Digitale Signaturen

Proseminar Kryptographie und Datensicherheit
SoSe 2009

Sandra Niemeyer

24.06.2009

Inhalt

1. Signaturgesetz
2. Ziele
3. Sicherheitsanforderungen
4. Erzeugung digitaler Signaturen
5. RSA-Signaturen
6. weitere Signaturverfahren
7. PGP-Systeme
8. Vorteile
9. Nachteile
10. Quellennachweis

Signaturgesetz

„Gesetz über Rahmenbedingungen für elektronische Signaturen“

„Eine sichere elektronische Signatur muss eindeutig das jeweilige Dokument einem Signator zuordnen.“

- seit 16.05.2001 (aktualisiert 2005)
- authentifiziert und identifiziert natürliche oder juristische Person
- nur wenige Geschäfte nicht mit digitalen Signaturen möglich (z.B. Testament, Grundstücksübertragung)
- zur Überwachung technischer Verfahren: Regulierungsbehörde für Telekommunikation und Post (RegTP)

Ziele

- Vertraulichkeit
- Integrität
- Authentizität
- Verbindlichkeit

Sicherheitsanforderungen

- Sicherheit des privaten Schlüssels

Ein Signaturverfahren ist nur sicher, wenn in vertretbarer Zeit aus dem öffentlichen Schlüssel der private Schlüssel nicht abgeleitet werden kann.

Heutzutage ist diese Sicherheit gewährleistet, da bestimmte Berechnungsprobleme in der Zahlentheorie noch schwer zu lösen sind.

Quantencomputer würden bekanntermaßen alle Signaturverfahren unsicher machen.

Sicherheitsanforderungen

- Eine digitale Unterschrift muss folgende Merkmale erfüllen:

1. kann nicht gefälscht werden
2. wurde willentlich unter ein Dokument gesetzt
3. kann nicht auf andere Dokumente übertragen werden
4. kann nachträglich nicht geleugnet werden
5. nachträgliche Änderungen im Dokument nicht möglich

Sicherheitsanforderungen

- Mögliche Attacken:
  - Key only attack
  - No message attack
  - Known message attack
  - Chosen message attack

Sicherheitsanforderungen

- Mögliche Ergebnisse eines Angriffs
  - Existential forgery
  - Selective forgery
  - Total break

Erzeugung digitaler Signaturen

- Symmetrische Verfahren:
  - Dokument kann im Nachhinein geändert werden
  - Merkmale nicht erfüllt → Symmetrische Verfahren entfallen
- Asymmetrische Verfahren:
  - erfüllen Merkmale

- Nachteile:
  - Asymmetrische Verfahren sind langsamer
  - Signaturen sind sehr groß

RSA-Signaturen

1. Schlüsselerzeugung
2. Signaturerzeugung
3. Verifikation
4. Angriffe
5. Sicherheitsvorkehrungen

RSA-Signaturen

- Alice signiert: $s = m^d$
- Bob verifiziert: $m = s^e \bmod n$
- erhält Bob m, ist s verifiziert

  - Dokument m
  - RSA-Modul n
  - Entschlüsselungsexponent d
  - Exponent e

RSA-Signaturen

Schlüsselerzeugung

- Wahl zweier großer Primzahlen p und q
- Wahl eines Exponenten e mit

$$1 < e < (p-1)(q-1) \text{ und } ggT(e, (p-1)(q-1)) = 1$$

- Berechnung von n = pq
- Berechnung von $d \in \mathbb{Z}$ mit

$$1 < d < (p-1)(q-1) \text{ und } de \equiv 1 \bmod (p-1)(q-1)$$

- geheimer Schlüssel: d
- öffentlicher Schlüssel: (n, e)

RSA-Signaturen

Signaturerzeugung

- Alice signiert $m \in \{0,1,\ldots,n-1\}$
- berechnet $s = m^d \bmod n$
- s = Signatur von m

- Diese Signaturmethode ist jedoch noch verbesserungsbedürftig.

