugang hatte.

3. Vertraulichkeit der Daten
   Kriterien definieren, um Daten nach Grad der Vertraulichkeit einstufen zu können. Regeln definieren, wer mit den Daten welcher Vertraulichkeit umgehen darf.

4. Vertrauenswürdiger Betrieb
   Betrieb der IuK-Systeme so organisieren, dass Datensicherheit garantiert ist. Beispiel: Regeln für den Umgang der Mitarbeiter mit Disketten und CDs.

5. Vertrauenswürdiges Personal
   Betrifft die Sicherheitsaspekte bei Auswahl, Probezeit, Kündigung, Qualifikation und Sicherheitsbewusstsein der Mitarbeiter.

4.31 Routingkontrolle

Aufgabe Erläutern Sie den Sicherheitsmechanismus »Routingkontrolle«!

Lösung Der Teilnehmer kann dadurch den Übertragungsweg einer Verbindung ändern, wenn er einen Angriff auf den aktuellen Übertragungsweg vermutet. In den klassischen Netzen inkl. ISDN ist es technisch nicht möglich, dass der Teilnehmer den Leitweg bestimmt. Im Internet ist es über die Auswahl des Gateways eingeschränkt möglich.

4.32 Beglaubigung

Aufgabe Erläutern Sie den Sicherheitsmechanismus »Beglaubigung«!

Lösung Um Rechtssicherheit elektronischer Geschäftsvorgänge zu garantieren, kann man die Kommunikation über einen Netznotar abwickeln. Dies ist ein neutraler und vertrauenswürdier Server, der Teilnehmeridentitäten, Kommunikationszeitpunkt, Inhaltsdaten usw. beglaubigen kann.

4.33 Sicherheitsmaßnahmen

Aufgabe Nennen Sie einige übliche Sicherheitsmaßnahmen!

Lösung

1. Maßnahmen gegen Schäden durch höhere Gewalt und Sabotage
2. Aufgabenanalyse und Stellenbeschreibung
3. Personalentwicklungsplan, Stellenbesetzungsplan, Ausbildungsplan
4. Vorschriften festlegen
5. Sicherheitsstellen schaffen
6. Test- und Echtbetrieb trennen

4.34 Sicherheitsaudit

Aufgabe Quelle: [4, Aufg. 9b]. Erläutern Sie den Begriff Sicherheitsaudit und die damit verbundenen Maßnahmen.

Lösung Sicherheitsaudits werden regelmäßig während des Betriebs eines IuK-Systems im Rahmen des Sicherheitsmanagements durchgeführt. Sie sollen zeigen, ob das aktuelle Sicherheitssystem im hochdynamischen Umfeld der Computerkriminalität bestehen kann oder wo es angepasst werden muss. Sicherheitsaudits sind damit wesentlich für jedes Sicherheitssystem. Maßnahmen dabei:

1. Aktuelle Sicherheitssituation ermitteln: Mitarbeiter befragen, Unterlagen zum Sicherheitskonzept lesen.
2. Sicherheitsmechanismen überprüfen bezüglich ...
   (a) ... globale Systemkonfiguration: Betriebssysteme, Dateisysteme, Domänenstruktur, lokale oder zentrale Datenspeicherung, Netzstruktur, Firewalls, Virenscanner, ...
   (b) ... Konfiguration und Version von Firewalls, Virenscannern, Betriebssystemen und Servern.
   (c) ... Umsetzung der Sicherheitspolitik in Firewalls, Betriebssystemen und Servern.
   (d) ... physikalische Sicherheit: Schutz vor Feuer, Wasser, Stromausfall und Sabotage.
   (e) ... Integrität der Backups.
3. Sicherheitsmaßnahmen überprüfen bezüglich ...
   (a) ... Sicherheitsbewusstsein der Mitarbeiter, Akzeptanz des Sicherheitssystems.
   (b) ... Widerstandsfähigkeit der Mitarbeiter gegen *social engineering*.
   (c) ... Umgang mit den existierenden Vorschriften und Regeln der Sicherheitspolitik.
   (d) ... Verfahren beim Ausscheiden eines Mitarbeiters (Zugangsberechtigung gelöscht?)
4. Penetrations-Tests
   Von innen und außen ausgeführt mit Angriffssimulatoren (VATs, RATs) und Analysewerkzeugen (*security scanner*), um Schwachstellen aufzudecken.
5. Bericht schreiben
   Er dokumentiert den Sicherheitsstand des überprüften IuK-Systems, ggf. ergänzt durch ein Zertifikat.

