Verification using BAN Logic

Software Security

Steffen Helke

Chair of Software Engineering

23rd January 2019

Brandenburgische Technische Universität Cottbus - Senftenberg

Objectives of today's lecture

- Understanding what the general *objectives of a security protocol analysis* are
- Getting to know the basic *syntax* and important *deduction rules* of the *BAN logic*
- Being able to apply the *BAN logic for small examples* and to derive security properties

General Remarks for Verification of Security Protocols

Motivation

➜ How can the correctness of a security protocol be assured?

Reviews & Tests

- Experts analyze protocols informally

  ➜ Drawback: *undetected faults can still be included*, often only incomplete specifications are used

Formal Modeling and Verification

- Analysis based on mathematical methods
- e.g. modeling languages that are defined on a calculus
- Proof of correctness is possible

  ➜ Drawback: *often too much effort*, or specifications with too strong assumptions are used

Objectives of a Security Protocol Analysis

Assumptions

- Secure encryption algorithms will be used
- The secret key can't be guessed
- For a given key k there exists no key k', with $k \neq k'$ such that k' can also used for decryption

Objective 1: Correctness

- Which properties are guaranteed by the protocol?
- Is it possible to reduce assumptions made?

Objective 2: Performance

- Is it possible to omit protocol operations?
- Is unencrypted message communication possible in parts?

Introduction into BAN Logic

BAN Logic

General Remarks

- *Logic of belief* – BAN is a modal logic
- First publication was in 1989
- Inventors are
  - Michael **B**urrows,
  - Martin **A**badi,
  - Rodger **N**eedham

A BAN model specifies ...

- all assumptions of a protocol, and
- the incremental increase in *belief* and *knowledge* by each protocol step

Modal Logic

Remarks

- The word *modal* ... is derived from mode (from Latin)
- A modal logic describes propositions for *several possible worlds*, not only for one real world
- A distinction is made between *possible* and *necessary true* propositions
- Possible propositions are fulfilled in at least one world, but necessary true propositions must be valid in all possible worlds

Example: German Football Championship

- It is possible that this year the FC Bayern München soccer team will be "Deutscher Meister"
- It is necessary for FC Bayern München to win the German championship on the last matchday with a four-point lead

Notation and Deduction Rules of the BAN Logic

Basic Syntax of the BAN Logic

- A **believes** X

  A is entitled to believe X

- S **controls** K

  S is the authority on K and we can trust it

- A **said** X

  A once said X, without indicating whether this statement is new or not

- **fresh**(X)

  X is fresh, i.e. X has never been used before

- A **sees** X

  Someone sent a message X to A in such a way that he can read it

How to model a key?

$A \xleftrightarrow{K} B$

K is a symmetric key for the communication between A and B.

$\xmapsto{K} A$

K is public key of A and the corresponding private key K^{-1} is only known to A

$A \overset{X}{\rightleftharpoons} B$

X is a shared secret of A and B, that can be used for identification, if it communicated in an encrypted manner

How to encrypt messages?

$\{X\}_K$

Message X is encrypted using the key K

$\langle X \rangle_Y$

X is equipped with secret Y

Deduction Rules [1]

- Message Meaning Rules

  - Testing using a public key

$$\frac{P \textbf{ believes } \stackrel{K}{\longmapsto} Q,\ P \textbf{ sees } \{X\}_{K^{-1}}}{P \textbf{ believes } Q \textbf{ said } X}$$

  - Decryption using a symmetric key

$$\frac{P \textbf{ believes } Q \stackrel{K}{\longleftrightarrow} P,\ P \textbf{ sees } \{X\}_{K}}{P \textbf{ believes } Q \textbf{ said } X}$$

  - Rule for shared secrets

$$\frac{P \textbf{ believes } P \stackrel{Y}{\rightleftharpoons} Q,\ P \textbf{ sees } \langle X \rangle_{Y}}{P \textbf{ believes } Q \textbf{ said } X}$$

[1] Note, we use so called *cut rules* to specify the deduction rules

Deduction Rules (2)

- Jurisdiction Rule (Take over someone else's beliefs)

$$\frac{P\ \textbf{believes}\ Q\ \textbf{controls}\ X,\ P\ \textbf{believes}\ Q\ \textbf{believes}\ X}{P\ \textbf{believes}\ X}$$