RSA-Signaturen

Verifikation

- Bob verifiziert s
- öffentlicher Schlüssel (n,e)
- berechnet $m = s^e \bmod n$

- erhält m aus s → erkennt s als Signatur von m und weiß, dass s von Alice ist

RSA-Signaturen

Angriffe – einfacher Angriff

- Charlie gibt seinen öffentlichen Schlüssel als Alice' aus
- erzeugt Signaturen, die Bob als Alice' Signaturen anerkennt

RSA-Signaturen

Angriffe – No-Message-Attack

- Charlie wählt $s \in \{0,1,\ldots,n-1\}$
- gibt s als Signatur von Alice aus

- ergibt sich beim Verifizieren ein sinnvolles m, scheint diese Signatur glaubwürdig

RSA-Signaturen

Angriffe – Chosen-Message-Attack

- RSA-Verfahren ist multiplikativ
- $m_1, m_2 \in \{0, \ldots, n-1\}$
- s_1, s_2 sind die Signaturen von m_1, m_2
- daraus folgt: $s = s_1 s_2 \bmod n = (m_1 m_2)^d \bmod n$ ist die Signatur von $m = m_1 m_2$
- Angreifer wählt m_1 und berechnet: $m_2 = m m_1^{-1} \bmod n$
- Lässt sich m_1 und m_2 signieren und kann $s = s_1 s_2 \bmod n$ von m berechnen

RSA-Signaturen

Sicherheitsvorkehrungen - allgemein

- Verwendung von Trustcentern

- p und q etwa gleich groß wählen
- müssen zufällig und möglichst gleichverteilt gewählt werden
- n darf nicht zerlegbar sein

RSA-Signaturen

Sicherheitsvorkehrungen - Hashwerte

- $h: \{0,1\}^* \rightarrow \{0,\ldots,n-1\}$
- öffentlich bekannte, kollisionsresistente Hashfunktion (Einwegfunktion)
- Signatur: $s = h(x)^d \bmod n$ (x - Dokument)
- Empfänger erhält (x, s)
- Empfänger berechnet: $m = s^e \bmod n$
- berechnet auch Hashwert h(x)
- stimmen h(x) und m überein, ist s gültig

Weitere Signaturverfahren

- Undeniable Signatures
  - Signator bestimmt Personen, die verifizieren dürfen
  - erfährt durch eigene Beteiligung an Verifizierung von Fälschungsversuchen
- Blind Signatures
  - Signator kennt Inhalt des Dokuments nicht
- Fail-Stop Signatures
  - es kann bewiesen werden, wenn ein Schlüssel geknackt wird (fail)
  - alle Signaturen werden zurückrufen (stop)

PGP-Systeme

Pretty Good Privacy

- 1986-1991 von Phil Zimmermann entwickelt
- Kein Verschlüsselungsalgorithmus → Softwareprodukt
- Fasst viele komplexe Verfahren zusammen

- Jeder Partner kann sich jederzeit Schlüsselpaare erstellen
- Zuordnung durch gegenseitige elektronische „Beglaubigung“ → Web of Trust

- Große Schwäche: verlorene, bekannt gewordene Schlüssel können nicht widerrufen werden

Vorteile

- geringer Zeitaufwand bei Identifizierung, wenn Empfänger bereits bekannt
- rechtlich anerkannt
- einfacher Ablauf von Korrespondenzen
- geringerer Arbeitsaufwand

Nachteile

- Problematik der Geheimhaltung
- Software könnte manipuliert werden
- Software erkennt möglicherweise „falsche“ mathematische Operationen, die von PGP-ähnlichen Programmen erstellt wurden, nicht
- Identitäten könnten vorgetäuscht werden, wenn kein Zertifikat vorliegt

Quellennachweis

- Cryptography – Theory and Practice, Stinson, 3. Auflage, Chapman & Hall
- Einführung in die Kryptographie, Buchmann, 3. erweiterte Auflage, Springer
- DUDEN Informatik A-Z, Schwill & Claus, 4. Auflage, Dudenverlag
- http://www.signaturrecht.de/index.html
- „Digitale Signaturen“, Folien von Sven Tabbert (Universität Potsdam)
- Verschiedene Wikipedia-Seiten:
  - Digitale Signatur
  - Trustcenter (Zertifizierungsstelle)
  - Undeniable signature
  - Fail-stop Signaturen