4.35 CERT

Aufgabe Quelle: [4, Aufg.8b]. Was ist ein CERT?

Lösung CERT: *computer emergency response team*. CERTs gehören zu den wichtigsten Informanten über Sicherheitslücken, aktuelle Angriffsarten und -ereignisse und für solide Empfehlungen für Sicherheitsvorkehrungen. Es gibt über 100 dieser Teams, zusammengeschlossen im »*Forum of Incident Response and Security Teams*« (FIRST). Aufgaben:

1. Möglichst frühzeitig die IT-Verantwortlichen über sicherheitsrelevante Fehler in Software benachrichtigen, um Schäden durch gezieltes Hacking vorzubeugen.
2. Ihnen gemeldete Sicherheitsvorfälle analysieren, die Ergebnisse untereinander tauschen und veröffentlichen.
3. Kooperation mit den Herstellern, um Konfigurationshinweise und Patches anbieten zu können, mit denen sicherheitsrelevante Fehler behoben werden können.

4.36 Verschlüsselung mit geheimen Schlüsseln

Aufgabe Erläutern Sie das Verfahren »Verschlüsselung mit geheimen Schlüsseln«.

Lösung Verschlüsselung mit geheimen Schlüsseln heißt auch »symmetrische Verschlüsselung«, weil für Verschlüsselung und Entschlüsselung derselbe Schlüssel verwendet wird. Verfahren:

1. Verteilung des geheimen Schlüssels k an beide Kommunikationspartner über einen sicheren Kanal.
2. Den Klartext m mit Verschlüsselungsfunktion f, parametrisiert mit Schlüssel k, verschlüsseln:
$$c = f_k(m)$$
3. Übertragung des Geheimtextes c über einen öffentlichen Nachrichtenkanal.
4. Den Geheimtext c mit Entschlüsselungsfunktion f^{-1}, parametrisiert mit Schlüssel k, entschlüsseln:
$$m = f_k^{-1}(c)$$

4.37 Praktisch sicheres Kryptosystem

Aufgabe Quelle: [3, Aufg. 8b]. Welche Kriterien muss ein auf Verschlüsselung basierendes Kryptosystem erfüllen, damit es als praktisch sicher gilt?

Lösung

- es muss kryptologisch sicher sein, d.i. robust gegen:
  - Geheimtextangriff (*ciphertext-only attack*)
  - Klartextangriff (*known-plaintext attack*)
  - Angriff mit ausgewähltem Geheimtext (*chosen-ciphertext attack*)
  - Angriff mit ausgewähltem Klartext (*chosen-plaintext attack*)

- es muss robust sein gegen vollständige Schlüsselsuche (*brute force attack*)
  - Dauer des Informationswertes < Dauer der Ermittlung des Schlüssels
  - Geldwert der Information < Geldwert zur Ermittlung des Schlüssels

4.38 Kerckhoffsches Prinzip

Aufgabe Quelle: [3, Aufg. 8c]. Was besagt das Prinzip von KERCKHOFF?

Lösung Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit beruht ausschließlich auf der Geheimhaltung des Schlüssels.

4.39 Produktalgorithmus

Aufgabe Was meint man, wenn man einen Verschlüsselungsalgorithmus als Produktalgorithmus bezeichnet?

Lösung Dass der Verschlüsselungsalgorithmus auf dem Prinzip der zyklischen Wiederholung des gleichen Schrittes basiert. Der Schritt ist kryptologisch einfach und relativ unsicher. Doch eine ausreichende Zahl von Zyklen bringt die notwendige Sicherheit.

