SIEMENS

CORPORATE TECHNOLOGY

Formale Analyse von Sicherheits-protokollen:

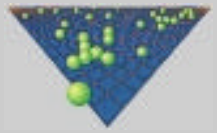
State-of-the-art

Volkmar Lotz

Siemens AG, Corporate Technology, Security

D-81730 München

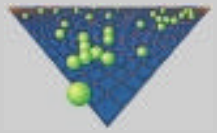
volkmar.lotz@siemens.com



Information & Communications Security

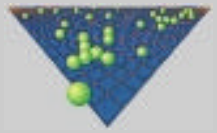
Übersicht

- **Problemstellung**
- **Abstraktionsniveau**
- **Ansätze**
- **Forschungsrichtungen**
- **Der Valikrypt-Ansatz**



Problemstellung

- **Sicherheitsprotokoll: Vorschrift zur Interaktion zwischen Entitäten zur Etablierung von Sicherheitszielen**
- **Sicherheitsziele:**
  - Authentizität der Protokollteilnehmer
  - sichere Schlüsselverteilung
  - Vertraulichkeit übertragener Daten
  - ...
- **Protokolle sind fehleranfällig!**
  - Definition der Sicherheitsziele
  - Berücksichtigung des Angreiferverhaltens
  - Anwendung kryptographischer Operationen
  - Verteilte Systeme

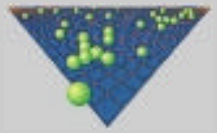


Das klassische Beispiel: Needham-Schroeder-Public-Key-Protokoll (1978/95)

$$
\begin{array}{lrcl}
\text{M1.} & A \to B & : & \{A, n_A\}_{K_B^+} \\
\text{M2.} & B \to A & : & \{n_A, n_B\}_{K_A^+} \\
\text{M3.} & A \to B & : & \{n_B\}_{K_B^+}
\end{array}
$$

$$
\begin{array}{lrcl}
\text{M1(1).} & A \to I & : & \{A, n_A\}_{K_I^+} \\
\text{M1(2).} & I(A) \to B & : & \{A, n_A\}_{K_B^+} \\
\text{M2(2).} & B \to I(A) & : & \{n_A, n_B\}_{K_A^+} \\
\text{M2(1).} & I \to A & : & \{n_A, n_B\}_{K_A^+} \\
\text{M3(1).} & A \to I & : & \{n_B\}_{K_I^+} \\
\text{M3(2).} & I(A) \to B & : & \{n_B\}_{K_B^+}
\end{array}
$$

- **Angriff erst durch formale Analyse gefunden (Lowe, 1995)**
- ***"Finally, protocols such as those developed here are prone to extremely subtle errors that are unlikely to be detected in normal operation. The need for techniques to verify the correctness of such protocols is great, and we encourage those interested in such problems to consider this area."***
  Needham/Schroeder 1978



Abstraktionsniveau

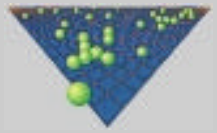
- **Nachrichten als Terme einer Algebra:**

$$m = \{A, n_A, \{B, n_B\}_{K_B^+}\}_{K_A^+}$$

- **Annahme perfekter Kryptographie**

$$\{m\}_k = \{m'\}_{k'} \Rightarrow m = m' \wedge k = k'$$

- **Dolev-Yao-Annahmen über Angreiferverhalten (1983):**
  - Angreifer hat vollständige Kontrolle über Kommunikation (Abhören, Löschen, Modifizieren, ...)
  - Angreifer kann keine Geheimnisse erraten



Aktuelle Ansätze (1)

- **Authentifikationslogiken**
  - Spezielle Modallogiken (BAN, GNY, …)
  - Nachteil: Idealisierung, Secrecy kann nicht gezeigt werden

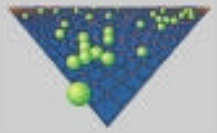
$$A \models B \models A \leftrightarrow_K B$$

- **Verifikationsansätze**
  - Induktive Methode (Paulson)
  - Strand Spaces (Guttman et al.)
  - Prozeßalgebren
    - CSP (Roscoe, Schneider et al.)
    - Spi-Kalkül (Abadi)

$$Fake \quad evs \in tr, Bx \neq E, Msg \in synth.analz.spies.evs \Rightarrow evs \ \# \ Says.E.Bx.Msg \ \in \ tr$$

$$InitiatorA?\ run.A\ ?\ \ send.A.B.msg1\ ?\ ([]m?\ Msg\ ...)$$

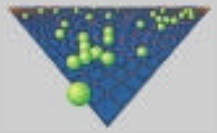
- **Automatische Validierung**
  - Model-Checking endlicher Repräsentationen des Protokolls
  - FDR, Mur?, Maude, …



Aktuelle Ansätze (2)

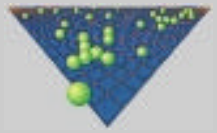
- **Constraint Solving**
  - Unendliche Zustandssysteme,
  - Session Instances
  - OFMC (Basin), Constraint Solver (Millen, Rusinowitch), …
- **Spezifikationssprachen**
  - CASPER (Lowe)
  - CAPSL (Millen)
  - HLPSL (AVISPA-Projekt)
  - Abbildung auf Zwischensprachen (CSP, CIL, IF) ab, in denen z.B. Angreifermodell und Operatoren festgelegt werden und die direkt analysiert werden können

```
PROTOCOL NeedhamSchroederPK;
VARIABLES
        A, B, S: PKUser;
        Na, Nb: Nonce;
        sks , ska : Pkey;
DENOTES
        sks = sk(S);
        ska = sk(A);
ASSUMPTIONS
        HOLDS A: B, S;
        HOLDS B: S;
MESSAGES
        1. A -> S: A, B;
        2. S -> A: {pk(B), B}sk(S);
        3. A -> B: A, {Na, A}pk(B);
        4. B -> S: B, A;
        5. S -> B: {pk(A), A}sk(S);
        6. B -> A: B, {Na, Nb}pk(A);
        7. A -> B: {Nb}pk(B);
GOALS
        SECRET Na;
        SECRET Nb;
        PRECEDES A: B | Na;
        PRECEDES B: A | Nb;
END;
```



Forschungsrichtungen

- **Probabilistische Berechnungsmodelle**
  - Annäherung an Eigenschaften realer kryptographischer Verfahren
- **Optimierung automatischer (Model-Checking)-Verfahren**
  - Abstraktionstechniken
  - Reduktion des Suchraums
  - Heuristiken
- **Beherrschung großer Protokolle**
  - Z.B. IETF, ITU, W3C



Der Valikrypt-Ansatz

- **Kombination trace-basierter und automatenbasierter Verifikations- und Validierungsansätze**
  - Paulson-Methode (✍ VSE)
  - Asynchrone Produktautomaten (✍ SHVT)
- **Systematischer, formaler Übergang zwischen Spezifikationen**
- **Erfassung kryptographischer Aspekte**
  - Erweiterte Modelle für die Protokollanalyse
  - Regelbasierte Auswahl konkreter Algorithmen und deren Parametrisierung