Kryptographie und Komplexität

Einheit 6.3

Teilnehmerauthentifikation

1. PIN und Passwörter
2. TAN und Einmal-Passwörter
3. iTAN: Challenge-Response-Protokolle
4. Zero-Knowledge Protokolle

Ist der Teilnehmer wer er vorgibt zu sein?

- **Identifikation ist an vielen Stellen notwendig**
  - Internetbanking: Nur Kontoinhaber dürfen den Kontostand einsehen oder Überweisungen tätigen. Die Bank muß feststellen können, ob der Zugreifende wirklich der Inhaber des Kontos ist.
  - Rechnerzugang: Benutzer auf Multiusersystemen haben spezifische Konten und Zugriffsrechte. Der Computer muß prüfen können, welcher Benutzer sich anmeldet
  - Zugang zu Räumen, Bankautomaten, Mobiltelephone, ...
- **Authentifikation prüft Identität von Teilnehmern**
  - Kann dem aktuellen Kommunikationspartner wirklich vertraut werden oder versucht jemand anderes seine Identität anzunehmen?
  - Authentifikation verleiht Rechte, bestimmte Aktivitäten durchzuführen
  - Anders als MACs nicht an konkrete Nachrichten gebunden
- **Teilnehmer brauchen unfälschbare Ausweise**
  - Digitale Information, die ihre Identität ‘eindeutig’ feststellt
  - Physikalische Artefakte (Personalausweis, Chipkarte, ...)

Teilnehmeridentifikation

- **Identifikationsprotokoll gewährt Zugang**
  - Berechtigung: Teilnehmer weist einem Verifizierer seine Identität nach
  - Realzeit: Teilnehmer demonstriert, daß Verifizierer gerade mit ihm kommuniziert oder kurz zuvor mit ihm kommuniziert hat
  - Einseitig oder gegenseitige Authentifikation möglich
- **Anforderungen an Verfahren**
  - Durchführbarkeit: Berechtigte müssen Identität nachweisen können
  - Schutz vor Impersonation: Unberechtigte Teilnehmer können sich nicht als andere ausgeben
  - Unübertragbarkeit: Verifizierer können keine Identitäten annehmen
- **Arten des Identitätsnachweises**
  - Wissen: Geheimnisse, die nur die berechtigte Person kennt
  - Besitz: Objekte, die nur die berechtigte Person besitzt
  - Biometrische Daten: eindeutige körperliche Merkmale der Person

Festcode-Verfahren und Passwörter

- **Teilnehmer besitzt persönliches Geheimnis**
  - Selbstgewählte oder zugewiesene Passwörter oder PIN
- **Verfahren prüft Namen und Geheimnis**
  - Teilnehmer übermittelt Identität und Geheimnis offen auf geschütztem Kanal
  - Verifizierer prüft, ob Geheimnis zur Identität gehört z.B. mithilfe einer (geschützen & verschlüsselten!) Passwortdatei
- **Gängiges Verfahren mit vielen Schwächen**
  - \+ Schnelle Durchführbarkeit, leicht zu implementieren
  - \+ Guter Schutz vor Impersonation durch Amateurangreifer
  - – Verifizierer besitzt alle Geheimnisse und kann jede Identität annehmen
  - – Viele erfolgreiche Angriffe möglich

Angriffe auf Festcode-Verfahren

- **Attacken auf schwache Passwörter**
  – Brute-Force Attacke auf PIN und zu kurze Passwörter
    · Es gibt nur 100000 verschiedene 5-Ziffern PIN
    · Es gibt nur $3{\cdot}10^{12}$ Worte mit 7 alphanumerischen Symbolen
  – Wörterbuchattacke auf Passworte mit Bedeutung
    · Es gibt weniger als 1000000 sinnvolle deutsche Wörter und Namen

  Gegenmaßnahmen
  – Verifizierer begrenzt Anzahl der Versuche (3 für PIN!)
  – Zufällige, komplizierte Passworte (ggf. auf Chipkarte gespeichert)

- **Replay-Attacke**
  – Leitung für Passwortübertragung kann belauscht werden
  – Angreifer kann fremde Identität und Passwort weiterbenutzen

  Gegenmaßnahmen
  – Verifikation erzwingt häufigen Wechsel des Passwortes
  – Aufbau gesicherter Leitungen für Identifikationsprozess
  – Verwendung von Einmalpasswörtern $\mapsto$ Wechselcode-Verfahren