4.40 Verschlüsselungsprinzipien im Feistel-Netzwerk

Aufgabe Nennen und erklären Sie die im Feistel-Netzwerk realisierten Verschlüsselungsprinzipien!

Lösung

Konfusion Die Beziehung zwischen Klartext- und Geheimtextbuchstaben wird verschleiert, damit es möglichst keine statistischen Abhängigkeiten[3] zwischen Klar- und Geheimtext mehr gibt. Realisiert durch Substitutionsalgorithmen: »Die Buchstaben bleiben wo sie sind, aber nicht was sie sind.«. Im Feistel-Netzwerk ist dies der Schritt $f_{k_i}(R_{i-1})$.

Diffusion Die im Klartext enthaltenen Buchstaben werden umgeordnet bzw. ihre Information wird über den gesamten Geheimtext oder Geheimtextblock verteilt. So sollen Strukturen im Klartext möglichst gut verwischt werden. Realisiert durch Transpositionsalgorithmen: »Die Buchstaben bleiben was sie sind, aber nicht wo sie sind.«. Im Feistel-Netzwerk sorgt die »Seitenvertauschung« (L_i hängt von R_{i-1}ab, $R_i$von L_{i-1}) für blockinterne Diffusion und die Betriebsart CBC für blockübergreifende Diffusion. Durch CBC hängt ja jeder Geheimtextblock von allen vorhergehenden Klartextblöcken (und dem Initialisierungsvektor und dem Schlüssel) ab, oder andersherum: die Information jedes Klartextblocks wird auf alle folgenden Geheimtextblöcke verteilt.

Lawineneffekt bei Blockchiffren ist »vollständige blockinterne Diffusion«. Jedes Bit eines Geheimtextblocks muss von jedem Bit des Klartextblocks und von jedem Bit des Schlüssels

[3] Würde man einfach jeden Buchstaben durch den folgenden Buchstaben des Alphabets ersetzen, gäbe es größtmögliche statistische Abhängigkeit zwischen Klartext- und Geheimtextbuchstaben: jeder Geheimtextbuchstabe entspricht ja genau einem Klartextbuchstaben. Natürlich ist bei DES ein Buchstabe kein Buchstabe des Alphabets, sondern ein 64-Tupel $(a_1 \dots a_{64}) \mid a_i \in \{0, 1\}$, aber das Prinzip wird so trotzdem klar.

abhängen. Um maximal gegen die Differentielle Kryptoanalyse zu schützen, muss sogar gelten: Wird ein Bit in Klartext oder Schlüssel geändert, so ändert sich jedes Geheimtextbit mit einer Wahrscheinlichkeit von genau 50%.

4.41 Betriebsarten von Blockalgorithmen

Aufgabe Nennen Sie die vier Betriebsarten von Blockalgorithmen und erläutern Sie zwei davon!

Lösung

ECB (*electronic code book*) Die Klartextblöcke werden sequentiell verschlüsselt und entschlüsselt. Jeder Geheimtextblock hängt nur vom Schlüssel ab! Nachteile: Mallory kann problemlos korrekt kodierte Blöcke herausnehmen oder einfügen; gleiche Klartextblöcke führen zu gleichen Geheimtextblöcken, was einen erfolgreichen Klartextangriff ermöglicht.

CBC (*cipher block chaining*) Vor der Verschlüsselung eines Klartextblocks K_i wird dieser mit dem zuletzt erzeugten Geheimtextblock G_{i-1} durch XOR[4] verknüpft: $G_i = f_k\,(K_i \oplus G_{i-1})$. Da nun jeder Geheimtextblock von allen vorhergehenden Klartextblöcken und dem Schlüssel abhängt, verschwimmen die Blockgrenzen. Die Probleme des ECB-Modus werden damit behoben.

CFB (*cipher feedback mode*)

OFB (*output feedback mode*)

4.42 RSA-Verschlüsselung mit öffentlichen Schlüsseln

Aufgabe Quelle: [3, Aufg. 9b]. Erläutern Sie (Skizze + Text) das Prinzip der Verschlüsselung mit öffentlichen Schlüsseln am Beispiel RSA.

