Hauptseminar Kryptographische Protokolle

Protokollverifikation mit BAN-Logik

Maximilian Schlund

Fakultät für Mathematik
TU München

29. Juni 2009

Wir wollen Protokolle für gegenseitige Authentifizierung studieren. D.h. nach dem Ablauf eines Protokolls soll A sich sicher sein können, dass sie mit B redet und umgekehrt.

Beispiele:

Wir wollen Protokolle für gegenseitige Authentifizierung studieren. D.h. nach dem Ablauf eines Protokolls soll A sich sicher sein können, dass sie mit B redet und umgekehrt.

Beispiele:

Symmetrisches Needham-Schroeder-Protokoll

M1 $A \rightarrow S : A, B, N_a$

M2 $S \rightarrow A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$

M3 $A \rightarrow B : \{K_{ab}, A\}_{K_{bs}}$

M4 $B \rightarrow A : \{N_b\}_{K_{ab}}$

M5 $A \rightarrow B : \{N_b - 1\}_{K_{ab}}$

Problem: Replay Attacke in Schritt 3 - *falls* ein Angreifer einen alten Sitzungsschlüssel K'_{ab} besitzt, kann er diesen B unterschieben.

Replay-Angriff

M3' $E(A) \rightarrow B : \{K'_{ab}, A\}_{K_{bs}}$

M4' $B \rightarrow E(A) : \{N_b\}_{K'_{ab}}$

M5' $E(A) \rightarrow B : \{N_b - 1\}_{K'_{ab}}$

B glaubt danach mit A zu reden, redet aber mit E.

Weiteres Beispiel: CCITT X.509 Protokoll (erster Entwurf) - sicherer signierter Dateiaustausch. A will an B (vertrauliche) Daten Y_a schicken, B antwortet umgekehrt mit Daten Y_b:

M1 $A \rightarrow B : A, \{T_a, N_a, B, \{Y_a\}_{K_b}\}_{K_a^{-1}}$

M2 $B \rightarrow A : B, \{T_b, N_b, A, N_a, \{Y_b\}_{K_a}\}_{K_b^{-1}}$

M3 $A \rightarrow B : A, \{N_b\}_{K_a^-1}$

Probleme:

Weiteres Beispiel: CCITT X.509 Protokoll (erster Entwurf) - sicherer signierter Dateiaustausch. A will an B (vertrauliche) Daten Y_a schicken, B antwortet umgekehrt mit Daten Y_b:

M1 $A \rightarrow B : A, \{T_a, N_a, B, \{Y_a\}_{K_b}\}_{K_a^{-1}}$

M2 $B \rightarrow A : B, \{T_b, N_b, A, N_a, \{Y_b\}_{K_a}\}_{K_b^{-1}}$

M3 $A \rightarrow B : A, \{N_b\}_{K_a^-1}$

Probleme:

- B kann sich nicht sicher sein, dass A Kenntnis von Y_a hat!

Weiteres Beispiel: CCITT X.509 Protokoll (erster Entwurf) - sicherer signierter Dateiaustausch. A will an B (vertrauliche) Daten Y_a schicken, B antwortet umgekehrt mit Daten Y_b:

M1 $A \rightarrow B : A, \{T_a, N_a, B, \{Y_a\}_{K_b}\}_{K_a^{-1}}$

M2 $B \rightarrow A : B, \{\quad N_b, A, N_a, \{Y_b\}_{K_a}\}_{K_b^{-1}}$

M3 $A \rightarrow B : A, \{N_b\}_{K_a^-1}$

Probleme:

- B kann sich nicht sicher sein, dass A Kenntnis von Y_a hat!
- T_b ist eigentlich redundant - warum?

Weiteres Beispiel: CCITT X.509 Protokoll (erster Entwurf) - sicherer signierter Dateiaustausch. A will an B (vertrauliche) Daten Y_a schicken, B antwortet umgekehrt mit Daten Y_b:

M1 $A \rightarrow B : A, \{ \quad N_a, B, \{Y_a\}_{K_b} \}_{K_a^{-1}}$

M2 $B \rightarrow A : B, \{ \quad N_b, A, N_a, \{Y_b\}_{K_a} \}_{K_b^{-1}}$

M3 $A \rightarrow B : A, \{N_b\}_{K_a^-1}$

Probleme:

- B kann sich nicht sicher sein, dass A Kenntnis von Y_a hat!
- T_b ist eigentlich redundant - warum?
- Vorschlag des Entwurfs: T_a sei auch redundant - warum ist das Quatsch?