Wechselcode Verfahren und Einmal-Passwörter

- **Passwort wird bei jeder Transaktion gewechselt**
  - Auswahl aus vorher vereinbarter Passwortliste (TAN)
  - Systematische Erzeugung aus Master-Passwort und Einwegfunktion
  - Replay-Attacke wird wirkungslos
- **Lamport Protokoll zur Passworterzeugung**
  - Teilnehmer und Verifizierer verwenden Einwegfunktion f
  - Teilnehmer wählt geheimen Zufallssstring w und Maximalwert t
  - Teilnehmer übermittelt Kontrollpasswort $z = f^t(w)$ an Verfizierer
  - Für Transaktion i verwendet Teilnehmer das Passwort $w_i = f^{t-i}(w)$
    Verifizierer prüft ob $f(w_i) = z$ gilt und setzt danach $z := w_i$
- **Wechselcode Verfahren mit Passwort**
  - Teilnehmer und Verifizierer verwenden Einwegfunktion f
  - Teilnehmer und Verifizierer einigen sich auf Passwort P
  - Passwort für Transaktion zum Zeitpunkt t ist $(t, f(t, P))$
  - Varianten mit öffentlichen Schlüsseln oder MACs möglich

Angriffe auf Wechselcode-Verfahren

- **Phishing Attacke**
  - Angreifer gibt sich gegenüber Teilnehmer als Verifizierer aus und verlangt unter einem Vorwand die Eingabe einer gültigen TAN
  - Leicht durchzuführen und erfolgreich bei gutgläubigen Teilnehmern

  Gegenmaßnahme (nur begrenzt erfolgreich)
  - Kontaktaufnahme darf ausschließlich durch Teilnehmer geschehen
- **Man-in-the-middle Attacke**
  - Angreifer unterbricht Kommunikation zwischen Teilnehmer und Verfizierer (z.B. durch fingierte Fehlermeldung)
  - Angreifer verwendet abgefangenes Geheimnis für eigene Transaktion

  Gegenmaßnahme
  - Auswahl des Passworts wird abhängig von spezifischer Transaktion

    $\mapsto$ Challenge-Response-Verfahren

Challenge-Response Identifikation

- **Teilnehmer muß konkrete Frage beantworten**
  - Auswahl der Frage (Challenge) wird durch Verifizierer kontrolliert
  - Nur berechtigte Teilnehmer kennen die zugehörige Antwort (Response)
  - Einmal gestellte Fragen werden niemals wiederverwendet
  - Einfache Man-in-the-Middle-Attacke wird wirkungslos
- **Einfachste Variante: iTAN-Verfahren**
  - Teilnehmer hat TAN-Liste mit Index
  - Verifizierer verlangt Angabe der TAN mit einem spezifischen Index
  - Gilt heute nicht mehr als sicher genug
- **Kryptographische Variante mit Schlüssel**
  - Teilnehmer berechnet Antwort aus Challenge durch Anwendung seines geheimen Schlüssels (z.B. TAN Generator mit Bankkarte)
  - Verfahren nutzt Verschlüsselung, Signatur oder parametrische Hashs

Kryptographische Challenge-Response Protokolle

- **Einsatz symmetrischer Kryptographie**
  - Verifizierer und Teilnehmer tauschen geheimen Schlüssel aus
  - Teilnehmer sendet Identität an Verifizierer
  - Verifizierer schickt Zufallszahl r als Challenge
  - Teilnehmer sendet $y = e_K(r)$ als Response
  - Verifizierer testet, ob $d_K(y) = r$ gilt

  Problem: Verifizierer muß Teilnehmergeheimnis lesegeschützt lagern

- **Einsatz asymmetrischer Kryptographie**
  - Teilnehmer besitzt geheimen und öffentlichen Schlüssel
  - nach Anmeldung schickt Verifizierer Zufallszahl r als Challenge
  - Teilnehmer berechnet Response $y = e_K(r)$ mit privatem Schlüssel
  - Verifizierer $d_K(y) = r$ mit dem öffentlichen Schlüssel des Teilnehmers