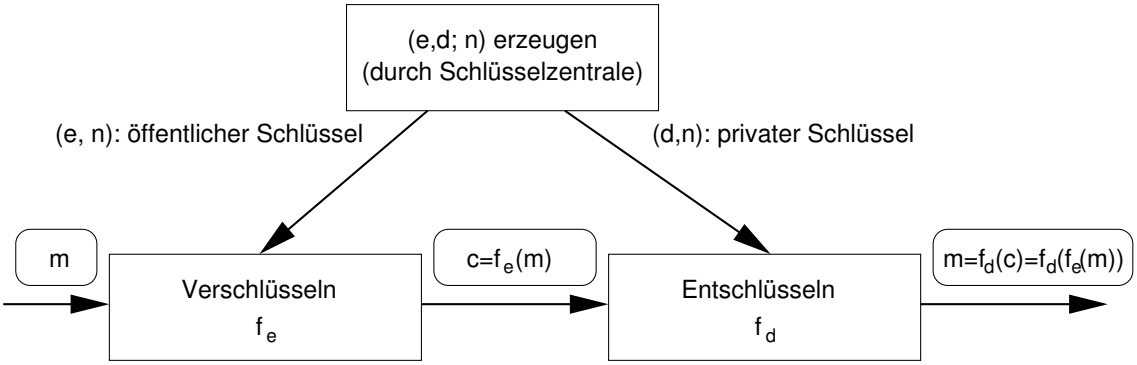

Abbildung 2: Verschlüsselung mit öffentlichen Schlüsseln am Beispiel RSA

Lösung Skizze in Abbildung 2.

1. Der Sender erhält den öffentlichen Schlüssel e und die natürliche Zahl n des Empfängers derart, dass er sie authentifizieren kann.

[4] geschrieben als $\oplus$, denn XOR entspricht der Addition ohne Übertrag, der sogenannten »Modulo-2-Addition«.

2. Der Sender teilt die Nachricht in Blöcke fester Länge auf, deren Zahlwert maximal $n-1$ betragen darf.

3. Der Sender verschlüsselt jeden Klartextblock m mit dem öffentlichen Schlüssel e des Empfängers gemäß
$$c = m^e \bmod n$$

4. Der Empfänger entschlüsselt jeden Geheimtextblock c mit seinem privaten Schlüssel d gemäß
$$m = c^d \bmod n$$

4.43 Digitale Signatur mittels RSA

Aufgabe Quelle: [4, Aufg. 10b]. Erläutern Sie (Skizze + Text) das Prinzip der digitalen Signatur mittels RSA.