- Freshness Rule

$$\frac{P\ \textbf{believes}\ \textbf{fresh}\ X}{P\ \textbf{believes}\ \textbf{fresh}\ (X, Y)}$$

- Nonce-Verification Rule

$$\frac{P\ \textbf{believes}\ \textbf{fresh}\ X,\ P\ \textbf{believes}\ Q\ \textbf{said}\ X}{P\ \textbf{believes}\ Q\ \textbf{believes}\ X}$$

Deduction Rules (3)

- Rules for decomposing propositions

$$\frac{P\ \textbf{believes}\ (X, Y)}{P\ \textbf{believes}\ X}$$

$$\frac{P\ \textbf{believes}\ X,\ P\ \textbf{believes}\ Y}{P\ \textbf{believes}\ (X, Y)}$$

$$\frac{P\ \textbf{believes}\ Q\ \textbf{believes}\ (X, Y)}{P\ \textbf{believes}\ Q\ \textbf{believes}\ X}$$

$$\frac{P\ \textbf{believes}\ Q\ \textbf{said}\ (X, Y)}{P\ \textbf{believes}\ Q\ \textbf{said}\ X}$$

Deduction Rules (4)

- Rules for the visibility of messages

$$\frac{P\ \textbf{sees}\ (X, Y)}{P\ \textbf{sees}\ X} \qquad \frac{P\ \textbf{sees}\ \langle X \rangle_Y}{P\ \textbf{sees}\ X}$$

$$\frac{P\ \textbf{believes}\ Q \overset{K}{\longleftrightarrow} P,\ P\ \textbf{sees}\ \{X\}_K}{P\ \textbf{sees}\ X}$$

$$\frac{P\ \textbf{believes} \overset{K}{\longmapsto} P,\ P\ \textbf{sees}\ \{X\}_K}{P\ \textbf{sees}\ X}$$

$$\frac{P\ \textbf{believes} \overset{K}{\longmapsto} Q,\ P\ \textbf{sees}\ \{X\}_{K^{-1}}}{P\ \textbf{sees}\ X}$$

Methodology and Critical Evaluation

Procedure

1. Idealize the protocol and then convert the steps of the idealized version into the BAN notation
2. Define assumptions for the initial state of the protocol
3. Derive new propositions for each protocol step using the given deduction rules

Criticisms

- Proof of correctness does not guarantee absolute security!
- There is a semantic gap between the original protocol and the idealized protocol variant
- Original version of the BAN logic has no semantics

Authentication Targets for the BAN Logic

What exactly is to be proven?

- There has been an intense debate about what propositions are required for successful authentication
- Two types of proposition goals where identified, but it remains unclear which type is more important

1. First-Order Goals

- A **believes** $A \xleftrightarrow{K} B$
- B **believes** $A \xleftrightarrow{K} B$

2. Second-Order Goals

- A **believes** B **believes** $A \xleftrightarrow{K} B$
- B **believes** A **believes** $A \xleftrightarrow{K} B$

Example: Wide Mouth Frog Protocol

- *Wide-Mouth Frog protocol* were proposed by Michael Burrows in 1990
- The protocol name was derived from Burrows nickname he had during his studies

Step 1: Specify an idealized protocol variant

Original Protocol

1. $A \to S : A, \{T_A, K_{AB}, B\}_{K_{AS}}$
2. $S \to B : \{T_S, K_{AB}, A\}_{K_{BS}}$

Idealized Protocol Variant

1. $A \to S : \{T_A, A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{AS}}$
2. $S \to B : \{T_S, A\,\textbf{believes}\,A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{BS}}$

What exactly is to be proven?

$$B\,\textbf{believes}\,A \overset{K}{\longleftrightarrow} B$$

Step 2: Specify necessary assumptions

A1 $A\,\textbf{believes}\,A \overset{K_{AS}}{\longleftrightarrow} S$

A2 $S\,\textbf{believes}\,A \overset{K_{AS}}{\longleftrightarrow} S$

A3 $B\,\textbf{believes}\,B \overset{K_{BS}}{\longleftrightarrow} S$

A4 $S\,\textbf{believes}\,B \overset{K_{BS}}{\longleftrightarrow} S$

A5 $A\,\textbf{believes}\,A \overset{K_{AB}}{\longleftrightarrow} B$

A6 $S\,\textbf{believes}\,\textbf{fresh}\;T_A$

A7 $B\,\textbf{believes}\,\textbf{fresh}\;T_S$

A8 $B\,\textbf{believes}\,(A\,\textbf{controls}\,A \overset{K_{AB}}{\longleftrightarrow} B)$

A9 $B\,\textbf{believes}\,(S\,\textbf{controls}\,(A\,\textbf{believes}\,A \overset{K_{AB}}{\longleftrightarrow} B))$

What are the deduction rules for this proof?