  Problem
  - Öffentlicher Teilnehmerschlüssel muß schreibgeschützt gelagert sein

Authentifizierung mit Zero-Knowledge Beweisen

- **Identifikation ohne Übertragung von Wissen**
  - Teilnehmer überzeugt Verifizierer, daß er ein Geheimnis kennt
  - Verifizierer erfährt dabei nichts über das konkrete Geheimnis
  - Angreifer kann korrekte Antwort auf neue Challenge nicht aus der Beobachtung von Challenge-Response Paaren herleiten
- **Allgemeines Protokoll**
  - Teilnehmer erzeugt Geheimnis und öffentliche Kontrollinformation
  - Commitment: Teilnehmer nimmt Kontakt auf und schickt Kontrollinformation zu einem zufällig gewählten zweiten Geheimnis
  - Challenge: Verifizierer fordert Teilnehmer auf, das zweite Geheimnis oder seine Kombination mit dem ersten offenzulegen
  - Response: Teilnehmer schickt geforderte Information zurück.
  - Verifizierer prüft Response anhand der Kontrollinformationen
- **Sicherheit**
  - Verifizierer stellt mit Wahrscheinlichkeit $1-2^{-k}$ fest ob Teilnehmer das Geheimnis kennt, wenn Protokoll k mal wiederholt wird
  - Geheimnis des Teilnehmers wird durch Zufallsinformation verschleiert

Fiat-Shamir Protokoll

- **Vorbereitung**
  - Teilnehmer T wählt eine Zahl n als Produkt zweier großer Primzahlen p und q, sowie eine zufällige Zahl $s \in \mathbb{Z}_n^*$ und berechnet $v = s^2 \bmod n$
  - Sein öffentlicher Schlüssel ist (v, n) während s geheim bleibt
- **Authentifizierung**
  - Commitment: T wählt zufälliges $r \in \mathbb{Z}_n^*$ und schickt $z = r^2 \bmod n$
  - Challenge: Verifizierer V schickt ein zufälliges Bit e an Teilnehmer T
  - Response: T schickt $y{=}r$ zurück, wenn $e{=}0$ und sonst $y = r{\cdot}s \bmod n$
  - Kontrolle: V prüft $z \equiv y^2 \bmod n$, wenn $e{=}0$ und sonst $z{\cdot}v \equiv y^2 \bmod n$
- **Durchführbarkeit und Sicherheit**
  - Berechtigte Teilnehmer geben immer korrekte Antworten
  - Angreifer kann nicht jede Authentifizierung erfolgreich bestehen
    - · Challenge verhindert, daß er nicht einfach $z = r^2{\cdot}v^{-1} \bmod n$ schickt
    - · Wer r und y sicher angeben kann, kann $s = r^{-1}{\cdot}y \bmod n$ berechnen
    - · Quadratwurzelberechnung modulo n ist so schwer wie Faktorisierung

Zero-Knowledge Beweis für Fiat-Shamir

- **Warum gewinnt Verifizierer kein Wissen?**
  - Verhalten des Teilnehmers gegenüber dem Verifizierer läßt sich simulieren, ohne daß das Geheimnis des Teilnehmer bekannt sein muß
  - Verifizierer gewinnt kein Wissen, wenn Simulator falsch antwortet
  - Folge korrekter Antworten ist von Kontakt durch berechtigte Teilnehmer nicht zu unterscheiden
  - Also kann Verifizierer aus Folge korrekter Antworten nichts lernen
- **Simulator für Fiat-Shamir**
  - Wähle zufälliges $r \in \mathbb{Z}_n^*$, ein Bit b und schicke $z = r^2 \cdot v^{-b} \bmod n$
  - Verifizierer schickt ein zufälliges Bit e
  - Wenn $b{=}e$, dann schicke r zurück an Verifizierer
  - Ansonsten streiche diese Runde des Protokolls
- **Eigenschaften des Simulators**
  - Simulator arbeitet, ohne Geheimnis s zu kennen
  - Dennoch liegen im Mittel nach $2k$ Runden k korrekte Antworten vor

Kriterien für Authentifizierungsprotokolle

- **Weitere Protokolle**
  - Verfahren von Schnorr bzw. von Okamoto oder Guillou-Quisquater verwenden signierte Zertifikate einer zentralen Agentur
  - Können authorisierte Teilnehmer effizient identifizieren
  - Können nichtauthorisierte Angreifer effizient identifizieren
- **Effizienzaspekte**
  - Verifizierer besitzt große Rechenkapazität, Teilnehmer i.a. wenig
  - Verifizierer muß die meiste Rechenlast tragen
  - Authentifizierungsaufwand für Teilnehmer muß gering sein
- **Sicherheitsaspekte**
  - Kryptographische Mittel können Replay Attackenverhindern
  - Man-in-the-middle Attacken können nur mit aufwendigeren Schlüsseletablierungsprotokollen unterbunden werden (z.B. Diffie-Hellman mit Zertifikaten und Zeitstempeln)
  - Viele Attacken werden durch geschützte Umgebungen eingeschränkt