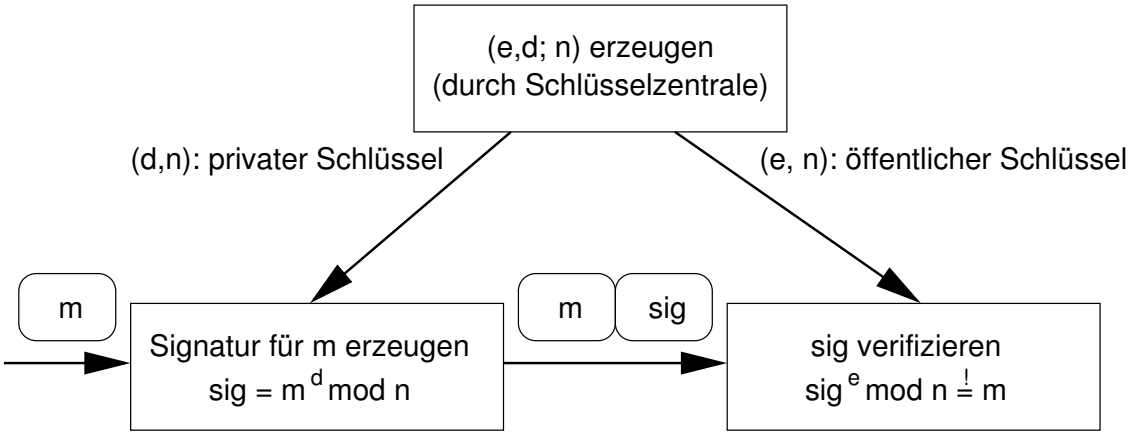

Abbildung 3: Digitale Signatur mit RSA

Lösung Skizze in Abbildung 3. Für Verschlüsselung und Entschlüsselung mit RSA gilt ja
$$(m^e)^d \bmod n = \left(m^d\right)^e \bmod n = m$$
Damit kann der private Schlüssel d auch zur Verschlüsselung, der öffentliche Schlüssel e auch zur Entschlüsselung genutzt werden. Genau das wird bei digitalen Signaturen genutzt: der Empfänger kann die Echtheit einer Nachricht überprüfen, indem er nachweist, dass der Absender den geheimen Schlüssel d kennt. Eine Signatur wird mit dem Signaturschlüssel d erzeugt gemäß
$$sig = m^d \bmod n$$
und mit dem Verifikationsschlüssel $e$verifiziert gemäß
$$sig^e \bmod n \stackrel{!}{=} m$$

4.44 Einweg-Hashwert

Aufgabe Quelle: [3, Aufg. 10a]. Erklären Sie den Begriff Einweg-Hashwert. Wozu wird so etwas benutzt?

Lösung Ein Einweg-Hashwert MAC (*message authetication code*) ist ein »kryptografischer Fingerabdruck einer Nachricht«. Eigenschaften:

- $h : MAC = h(m)$ ist eine »kollisionsfreie Einwegfunktion«:

  kollisionsfrei: es ist praktisch unmöglich[5] zwei verschiedene Nachrichten m und m' zu finden, die denselben MAC haben.

  Einwegfunktion[6]: MAC kann leicht aus m bestimmt werden, umgekehrt ist es praktisch unmöglich.

- $h : MAC = h(m)$verkürzt eine Nachricht beliebiger Länge auf ein Kodewort fester Länge (den Hashkode, oft 16 Byte).

MACs werden verwendet, um ...

- ... zu signierende Nachrichten zu kürzen, denn umfangreiche Nachrichten mit RSA zu signieren ist zu aufwendig. Deshalb berechnet man nicht die Signatur der gesamten Nachricht, sondern eines Einweg-Hashwertes $MAC = h(m)$ dieser Nachricht gemäß $sig = (h(m))^d \mod n$. Sonst entspricht das Verfahren der digitalen Signatur mit RSA.
- ... Passwörter aus Passphrasen zu berechnen[7].
- ... kryptografische Fingerabdrücke öffentlicher Schlüssel zu erstellen.
- ... Initialisierungsvektoren und Zufallsgrößen zu erzeugen.
- ... eine Datei auf Integrität zu prüfen, etwa um Downloadfehler auszuschließen.

4.45 Anforderungen an das Schlüsselmanagement

Aufgabe Welche sicherheitsrelevanten Anforderungen sollte ein sicheres Schlüsselmanagement erfüllen?

Lösung

Vertraulichkeit Private Schlüssel werden während ihrer Erzeugung, Verteilung (oder Vereinbarung), Aufbewahrung und während ihrer Anwendung in einem Verschlüsselungsalgorithmus geheim gehalten.

Integrität Integritätsverletzung von Schlüsseln muss ausgeschlossen sein oder erkannt werden können.

Schlüsselzerstörung Ein Sitzungsschlüssel muss bei Benutzung in einer zweiten Sitzung als ungültig erkannt werden.

Erkennen von Verzögerungen bei der Schlüsselverteilung als Hinweise auf mögliche Unregelmäßigkeiten.

[5] »praktisch unmöglich« ist eine Aufgabe dann, wenn ihre Lösung mit aktuellen Methoden und Rechnern viel zu lange dauern würde, z.B. ein Jahrhundert.

[7] Sollte es nicht heißen: Passphrasen aus Passwörtern? Dann wären Passphrasen die im System gespeicherten Hashwerte von Passwörtern. Weil h eine Einwegfunktion ist wäre es praktisch unmöglich, die ein geeignetes Passwort aus der öffentlich zugänglichen Passphrase zu berechnen.

