Einführung

Alice erfährt im Büro, daß ihre Zimmergenossin Eve ihrem gemeinsamen Chef Bob eine Falle gestellt hat. Wenn er mittags ins Büro kommt, wird die Steuerfahnung auf ihn warten. Wie kann sie ihn warnen, ohne daß Eve mißtrauisch wird?

Communication in the presence of adversaries (Rivest)

Ziel: Sichere Kommunikation in einer unsicheren Umgebung.

Beispiele für unsichere Umgebungen: Telefonleitungen, Briefe, Funk, Internet.

- Attacken gibt es seit es Computer gibt, geändert hat sich mit dem Internet die Situation: per Modem ca. 20 Millionen Computer und 50 Millionen Benutzer (1996) erreichbar.

- etwas Geschichte:

  1. memory protection hardware 1960
  2. file access control 1962
  3. Passwortsicherung durch Einwegfunktionen 1967
  4. TCP/IP für "sichere" Kommunikation in Netzen 1969
  5. Unix-Unix system mail (UUCP): man kann Befehle auf anderen Maschinen ausführen 1975
  6. Public-key und digitale Signaturen 1976
  7. RSA 1978
  8. erste Studie über Passwörter: größtes Problem: geschicktes Raten (Name der Freundin, ...) 1978
  9. Electronic Cash 1978
  10. DNS für das Internet 1983
  11. Computerviren 1984

12. neue Passwortmethoden: callback, challenge-response, one-time passwort/Smartcard 1985
13. Clifford Stoll fängt einen KGB-Hacker (The Cuckoo's Egg) 1986
14. Internetwurm 1988
15. PGP, PEM 1989
16. anonyme Remailer 1990
17. Firewalls 1993
18. Javasicherheitsprobleme 1996
19. DES-Cracker 1998

- etwas Vokabular
  - eavesdropping: lauschen
  - snooping: Dateien durchstöbern und kopieren
  - tampering oder data diddling: Dateien und Software unauthorisiert ändern
  - spoofing: sich für jemand anderen ausgeben (User oder auch Rechner)
  - looping: sich von Rechner zu Rechner hangeln (Spuren verwischen)
  - jamming oder flooding: Resourcen blockieren

Computersicherheit

- Information schützen
  - Passwörter schützen
  - Kreditkartennummern verschlüsselt übermitteln
  - Dokumente mit digitalen Unterschriften versehen

- Systeme schützen
  - Viren, Trojanische Pferde, Würmer, . . .
  - Java Applets
  - Eindringlinge
  - Lauscher

Wo ansetzen?

- Hardwaresicherheit
- Softwaresicherheit
- Datensicherheit

Bedrohung := mögliche Verletzung der Sicherheit eines Sytems

Kontrolle := Gegen- oder Schutzmaßnahme, die das Risiko durch eine Bedrohung reduzieren oder eliminieren kann

Dimensionen von Sicherheit

- Vertraulichkeit (confidentiality)
- Integrität (integrity)
- Verfügbarkeit (availability)
- Authentifikation (authentication)
- Verbindlichkeit (non-repudiation)

Bedrohungen

- Computerkriminalität
  - Spionage
  - Sabotage
  - Betrug
  - Erpressung
- Physikalische Ereignisse
  - Kompromittierende Strahlung
  - Elektromagnetische Impulse
  - Computerausfall
- Menschliche Fehler
  - Fehlbedienung
  - Fehler in der Entwicklung (Jahr 2000)

Risiko

Risiko := Möglichkeit des Erleidens eines Schadens

Risikomanagement := Alle Aktivitäten zur Identifizierung und Bewältigung von Risiken

1. Risikoanalyse

2. Sicherheitsplanung

3. Durchführung und Kontrolle

Risikoanalyse

Abschätzung von *Kosten Schäden* $\Longleftrightarrow$ *Kosten Prävention*

1. Alle Komponenten des Computersystems und alle Bedrohungen auflisten, sinnvollerweise die Systemkomponenten als Zeilen und die Risikosituationen als Spalten einer Matrix. Jede Zelle definiert dann eine mögliche *Verwundbarkeit*.

2. Für alle n Verwundbarkeiten Schadenhäufigkeiten H_i und Schadenskosten K_i abschätzen. Folgekosten miteinbeziehen. Der jährlich zu erwartende Verlust kann als $V = \sum_{i=1}^{n} H_i \star K_i$ quantifiziert werden.

3. Ist V zu groß, müssen Kontrollen mit Umsetzungskosten U_i in die Rechnung einbezogen werden. Ist für eine Kontrolle $U_i - H_i \star K_i$ negativ, so reduziert sich das Risiko um mehr als es kostet und die Kontrolle sollte umgesetzt werden.

Risikoanalyse 2

Problem: Beruht alles auf den Schätzungen.

Dennoch kann eine seriöse Risikoanalyse das Problembewußtsein und das -verständnis unter den betroffenen Mitarbeitern steigern.

Restrisiko := Alle Bedrohungen, die zwar erkannt, aber aus technischen, organisatorischen oder finanziellen Gründen nicht verhindert werden.

Ein Restrisiko bleibt immer. Jedes Unternehmen muß entscheiden, was tolerierbar ist.