Weiteres Beispiel: CCITT X.509 Protokoll (erster Entwurf) - sicherer signierter Dateiaustausch. A will an B (vertrauliche) Daten Y_a schicken, B antwortet umgekehrt mit Daten Y_b:

M1 $A \rightarrow B : A, \{ \quad N_a, B, \{Y_a\}_{K_b} \}_{K_a^{-1}}$

M2 $B \rightarrow A : B, \{ \quad N_b, A, N_a, \{Y_b\}_{K_a} \}_{K_b^{-1}}$

M3 $A \rightarrow B : A, \{N_b\}_{K_a^-1}$

Probleme:

- B kann sich nicht sicher sein, dass A Kenntnis von Y_a hat!
- T_b ist eigentlich redundant - warum?
- Vorschlag des Entwurfs: T_a sei auch redundant - warum ist das Quatsch?

$\rightsquigarrow$ Replay-Möglichkeit

Eine mögliche Abhilfe gegen solche Fehler

formale Methoden", d.h. mathematische Modellierung und Verifikation des Modells.

Eine mögliche Abhilfe gegen solche Fehler

formale Methoden", d.h. mathematische Modellierung und Verifikation des Modells.

Zu modellieren sind:

- Nachrichten, Teilnehmer, Kommunikationskanäle (z.B.: Wörter, Automaten, logische Formeln, . . .)
- Angreifer, z.B.:
  - Kann Nachrichten lesen, abfangen, wiedereinspielen, erfinden.
  - Kann nicht: Verschlüsselung brechen $\rightsquigarrow$ Dolev-Yao-Modell
- Protokoll (informelle Beschreibung $\rightarrow$ Modellbeschreibung) (z.B.: Übergangsfunktion von Automaten, Transformation von Formelmengen,. . .)

Prinzipielles Problem beim Modellieren:

Bildet mein Modell die Realität hinreichend gut ab? D.h. lassen sich die gewünschten Aussagen über das Modell auf die Realität übertragen?

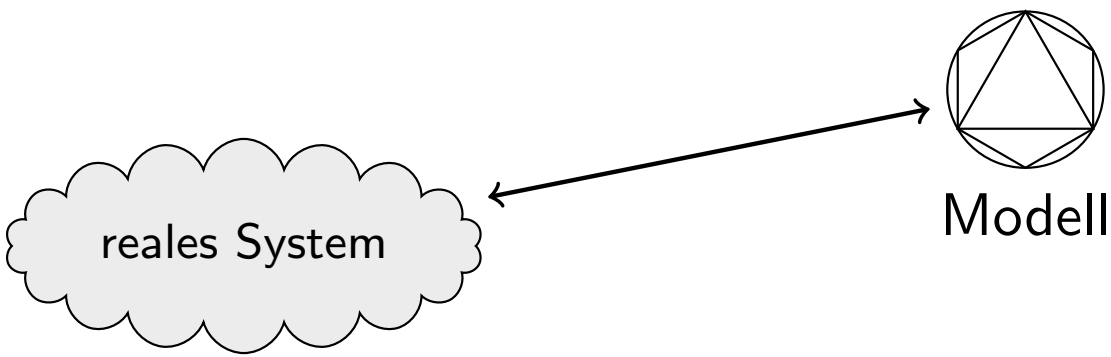

Abbildung: Was wir haben wollen...

Prinzipielles Problem beim Modellieren:

Bildet mein Modell die Realität hinreichend gut ab? D.h. lassen sich die gewünschten Aussagen über das Modell auf die Realität übertragen?