R1 $$\frac{P\ \textbf{believes}\ Q \overset{K}{\longleftrightarrow} P,\ P\ \textbf{sees}\ \{X\}_K}{P\ \textbf{believes}\ Q\ \textbf{said}\ X}$$

R2 $$\frac{P\ \textbf{believes}\ \textbf{fresh}\ X}{P\ \textbf{believes}\ \textbf{fresh}\ (X, Y)}$$

R3 $$\frac{P\ \textbf{believes}\ \textbf{fresh}\ X,\ P\ \textbf{believes}\ Q\ \textbf{said}\ X}{P\ \textbf{believes}\ Q\ \textbf{believes}\ X}$$

R4 $$\frac{P\ \textbf{believes}\ (X, Y)}{P\ \textbf{believes}\ X}$$

R5 $$\frac{P\ \textbf{believes}\ Q\ \textbf{controls}\ X,\ P\ \textbf{believes}\ Q\ \textbf{believes}\ X}{P\ \textbf{believes}\ X}$$

Step 3: Proof for the first protocol step

S **sees** $\{T_A, A \stackrel{K_{AB}}{\longleftrightarrow} B\}_{K_{AS}}$

S **believes** $A \stackrel{K_{AS}}{\longleftrightarrow} S$ (**A1**)

$\Rightarrow$ (with **R1**, message meaning rule)

S **believes** A **said** $(T_A, A \stackrel{K_{AB}}{\longleftrightarrow} B)$

S **believes fresh** T_A (**A6**)

$\Rightarrow$ (with **R3**, freshness nonce verification rule, before apply **R2**)

S **believes** A **believes** $(T_A, A \stackrel{K_{AB}}{\longleftrightarrow} B)$

Step 3: Proof for the second protocol step (1)

$B\ \textbf{sees}\ \{T_S, A\ \textbf{believes}\ A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{BS}}$

$B\ \textbf{believes}\ B \overset{K_{BS}}{\longleftrightarrow} S$ (**A3**)

$\Rightarrow$ (with **R1**, message meaning rule)

$B\ \textbf{believes}\ S\ \textbf{said}\ (T_S, A\ \textbf{believes} \overset{K_{AB}}{\longleftrightarrow} B)$

$B\ \textbf{believes}\ \textbf{fresh}\ T_S$ (**A7**)

$\Rightarrow$ (with **R3**, freshness nonce verification rule, before apply **R2**)

$B\ \textbf{believes}\ S\ \textbf{believes}\ (T_S, A\ \textbf{believes}\ A \overset{K_{AB}}{\longleftrightarrow} B)$

$\Rightarrow$ (with **R4**)

$B\ \textbf{believes}\ S\ \textbf{believes}\ (A\ \textbf{believes}\ A \overset{K_{AB}}{\longleftrightarrow} B)$

Step 3: Proof for the second protocol step (2)

B **believes** S **believes** $(A$ **believes** $A \xleftrightarrow{K_{AB}} B)$

B **believes** S **controls** $(A$ **believes** $A \xleftrightarrow{K_{AB}} B)$ (**A9**)

$\Rightarrow$ (with **R5**)

B **believes** A **believes** $A \xleftrightarrow{K_{AB}} B$

B **believes** A **controls** $A \xleftrightarrow{K_{AB}} B$ (**A8**)

$\Rightarrow$ (with **R5**)

B **believes** $A \xleftrightarrow{K_{AB}} B$

Repetition: Needham-Schroeder Protocol

Symmetric Variant of the Needham-Schroeder Protocol

1. $A \rightarrow S : A, B, N_A$
2. $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$
3. $A \rightarrow B : \{K_{AB}, A\}_{K_{BS}}$
4. $B \rightarrow A : \{N_B\}_{K_{AB}}$
5. $A \rightarrow B : \{N_B - 1\}_{K_{AB}}$