Zertifizierung So wird nachgewiesen, dass ein öffentlicher Schlüssel zu einer bestimmten Person oder Instanz gehört. Zertifizierung hindert die *man in the middle attack*.

Verifikation der Gültigkeit Der Empfänger eines eigenen privaten Schlüssels oder fremden öffentlichen Schlüssels verifiziert seine Gültigkeit, etwa durch MAC (direktes Vertrauen) oder dritte Instanzen (indirektes Vertrauen).

Empfangsbestätigung Der Empfänger teilt dem Absender mit, dass er als rechtmäßiger Empfänger den gesendeten Schlüssel erhalten hat.

4.46 Authentifizierung öffentlicher Schlüssel mittels MAC

Aufgabe Quelle: [4, Aufg. 10a]. Erläutern Sie die das Verfahren »Authentifizierung öffentlicher Schlüssel mittels MAC«.

Lösung

1. Alice erhält von Bob einen öffentlichen Schlüssel über einen unsicheren Übertragungsweg.
2. Alice berechnet mit einer öffentlichen Einweg-Hashfunktion den MAC des erhaltenen Schlüssels.
3. Alice lässt sich den errechneten Wert von Bob über einen authentischen Kommunikationskanal (Brief, Telefon, persönlicher Kontakt) bestätigen.Bob könnte den MAC seines öffentlichen Schlüssels auch gedruckt veröffentlichen, etwa auf seiner Visitenkarte.

4.47 Authentifizierung öffentlicher Schlüssel mittels dritter Instanzen

Aufgabe Erläutern Sie die das Verfahren »Authentifizierung öffentlicher Schlüssel mittels dritter Instanzen« bei zentral verwalteten Zertifikaten.

Lösung

1. Alice möchte Bob eine verschlüsselte Nachricht senden und benötigt dazu also seinen authentifizierten öffentlichen Schlüssel.
2. Alice ermittelt den öffentlichen Schlüssel von Bob durch Recherche in den öffentlichen Verzeichnissen der Zertifizierungsstellen (*trust center*).
3. Alice prüft die Gültigkeit des Zertifikats, das Bob seinen öffentlichen Schlüssel zuordnet, durch Verifikation der digitalen Unterschrift mittels des öffentlichen Schlüssels der Zertifizierungsstelle.
4. Alice authentifiziert den öffentlichen Schlüssel der Zertifizierungsstelle mit demselben Verfahren, mit dem sie Bobs Schlüssel authentifizierte: Recherche im öffentlichen Verzeichnis der übergeordneten Zertifizierungsstelle, Verifikation des gefundenen Zertifikats mit dem Schlüssel der übergeordneten Zertifizierungsstelle. Alice wiederholt dieses Verfahren, bis sie den CPT (*common point of trust*) erreicht. Diese Wurzelinstanz hat als einzige das Privileg, ihren Verifikationsschlüssel (d.i. ihren öffentlichen Schlüssel) selbst zu zertifzieren.
5. Wurzelinstanzen verschiedener nationaler Systeme zertifizieren sich gegenseitig (Kreuzzertifizierung), so dass auch Zertifikate der Wurzelinstanz verifiziert werden können.

4.48 Schritte bei Erzeugung eines zertifizierten Schlüsselpaares

Aufgabe Nennen Sie die Schritte, mit denen eine Zertifizierungsinstanz ein zertifiziertes Schlüsselpaar erzeugt.

Lösung

1. Registrierung und Identifizierung des Teilnehmers
2. Schlüsselerzeugung nach genau einer folgenden Alternative:
   - Die Schlüsselerzeugungsinstanz der Zertifizierungsstelle generiert das Schlüsselpaar.
   - Der Kartenhalter erzeugt sein Schlüsselpaar mit Hilfe seiner ICC selbst.
3. Zertifikats-Ausstellung
4. Personalisierung
5. Publikation des öffentlichen Schlüssels

4.49 Elemente eines Schlüsselzertifikats nach X.509v3

Aufgabe Quelle: [3, Aufg. 10b]. Nennen Sie 5 Elemente eines Schlüsselzertifikats nach X.509v3.