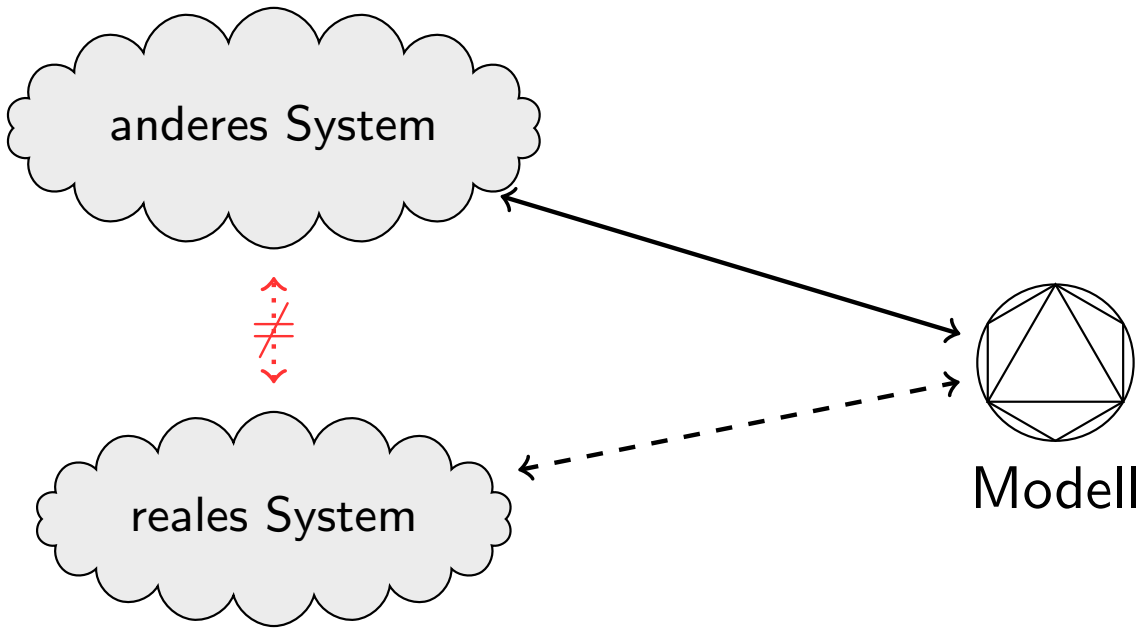

Abbildung: Was wir haben wollen. . . und was wir oft bekommen

Prinzipielles Problem beim Modellieren:

Bildet mein Modell die Realität hinreichend gut ab? D.h. lassen sich die gewünschten Aussagen über das Modell auf die Realität übertragen?

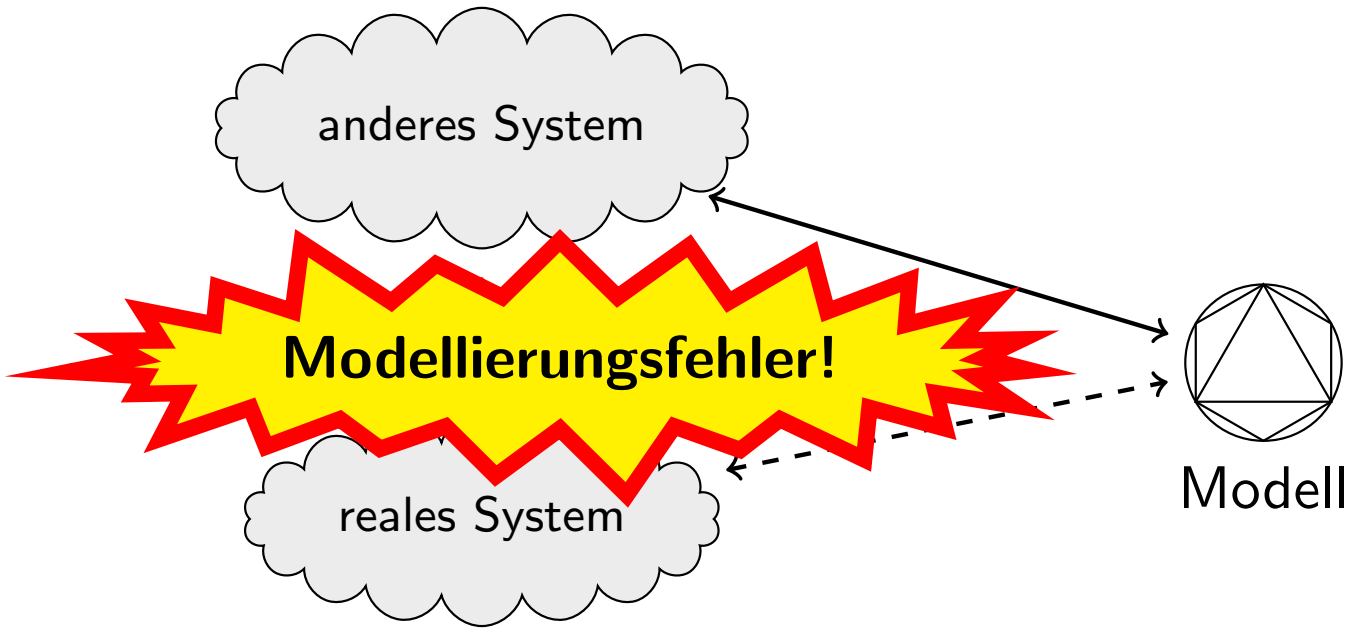

Abbildung: Was wir haben wollen. . . und was wir oft bekommen

Verschiedene Ansätze zur formalen Verifikation von Protokollen

- Model Checking
- Induktive Verifikation (L.C. Paulson, Inductive Verification for Crypto-Protocols)
- Prozesskalküle (π-Kalkül, Milner - CCS)
- Modallogik (BAN-Logik, GNY-Logik)
- ...