Sicherheitsplanung

Anzustreben ist eine einheitliche *Sicherheitspolitik*, die auf einem *Sicherheitsplan* beruht, der beschreibt, wie das Unternehmen seinen Sicherheitsbedürfnissen zu entsprechen versucht.

Der Sicherheitsplan sollte enthalten:

- die Ergebnisse der Risikoanalyse
- nach Prioritäten geordnete Empfehlungen
- Ziele und Verantwortungensbereiche der beteiligten Personen
- Zeitplan für die Umsetzung der Kontrollen
- Datum der nächsten Risikoanalyse

Wichtige Komponenten der Sicherheitsplanung

- Sicherheitstraining für Mitarbeiter

  "Security continues to be and probably will always be a people problem. If you overlook that, you're in trouble."

- **DATENSICHERUNG**
  - Backup-Strategien
  - Aufbewahrung und Schutz

- Systemüberwachung
  - Protokollieren sicherheitsrelevanter Vorgänge
  - Probleme mit dem Datenschutz

Gefährdungen bei der Datenkommunikation

- Wer die Nachricht abhört, kann das Verhalten des Senders und des Empfängers interpretieren.

- Wer die Nachricht abändern kann, kann das Verhalten des Empfängers beeinflussen.

- Passive Angriffe (keine Änderung der Daten)
  - Abhören der Teilnehmer-Identitäten
  - Abhören der Daten
  - Verkehrsflußanalyse
- Aktive Angriffe (Verfälschen des Nachrichtenstroms)
  - Wiederholung oder Verzögerung einer Information
  - Einfügen oder Löschen von Daten
  - Boykott des Kommunikationssystems
  - Modifikation der Daten
  - Vortäuschen einer falschen Identität
  - Leugnen der Kommunikationsbeziehung
- Zufällige Verfälschungsmöglichkeiten
  - Fehlrouting von Informationen
  - Fehlbedienung
  - Übertragungsfehler

Sicherheitsdienste

Was ein Kommunikationssytem bieten kann/soll/muß.

- Vertraulichkeit der Daten
- Verhinderung einer Verkehrsflußanalyse
- Integrität der Daten
- Authentizitätsüberprüfung für Sender und Empfänger
- Zugangskontrolle für Betriebsmittel
- Sendernachweis
- Empfängernachweis

Sicherheitsmechanismen

1. Verschlüsselung
2. Digitale Unterschrift
3. Hashfunktionen
4. Authetizitätsprüfung
5. Zugangskontrolle
6. Datenintegritätsmechanismen
7. Fülldate
8. Routingkontrolle
9. Notariatsfunktion

Mechanismen: Dienste	Ver- schlüs- selung	Digitale Unter- schrift	Zugangs- kontroll- mechanismus	Datenunver- sehrtheits- mechanismus	Authen- tifikations- protokoll	Füll- daten	Routing- kontrolle	Notariat
Authentizitätsprüfung des Kommunikationspartners	U	U			U			U
Zugangskontrolle			J					
Vertraulichkeit der Verbindung	J						U	
Vertraulichkeit ohne Verbindung	J						U	
Vertraulichkeit ausgewählter Felder	J							
Verhinderung einer Verkehrs-flußanalyse	J							
Datenunversehrtheit der Verbindung mit Recovery	U			J				
Datenunversehrtheit der Verbindung ohne Recovery	U			J				
Datenunversehrtheit ausge-wählter Felder	U			J				
Datenunversehrtheit der Daten ohne Verbindung	U	U		J				
Datenunversehrtheit ausge-wählter Felder ohne Verbindung	U	U		J				
Authentizitätsprüfung des Absenders der Daten	U	U		U				U
Sendernachweis		U		U				U
Empfängernachweis		U		U				U

J = Ja, U = Unter Umständen

Kernfrage 1

Wie kann ich mit jemand vertraulich kommunizieren?
Frage nach der *Geheimhaltung der Information*.

- Organisatorische Maßnahmen

- Physikalische Maßnahmen

- Kryptographische Maßnahmen

Wer das “Geheimnis” kennt, kommt auch an die Information.

Kernfrage 2

Wie kann ich mich gegenüber einem anderen zweifelsfrei ausweisen?
Wie kann ich sicher sein, daß eine Nachricht wirklich von dem anderen Sender stammt?

Frage nach der *Authentifikation*.

- Teilnehmerauthentifikation
  Ich weise meine Identität dadurch nach, daß ich etwas habe, was kein anderer hat

  – biologische Eigenschaft
  – etwas Einzigartiges besitzen
  – Wissen

  Idee: Nachweis der Identität durch geheimes Wissen.
  Problem: Wie überzeuge ich andere davon, daß ich das geheime Wissen habe?

- direkt übertragen oder indirekt erschließen?
- braucht das Gegenüber auch geheimes Wissen oder reicht öffentliches Wissen?

- Nachrichtenauthetifikation
  - Unterschriften
  - Echtheitsmerkmale

  Der Ersteller besitzt etwas, mit dessen Hilfe er das Dokument authentisch macht.

Kernfrage 3

Kann ich kommunizieren, ohne daß anschließend jemand weiß, daß ich kommuniziert habe?

Frage nach der *Anonymität*.

- Bezahlen mit Bargeld
- Anrufe bei der Telefonseelsorge
- Chiffreanzeigen

Problem: Anonymität $\Longleftrightarrow$ Verläßlichkeit