Lösung Das vollständige Format eines Eintrags in SiG-konformen Verzeichnissen nach ISO X.509v3:

Versionsnummer Version des Formats.

Zertifikatsnummer Fortlaufende Identifikationsnummer.

ID des Signaturalgorithmus der CA Kennung des von der *certification authority* verwendetenSignaturalgorithmus.

Aussteller »*distinguished name*« des Trustcenters in X.500 Notation.

Gültigkeitszeitraum Spezifiziert den Gültigkeitszeitraum des Zertifikats.

Zertifikatnehmer »*distinguished name*« des Teilnehmers in X.500 Notation.

Verwendungszweck Unterscheidung von Anwendungszwecken des öffentlichen Schlüssels des Zertifikatsnehmers wie Signatur, Ausstellung von Zertifikaten, Verschlüsselung usw.

ID des Algorithmus Kennung des Algorithmus mit dem der öffentliche Schlüssel des Zertifikatsnehmers verwendet werden kann.

e_{TN} Öffentlicher Schlüssel des Zertifikatsnehmers.

ID der CA Kennung der Zertifizierungsinstanz.

Zertifikatserweiterungen $(0 \ldots N)$ Angaben über Güteklassen zur Definition von Vertrauenswürdigkeitsstufen: nur privater Gebrauch, Beschränkung des Geschäftswertes, Anwendung nur zur Zugangskontrolle usw.

Digitale Signatur der CA Mittels Signaturschlüssel d_{CA} der CA aus einem MAC der o.a. Daten erzeugte Signatur der CA.

4.50 Diskussion zentral verwalteter Zertifikate

Aufgabe Diskutieren Sie die Vor- und Nachteile zentral verwalteter Zertifikate.

Lösung Vorteile

- Alle Zertifizierungsstellen sind vertrauenswürdig und haben strenge Richtlinien. Das bietet ein sehr hohes Maß an Sicherheit.
- Teilnehmer, die sich nicht an vorgegebene Richtlinien halten, können aus dem System ausgeschlossen werden.
- Schlüssel können einfach zurückgerufen oder gesperrt werden.
- Spontane Kommunikation von Konkurrenten ist möglich, wenn beide Teilnehmer einen zertifizierten öffentlichen Schlüssel haben.

Nachteile

- Hierarchisch geordnete zentrale Zertifizierungsinstanzen nach ISO X.509 sind sehr aufwendig zu realisieren.
- Kommunikation nicht konkurrierender Teilnehmer benötigt nicht die hohe Sicherheit, also auch nicht den hohen Aufwand zentral verwalteter Zertifikate.

4.51 Vetrauen und Gültigkeit in PGP

Aufgabe Unterscheiden Sie in der Terminologie des PGP »Web of Trust«: »Vertrauen« und »Gültigkeit«. Welche Faktoren beeinflussen Vertrauen und Gültigkeit wie?

Lösung

Gültigkeit (*validity*) ist ein für jeden öffentlichen Schlüssel errechnetes Maß an Sicherheit, dass er dem angegebenen Eigentümer gehört. Dieses Maß kann die Werte »gültig«, »zweitrangig gültig« und »ungültig« annehmen. Nur »gültige« Schlüssel können verwendet werden. Ein Schlüssel wird »gültig« durch Zertifikate von Schlüsselverwaltern: entweder durch eines von »implizit vertrauenswürdigem« oder »voll vertrauenswürdigem« Schlüsselverwalter oder durch zwei von »eingeschränkt vertrauenswürdigen« Schlüsselverwaltern.

Vertrauen (*trust*) ist die Motivation, mit der ein Benutzer einen anderen zu einem »voll vertrauenswürdigen« oder »eingeschränkt vertrauenswürdigen« Schlüsselverwalter macht. Alle anderen hält der Benutzer für »nicht vertrauenswürdig«, sich selbst für »implizit vertrauenswürdig«. Schlüsselverwalter sind alle, deren Schlüssel am »öffentlichen Schlüsselbund« ist, darunter stets der eigene Schlüssel. Nur jemand mit gültigem Schlüssel kann zum Schlüsselverwalter gemacht werden.