Was ist BAN-Logik?

- Burrows, Abadi, Needham: "A Logic of Authentication"

$\longrightarrow$ Modell für Authentifizierungsprozess

- Modelliert Entwicklung von Vertrauen/Glauben während eines Protokollablaufs. Erlaubt Aussagen, wie "Alice glaubt, dass Bob Nachricht N gesendet hat"
- Erlaubt keine Aussagen über Sicherheit von Geheimnissen, Zeit, etc.

Was braucht man zur Definition eines Logikkalküls? $\rightsquigarrow$ Syntaxdefinition, (Axiome) und logische Schlussregeln.

Formeln (Auswahl) der BAN-Logik (induktiv! - X ist eine Formel):

- $A \models X$: A glaubt/kennt X
- $A \triangleleft X$: A sieht X ($\rightsquigarrow$ A empfängt Nachricht X)
- $A \mid\sim X$: A sagte X
- $S \Rightarrow X$: S kann bezüglich X vertraut werden.
- $A \overset{K}{\longleftrightarrow} B$: K ist gemeinsamer Schlüssel (nur) für A und B
- $\overset{K}{\mapsto} A$: K ist öffentlicher Schlüssel von A
- $\sharp(X)$: Formel X ist "frisch" bzw. "aktuell" ($\rightsquigarrow$ Timestamps und Nonces)
- $\{X\}_K$: X ist verschlüsselt mit K

Logische Schlussregeln (Auswahl):

Erinnerung:

- $A \triangleleft X$: A sieht X
- $A \mid\sim X$: A sagte X
- $\overset{K}{\mapsto} A$: K ist Pubkey von A
- $A \overset{K}{\leftrightarrow} B$: K ist Schlüssel für A und B

"Message Meaning Rules"

$$\frac{A \mid\equiv A \overset{K}{\leftrightarrow} B, \quad A \triangleleft \{X\}_K}{A \mid\equiv B \mid\sim X} \ (MM_{sym})$$

$$\frac{A \mid\equiv \overset{K}{\mapsto} B, \quad A \triangleleft \{X\}_{K^{-1}}}{A \mid\equiv B \mid\sim X} \ (MM_{asym})$$

Erinnerung:

- $A \mid\sim X$: A sagte X
- $\sharp(X)$: X ist frisch/aktuell

"Nonce Verification Rule"

$$\frac{A \models \sharp(X), \quad A \models B \mid\sim X}{A \models B \models X} \ (NV)$$

D.h. wenn A glaubt, dass die Formel X frisch ist dann glaubt A, dass der Sender B sie noch glaubt.

"Jurisdiction Rule"

$$\frac{A \models S \Rightarrow X, \quad A \models S \models X}{A \models X} \ (J)$$

Wenn A glaubt, dass sie S in Puncto X vertrauen kann und auch glaubt, dass S X glaubt, so glaubt sie selbst an X.

Ein Teil frisch $\Rightarrow$ ganze Formel frisch

$$\frac{A \models \sharp(X)}{A \models \sharp(X, Y)} \ (F_I)$$

Entschlüsselungsregeln

$$\frac{A \models A \overset{K}{\leftrightarrow} B, \quad A \triangleleft \{X\}_K}{A \triangleleft X} \ (Dec_{sym})$$

$$\frac{A \models \overset{K}{\mapsto} A, \quad A \triangleleft \{X\}_K}{A \triangleleft X} \ (Dec_{asym})$$

Gleich mal ein kleines Beispiel:

M1 $A \rightarrow B : N_a$

M2 $B \rightarrow A : \{N_a, X\}_{K_{ab}}$

Gleich mal ein kleines Beispiel:

M1 $A \rightarrow B : N_a$

M2 $B \rightarrow A : \{N_a, X\}_{K_{ab}}$

Wir nehmen an: $A \models A \overset{K_{ab}}{\longleftrightarrow} B$ und $A \models \sharp(N_a)$.
und aus der Protokollbeschreibung: $A \triangleleft \{N_a, X\}_{K_{ab}}$.
Hieraus können wir ableiten:

Gleich mal ein kleines Beispiel:

M1 $A \rightarrow B : N_a$

M2 $B \rightarrow A : \{N_a, X\}_{K_{ab}}$

Wir nehmen an: $A \models A \overset{K_{ab}}{\longleftrightarrow} B$ und $A \models \sharp(N_a)$.
und aus der Protokollbeschreibung: $A \triangleleft \{N_a, X\}_{K_{ab}}$.
Hieraus können wir ableiten:

$$\frac{A \triangleleft \{T_a, X\}_{K_{ab}} \qquad A \models A \overset{K_{ab}}{\longleftrightarrow} B}{A \models B \mid\sim (T_a, X)} (MM)$$

Gleich mal ein kleines Beispiel:

M1 $A \rightarrow B : N_a$

M2 $B \rightarrow A : \{N_a, X\}_{K_{ab}}$

Wir nehmen an: $A \models A \overset{K_{ab}}{\longleftrightarrow} B$ und $A \models \sharp(N_a)$.
und aus der Protokollbeschreibung: $A \triangleleft \{N_a, X\}_{K_{ab}}$.
Hieraus können wir ableiten:

$$\frac{A \triangleleft \{T_a, X\}_{K_{ab}} \qquad A \models A \overset{K_{ab}}{\longleftrightarrow} B}{A \models B \mid\sim (T_a, X)} (MM)$$

$$(F_I) \frac{A \models \sharp(T_a)}{A \models \sharp(T_a, X)}$$

Gleich mal ein kleines Beispiel:

M1 $A \rightarrow B : N_a$

M2 $B \rightarrow A : \{N_a, X\}_{K_{ab}}$

Wir nehmen an: $A \models A \overset{K_{ab}}{\longleftrightarrow} B$ und $A \models \sharp(N_a)$.
und aus der Protokollbeschreibung: $A \triangleleft \{N_a, X\}_{K_{ab}}$.
Hieraus können wir ableiten:

$$(F_I)\ \frac{\dfrac{A \models \sharp(T_a)}{A \models \sharp(T_a, X)} \qquad \dfrac{A \triangleleft \{T_a, X\}_{K_{ab}} \qquad A \models A \overset{K_{ab}}{\longleftrightarrow} B}{A \models B \mid\sim (T_a, X)}\ (MM)}{A \models B \models (T_a, B)}\ (NV)$$

Wie verifizieren wir damit denn bitteschön ein Protokoll???

- Protokoll = Folge von Send-Statements $S_1, S_2, \ldots, S_n$

Wie verifizieren wir damit denn bitteschön ein Protokoll???

- Protokoll = Folge von Send-Statements $S_1, S_2, \ldots, S_n$
- Jedes Send-Statement verändert das Vertrauen/den Glauben der Teilnehmer an bestimmte Aussagen

Wie verifizieren wir damit denn bitteschön ein Protokoll???

- Protokoll = Folge von Send-Statements $S_1, S_2, \ldots, S_n$
- Jedes Send-Statement verändert das Vertrauen/den Glauben der Teilnehmer an bestimmte Aussagen

$\rightsquigarrow$ Glauben ist durch BAN-Formeln beschreibbar!

Wie verifizieren wir damit denn bitteschön ein Protokoll???

- Protokoll = Folge von Send-Statements $S_1, S_2, \ldots, S_n$
- Jedes Send-Statement verändert das Vertrauen/den Glauben der Teilnehmer an bestimmte Aussagen

$\rightsquigarrow$ Glauben ist durch BAN-Formeln beschreibbar!

- Jedes Send-Statement transformiert also eine Menge von BAN-Formeln (Axiomatische Semantik!)

Wie verifizieren wir damit denn bitteschön ein Protokoll???

- Protokoll = Folge von Send-Statements $S_1, S_2, \ldots, S_n$
- Jedes Send-Statement verändert das Vertrauen/den Glauben der Teilnehmer an bestimmte Aussagen

$\rightsquigarrow$ Glauben ist durch BAN-Formeln beschreibbar!

