Seminar Datenschutz

Ulrich Kühn & Uwe Schläger

Verschlüsselungstechniken

Andreas Tägener

Übersicht

- Chiffrier-Verfahren
  - Symmetrisch
  - Public-Key
- Digitale Signatur
- Schlüsselverwaltung
- Chiffrierte Datenhaltung
- Sicherheit

Symmetrische Verfahren

- Derselbe Schlüssel zum ver- und entschlüsseln
- Schnell
- Kurze Schlüssel
- One-Time-Pad ist absolut sicher

Public-Key Verfahren

- Zwei verschiedene Schlüssel zum Ver- und Entschlüsseln
- Manche Verfahren zur Signatur geeignet, z.B. RSA und El Gamal
- Sicherheit abhängig von Problemen wie diskreter Logarithmus, faktorisieren einer Zahl, ...
- Lange Schlüssel
- Durch elliptische Kurven kurze Schlüssel möglich, z.B. kann bei Fast Elliptic Encryption jeder leicht zu merkende String als Private-Key dienen

Digitale Signatur (1)

- Anforderungen an eine Signatur
  - Authentisch
  - Kann nicht gefälscht werden
  - Fest an ein Dokument gebunden
  - Ein signiertes Dokument kann nicht geändert werden
  - Kann nicht geleugnet werden

Digitale Signatur (2)

- Realisierbar durch
  - Symmetrische Verfahren
  - Public-Key Verfahren
  - Timestamps
  - Hash-Funktionen

- Problem: Wenn der Schlüssel gestohlen wird, ist weder der Mißbrauch noch der berechtigte Gebrauch in jedem Fall nachweisbar

Schlüsselverwaltung

- Erstellen eines Schlüssels
- Übertragen an den Kommunikationspartner
- Verifizieren
- Verwenden
- Speichern
- Gültigkeitsdauer
- Kompromittierte Schlüssel
- Zerstören

Erzeugen von Schlüsseln

- Den gesamten Schlüsselraum nutzen
- Passphrase mit key crunching statt Passwort
- Schwache Schlüssel aussortieren
- Echte Zufallszahlen
- Standards:
  - X9.17
  - Department of Defense

Übertragen von Schlüsseln

- Key encryption keys
- Key splitting
- Key Server
- Vorteil Public-Key Verfahren:
  Der Public-Key kann auf beliebigen Umwegen und unverschlüsselt zum Empfänger geschickt werden (z.B. über eine Public-Key Datenbank)

Verifizieren von Schlüsseln

- Persönlich
- Signatur von vertrauenswürdigen Personen
- (Hash-) Wert per Telefon
- Vertrauen auf Geheimhaltung des key encryption keys

Verwenden von Schlüsseln

- Möglichst mit Session Keys arbeiten
- Verwendbarkeit von Schlüsseln einschränken
  z.B. nur signieren oder nur chiffrieren
- Vorsicht bei Multitasking-Systemen
- Bevorzugt tamper-resistant Hardware verwenden

Speichern von Schlüsseln

- Im Kopf
- Auf einer Chip-Karte
- Verschlüsselt auf Workstation, Server, etc.
  z.B. RSA Schlüssel mit IDEA Chiffriert

Kompromittierte Schlüssel

- Symmetrische Verfahren:
  - Neuen Schlüssel generieren und den Kommunikationspartnern mitteilen
- Public-Key Verfahren:
  - Sämtliche Public-Key Datenbanken benachrichtigen bei z.B. PGP schwer durchführbar (Web of trust)
  - Da der Public-Key weltweit bekannt ist, kann jemand eine fremde Identität annehmen
  - Größte Gefahr: Falsche Signatur von Dokumenten
  - Timestamps zum Beschränken der Gültigkeitsdauer

Begrenzte Lebensdauer von Schlüsseln

- Grund:
  - Gefahr, daß der Schlüssel bekannt wird
  - Wert der geschützten Daten steigt
  - Nutzten-Kosten Verhältnis beim Knacken
  - Große Menge Chiffre erleichtert die Kryptoanalyse
- Empfohlene Lebensdauer:
  - Wählverbindung: eine Session
  - Standleitung: abhängig vom Datenvolumen
  - Key encryption key: lang (Übertragung ist riskant)
  - File Keys: lang
  - Signatur: wird evtl. ewig benötigt, aber trotzdem von Zeit zu Zeit wechseln

Verschlüsselung auf Massenspeichern

- Anforderungen:
  - Mehrere Benutzer müssen auf eine Datei zugreifen können
  - Hohe Geschwindigkeit
  - Random Access bei Datenbanken

- Realisation:
  - Für jede Datei ein zufälliger Schlüssel (file-enc. key)
  - jeder Benutzer hat eine mit seinem Schlüssel chiffrierte Teilliste von File-Keys
  - Master key zum chiffrieren aller file-encryption keys
  - spezielle Algorithmen für max. Geschwindigkeit

IBM Secret Key Management Protocol

- Sichere Kommunikation zwischen Terminal und Server sowie zwischen mehreren Servern
- Chiffrierte Speicherung der Daten auf dem Server
- Automatisiert Schlüssel Erzeugung, Verteilung, Installation, Speicherung, Änderung und Zerstörung
- Benötigt tamper-resistant Ver- und Entschlüsselungs Gerät, in denen die Schlüssel gespeichert werden

Sicherheit

- Algorithmen
- Schlüsselverwaltung
- Sonstiges

Sicherheit von Algorithmen (1)

- Kategorien des brechens eines Algorithmus
  - Total break
  - Global deduction
  - Instance (oder local) deduction
  - Information deduction

Sicherheit von Algorithmen (2)

- Komplexität des Angriffs
  - Data complexity
  - Processing complexity
  - Storage requirements

Kryptoanalytische Angriffe

- Ciphertext only
  Der Angreifer kennt nur die Chiffre
- Known plaintext
  Der Angreifer kennt den Klartext zu der Chiffre
- Choosen plaintext
  Der Angreifer kann zu jedem Klartext eine Chiffre erzeugen
- Adaptive choosen plaintext
  Zusätzlich zu c.p. kann der Angreifer den Klartext auf Basis vorheriger Verschlüsselungen ändern

Angriffe gegen Schlüsselverwaltung

- „Raten” des Schlüssels
  - Brute force
  - Dictionary attack
- Schlüsselgenerator
- Schlüsselübermittlung abfangen
- Diebstahl
- Erpressung

Sonstige sicherheitsrelevante Dinge

- Erst signieren, dann chiffrieren
- Erst hashen, dann signieren
- Erst komprimieren, dann chiffrieren
- Session Keys verwenden
- Je wichtiger ein Schlüssel ist, desto seltener ihn verwenden

PGP

- IDEA zum Verschlüsseln der Private Keys und der Daten durch Session Keys (128 bit Schlüssel)
- RSA zum Signieren der Daten und Verschlüsseln des IDEA Session Keys (je nach PGP Version über 4000 bit Schlüssel möglich)
- MD5 als Hash-Funktion
- Distributed key management (Web of trust)
- ZIP Komprimierung vorm Chiffrieren
- Zeit zwischen dem Drücken der Tasten dient als Basis für den Zufallszahlengenerator