Teil II
Datenschutz

Literatur

[1] Prof. Dr. W. Schmitt: »Hilfsblätter zur Vorlesung Datenschutz und Datensicherheit; Teil II - Datensicherheit; SS 2003«. Version vom 2003-04-07. Dies ist das offizielle Skript zum Teil »Datensicherheit« der Veranstaltung »Datenschutz und Datensicherheit« und enthält alles, was Prof. Schmitt mit dem Beamer in der Vorlesung vorführt. Verkauf in der Vorlesung für 1,20 EUR. Es ist so weitgehend identisch mit dem Skript aus den letzten Jahren, dass sich ein Neuerwerb nicht lohnt. Das Skript steht nicht im Internet zur Verfügung und darf auch nicht ins Internet gestellt werden.

[2] Prof. Dr. W. Schmitt: Persönliche Homepage. Enthält Terminpläne und Klausuren zur Veranstaltung »Datenschutz und Datensicherheit«. http://homepages.fh-giessen.de/~hg6421/

[3] Prof. Dr. W. Schmitt: »Klausur Datenschutz und Datensicherheit / Sommersemester 2002; Teil 2: Datensicherheit«; 24.9.2002. Quelle: http://homepages.fh-giessen.de/~hg6421/DuD/SS02.pdf, referenziert auf [2].

[4] Prof. Dr. W. Schmitt: »Klausur Datenschutz und Datensicherheit / Wintersemester 2002; Teil 2: Datensicherheit«; 3.2.2002. Quelle: http://homepages.fh-giessen.de/~hg6421/DuD/WS02.pdf, referenziert auf [2].

[5] Hajo Köppen: Skript zur Vorlesung Datenschutzrecht. Nach http://www.fh-friedberg.de/fachbereiche/suk/Team/feyerabend/downloads.html kann es bei Hajo Köppen für 3 EUR erworben werden. Es wird auch in der Vorlesung verkauft.

[6] Hajo Köppen: Präsentation zur Vorlesung Datenschutzrecht. Entweder als eine einzige oder getrennt in 13 Powerpoint-Dateien. Diese Präsentation enthält den Stoff gegenüber [5] weniger ausführlich. Quelle: Downloads zur Vorlesung Datenschutzrecht http://www.fh-friedberg.de/fachbereiche/suk/Team/feyerabend/downloads.html.

[7] Hajo Köppen: Repetitorium Datenschutzrecht. Eine Hilfe zur Wiederholung und Klausurvorbereitung. Quelle: http://www.fh-friedberg.de/fachbereiche/suk/Team/feyerabend/datenschutzrecht/Repetitorium.zip, referenziert auf Downloads zur Vorlesung Datenschutzrecht http://www.fh-friedberg.de/fachbereiche/suk/Team/feyerabend/downloads.html.

[8] Dozenten im Studiengang »Technische Redaktion und multimediale Dokumentation« an der FH Gießen-Friedberg :: Hajo Köppen. Übersicht über Vita und Veröffentlichungen von Hajo Köppen. http://fjmd.fh-giessen.de/wer/koeppen_hajo/koeppen_hajo.html

[9] Daniel Webelsiep: »Datenschutz«. Herr Köppen gibt im Teil Datenschutz der Veranstaltung »Datenschutz un Datensicherheit« an der FH Gießen-Friedberg, Studiengang Informatik, Fragen zur Klausurvorbereitung aus. Dieses Dokument besteht aus diesen Fragen mit Antworten von Daniel Webelsiep aus dem SS 2002. Größe 33811 Byte. Quelle: http://www.webelsiep.de/downloads/skripte/datenschutz.pdf, referenziert auf http://www.webelsiep.de/default.php?main=studium.

[10] M. Wojcicki: »Sichere Netze - Analysen, Maßnahmen, Koordination«. C. Hanser, München / Wien (1991).