- Jedes Send-Statement transformiert also eine Menge von BAN-Formeln (Axiomatische Semantik!)
- Idee analog zum Floyd-Hoare-Kalkül: Annotiere das Protokoll mit Formeln $[A_i]$

Wie verifizieren wir damit denn bitteschön ein Protokoll???

- Protokoll = Folge von Send-Statements $S_1, S_2, \ldots, S_n$
- Jedes Send-Statement verändert das Vertrauen/den Glauben der Teilnehmer an bestimmte Aussagen

$\rightsquigarrow$ Glauben ist durch BAN-Formeln beschreibbar!

- Jedes Send-Statement transformiert also eine Menge von BAN-Formeln (Axiomatische Semantik!)
- Idee analog zum Floyd-Hoare-Kalkül: Annotiere das Protokoll mit Formeln $[A_i]$

$\rightsquigarrow$ $[A_0]S_1[A_1]S_2 \ldots [A_{n-1}]S_n[A_n]$

Wie verifizieren wir damit denn bitteschön ein Protokoll???

- Protokoll = Folge von Send-Statements $S_1, S_2, \ldots, S_n$
- Jedes Send-Statement verändert das Vertrauen/den Glauben der Teilnehmer an bestimmte Aussagen

$\rightsquigarrow$ Glauben ist durch BAN-Formeln beschreibbar!

- Jedes Send-Statement transformiert also eine Menge von BAN-Formeln (Axiomatische Semantik!)
- Idee analog zum Floyd-Hoare-Kalkül: Annotiere das Protokoll mit Formeln $[A_i]$

$\rightsquigarrow$ $[A_0]S_1[A_1]S_2 \ldots [A_{n-1}]S_n[A_n]$

- Verifiziere lokale Konsistenz - für jedes S_i beweise: wenn vor dem Senden von S_i A_{i-1} gilt, dann gilt nach dem Senden auch A_n.

Seien Γ und Φ Formelmengen der BAN-Logik, wir schreiben $\Gamma \vdash \Phi$ falls sich jedes $\varphi \in \Phi$ durch Anwenden von Schlussregeln aus Γ herleiten lässt.

Definition ((lokale) Konsistenz)

$[A_{i-1}]\ \underbrace{P \rightarrow Q : X}_{S_i}\ [A_i]$ heißt lokal konsistent annotiert, gdw.

$$A_{i-1} \cup (Q \triangleleft X) \vdash A_i$$

Die Sequenz $[A_0]S_1[A_1]S_2 \ldots [A_{n-1}]S_n[A_n]$ heißt konsistent annotiert wenn jedes Tripel $[A_{i-1}]\ S_i\ [A_i]$ lokal konsistent ist.

“Korrektheit“ der BAN-Logik?

Korrektheit: Falls ein Protokoll konsistent annotiert ist so gilt: Wenn die Annahmen A_0 erfüllt sind so gelten nach dem Ablauf des Protokolls die Aussagen in A_n.

"Korrektheit" der BAN-Logik?

Korrektheit: Falls ein Protokoll konsistent annotiert ist so gilt: Wenn die Annahmen A_0 erfüllt sind so gelten nach dem Ablauf des Protokolls die Aussagen in A_n.

Achtung!

Diese Aussage ist trivial, falls wir als Semantik für die S_i die axiomatische Semantik nehmen! Damit sie an Wert für die Realität gewinnt müsste man eine realistischere (z.B. operationale) Semantik für den Protokollablauf aufstellen und dann die Korrektheit beweisen!

Modellierung

1. idealisierte Protokollbeschreibung (welche Formeln werden hin und hergeschickt?)
2. Formulierung von Annahmen und Verifikationsziele
3. Überprüfen, ob die Ziele aus den Annahmen herleitbar sind

Beispiele für sinnvolle Annahmen

- $A \models \sharp(N_a)$, falls N_a eine Nonce ist, die von A erstellt wurde
- $A \models S \Rightarrow K_{ab}$, A vertraut S zur Schlüsselerzeugung
- $A \models A \overset{K}{\leftrightarrow} S$, falls A und S schon einen gemeinsamen Schlüssel besitzen

Beispiele für Authentifikationsziele

- $A \models A \overset{K_{ab}}{\longleftrightarrow} B$ und $B \models A \overset{K_{ab}}{\longleftrightarrow} B$: Austausch eines gemeinsamen Schlüssels.
- $A \models \overset{B}{\mapsto}$ (und/oder) $B \models \overset{A}{\mapsto}$: Austausch von öffentlichen Schlüsseln.
- $A \models A \overset{Y}{\rightleftharpoons} B$: Austausch eines gemeinsames Geheimnis.

Breitmaulfrosch-Protokoll

M1 $A \rightarrow S : A, \{T_a, B, K_{ab}\}_{K_{as}}$

M2 $S \rightarrow B : S, \{T_s, A, K_{ab}\}_{K_{bs}}$

Idealisierte Version

M1 $A \rightarrow S : \{T_a, (A \overset{K_{ab}}{\longleftrightarrow} B)\}_{K_{as}}$

M2 $S \rightarrow B : \{T_s, A \models A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}$

Annotierte Version

$$[A_0]\ M_1\ [A_0]\ M2\ [B \models A \overset{K_{ab}}{\longleftrightarrow} B, A \models A \overset{K_{ab}}{\longleftrightarrow} B]$$

Breitmaulfrosch-Protokoll

M1 $A \rightarrow S : A, \{T_a, B, K_{ab}\}_{K_{as}}$

M2 $S \rightarrow B : S, \{T_s, A, K_{ab}\}_{K_{bs}}$

Idealisierte Version

M1 $A \rightarrow S : \{T_a, (A \overset{K_{ab}}{\longleftrightarrow} B)\}_{K_{as}}$

M2 $S \rightarrow B : \{T_s, A \models A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}$

Annotierte Version

$$[A_0]\ M_1\ [A_0]\ M2\ [B \models A \overset{K_{ab}}{\longleftrightarrow} B, A \models A \overset{K_{ab}}{\longleftrightarrow} B]$$

Annahmen ($= A_0$)

- $A \models A \overset{K_{as}}{\longleftrightarrow} S$
- $S \models A \overset{K_{as}}{\longleftrightarrow} S$
- $A \models A \overset{K_{ab}}{\longleftrightarrow} B$
- $S \models \sharp(T_a)$
- $B \models \sharp(T_s)$
- $B \models A \overset{K_{bs}}{\longleftrightarrow} S$
- $S \models B \overset{K_{bs}}{\longleftrightarrow} S$
- $B \models (A \Rightarrow A \overset{K_{ab}}{\longleftrightarrow} B)$
- $B \models (S \Rightarrow A \models A \overset{K_{ab}}{\longleftrightarrow} B)$

$$(F_I)\ \frac{S \models \sharp(T_a) \qquad \dfrac{S \lhd \{T_a, (A \overset{K}{\longleftrightarrow} B)\}_{K_{as}} \qquad S \models A \overset{K_{as}}{\longleftrightarrow} S}{S \models A \mid\sim (T_a, A \overset{K_{ab}}{\longleftrightarrow} B)}\ (MM)}{S \models A \models (T_a, A \overset{K_{ab}}{\longleftrightarrow} B)}\ (NV)$$

$$\dfrac{\dfrac{\dfrac{B \lhd \{T_s, A \models (A \overset{K_{ab}}{\longleftrightarrow} B)\}_{K_{bs}} \qquad B \models B \overset{K_{bs}}{\longleftrightarrow} S}{B \models S \mid\sim (T_s, A \models (A \overset{K_{ab}}{\longleftrightarrow} B))}\,(MM) \qquad \dfrac{B \models \sharp(T_s)}{B \models \sharp(T_s, A \models (A \overset{K_{ab}}{\longleftrightarrow} B))}\,(F_I)}{B \models S \models (T_s, A \models (A \overset{K_{ab}}{\longleftrightarrow} B))}\,(NV)}{(1)\ B \models S \models A \models (A \overset{K_{ab}}{\longleftrightarrow} B)}\,(BB_E)$$

$$\dfrac{\dfrac{(1) \qquad B \models (S \Rightarrow A \models A \overset{K_{ab}}{\longleftrightarrow} B)}{B \models A \models A \overset{K_{ab}}{\longleftrightarrow} B}\,(J) \qquad B \models (A \Rightarrow A \overset{K_{ab}}{\longleftrightarrow} B)}{B \models A \overset{K_{ab}}{\longleftrightarrow} B}\,(J)$$

Needham-Schroeder-Protokoll

M1 $A \rightarrow S : A, B, N_a$

M2 $S \rightarrow A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$

M3 $A \rightarrow B : \{K_{ab}, A\}_{K_{bs}}$

M4 $B \rightarrow A : \{N_b\}_{K_{ab}}$

M5 $A \rightarrow B : \{N_b - 1\}_{K_{ab}}$

Needham-Schroeder-Protokoll

M1 $A \rightarrow S : A, B, N_a$

M2 $S \rightarrow A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$

M3 $A \rightarrow B : \{K_{ab}, A\}_{K_{bs}}$

M4 $B \rightarrow A : \{N_b\}_{K_{ab}}$

M5 $A \rightarrow B : \{N_b - 1\}_{K_{ab}}$

Idealisierte Version

M2' $S \rightarrow A : \left\{ N_a, A \overset{K_{ab}}{\longleftrightarrow} B, \sharp(A \overset{K_{ab}}{\longleftrightarrow} B), \left\{ A \overset{K_{ab}}{\longleftrightarrow} B \right\}_{K_{bs}} \right\}_{K_{as}}$

M3' $A \rightarrow B : \left\{ A \overset{K_{ab}}{\longleftrightarrow} B \right\}_{K_{bs}}$

M4' $B \rightarrow A : \left\{ N_b, A \overset{K_{ab}}{\longleftrightarrow} B \right\}_{K_{ab}}$

M5' $A \rightarrow B : \left\{ N_b, A \overset{K_{ab}}{\longleftrightarrow} B \right\}_{K_{ab}}$

Idealisierte Version

M2' $S \rightarrow A : \left\{ N_a, A \overset{K_{ab}}{\longleftrightarrow} B, \sharp(A \overset{K_{ab}}{\longleftrightarrow} B), \left\{ A \overset{K_{ab}}{\longleftrightarrow} B \right\}_{K_{bs}} \right\}_{K_{as}}$

M3' $A \rightarrow B : \left\{ A \overset{K_{ab}}{\longleftrightarrow} B \right\}_{K_{bs}}$

M4' $B \rightarrow A : \left\{ N_b, A \overset{K_{ab}}{\longleftrightarrow} B \right\}_{K_{ab}}$

M5' $A \rightarrow B : \left\{ N_b, A \overset{K_{ab}}{\longleftrightarrow} B \right\}_{K_{ab}}$

sinnvolle Annahmen (u.a):

- $B \models B \overset{K_{bs}}{\longleftrightarrow} S$
- $B \models \sharp(N_b)$
- $B \models (S \Rightarrow A \overset{K_{ab}}{\longleftrightarrow} B)$
- $B \models (S \Rightarrow \sharp(A \overset{K_{ab}}{\longleftrightarrow} B))$

Ziel: $B \models A \overset{K_{ab}}{\longleftrightarrow} B$

M3' gibt uns nur: $B \models S \mid\sim A \overset{K_{ab}}{\longleftrightarrow} B$

wir bräuchten: $B \models \sharp(A \overset{K_{ab}}{\longleftrightarrow} B)$

Das ist aber nicht herleitbar!

Vorteile von BAN-Logik

- kann subtile Fehler entdecken
- fördert genaueres Verständnis eines Protokolls
- hilft bei der Identifikation von Redundanz im Protokoll
- Automatisierbarkeit (BAN-Logik ist entscheidbar - sogar für die Praxis relativ effizient)

Vorteile von BAN-Logik

- kann subtile Fehler entdecken
- fördert genaueres Verständnis eines Protokolls
- hilft bei der Identifikation von Redundanz im Protokoll
- Automatisierbarkeit (BAN-Logik ist entscheidbar - sogar für die Praxis relativ effizient)

Nachteile von BAN-Logik

- unklare Semantik
  - $\rightsquigarrow$ kein Schema für Protokollidealisierung ("meistens klar. . . ")
  - $\rightsquigarrow$ Fehlerhafte Modellierung ist ziemlich einfach :-) $\Rightarrow$ Korrektheits-"beweise" sind dann nichts mehr wert (gefährlich!)
- keine Formalisierung und Betrachtung von "Geheimhaltung"(also: Niemand außer A oder B kennt K_{AB}").

Fazit

nettes Werkzeug in der Sammlung zum Auffinden von Fehlern - aber nicht gut geeignet um Abwesenheit von Fehlern zu beweisen!

Fazit

nettes Werkzeug in der Sammlung zum Auffinden von Fehlern - aber nicht gut geeignet um Abwesenheit von Fehlern zu beweisen!

Erweiterungen

- z.B. GNY-Logik
- mehr Operatoren und Regeln
- genauere Modellierung möglich
- prinzipielle Schwächen bleiben dennoch! (Semantik)

Fragen???

- bitte jetzt stellen!