Step 1: Specify an idealized protocol variant

1. $A \rightarrow S : A, B, N_A$

   Plain text messages are not necessary for idealization

2. $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$

   $S \rightarrow A : \{N_A, A \stackrel{K_{AB}}{\longleftrightarrow} B, \textbf{fresh}(A \stackrel{K_{AB}}{\longleftrightarrow} B), \{A \stackrel{K_{AB}}{\longleftrightarrow} B\}_{K_{BS}}\}_{K_{AS}}$

3. $A \rightarrow B : \{K_{AB}, A\}_{K_{BS}}$

   $A \rightarrow B : \{A \stackrel{K_{AB}}{\longleftrightarrow} B\}_{K_{BS}}$

4. $B \rightarrow A : \{N_B\}_{K_{AB}}$

   $B \rightarrow A : \{N_B, A \stackrel{K_{AB}}{\longleftrightarrow} B\}_{K_{AB}}$

5. $A \rightarrow B : \{N_B - 1\}_{K_{AB}}$

   $A \rightarrow B : \{N_B, A \stackrel{K_{AB}}{\longleftrightarrow} B\}_{K_{AB}}$

Step 2: Specify necessary assumptions

A1 A **believes** $A \overset{K_{AS}}{\longleftrightarrow} S$

A2 B **believes** $B \overset{K_{BS}}{\longleftrightarrow} S$

A3 A **believes** S **controls** $A \overset{K_{AB}}{\longleftrightarrow} B$

A4 B **believes** S **controls** $A \overset{K_{AB}}{\longleftrightarrow} B$

A5 A **believes** S **controls fresh** $A \overset{K_{AB}}{\longleftrightarrow} B$

A6 A **believes fresh** N_A

A7 B **believes fresh** N_B

A8 B **believes fresh** $A \overset{K_{AB}}{\longleftrightarrow} B$

➜ Note that the assumption **A8** is too strong (cf. replay attack for the symmetric variant of NSP, slides from 10.1.2018)

What are the deduction rules for this proof?

R1 $$\frac{P\ \textbf{believes}\ Q \overset{K}{\longleftrightarrow} P,\ P\ \textbf{sees}\ \{X\}_K}{P\ \textbf{believes}\ Q\ \textbf{said}\ X}$$

R2 $$\frac{P\ \textbf{believes}\ \textbf{fresh}\ X}{P\ \textbf{believes}\ \textbf{fresh}\ (X, Y)}$$

R3 $$\frac{P\ \textbf{believes}\ \textbf{fresh}\ X,\ P\ \textbf{believes}\ Q\ \textbf{said}\ X}{P\ \textbf{believes}\ Q\ \textbf{believes}\ X}$$

R4 $$\frac{P\ \textbf{believes}\ (X, Y)}{P\ \textbf{believes}\ X}$$

R5 $$\frac{P\ \textbf{believes}\ Q\ \textbf{controls}\ X,\ P\ \textbf{believes}\ Q\ \textbf{believes}\ X}{P\ \textbf{believes}\ X}$$

How to prove the correctness of the symmetric Needham-Schroeder protocol variant?

Step 3: Proof for the second protocol step (1)

$A\,\textbf{sees}\,\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B,\ \textbf{fresh}\,A \overset{K_{AB}}{\longleftrightarrow} B,\ \{A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{BS}}\}_{K_{AS}}$

$A\,\textbf{believes}\,A \overset{K_{AS}}{\longleftrightarrow} S$ (**A1**)

$\Rightarrow$ (with **R1**, message meaning rule)

$A\,\textbf{believes}\,S\,\textbf{said}\,\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B,\ \textbf{fresh}\,A \overset{K_{AB}}{\longleftrightarrow} B,\ \{A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{BS}}\}$

$A\,\textbf{believes}\,\textbf{fresh}\,N_A$ (**A6**)

$\Rightarrow$ (with **R3**, freshness nonce verification rule, before apply **R2**)

$A\,\textbf{believes}\,S\,\textbf{believes}\,\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B,\ \textbf{fresh}\,A \overset{K_{AB}}{\longleftrightarrow} B,\ \{A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{BS}}\}$

Step 3: Proof for the second protocol step (2)

$\Rightarrow$ (decompose with **R4**)

A **believes** S **believes** $A \stackrel{K_{AB}}{\longleftrightarrow} B$

A **believes** S **believes fresh** $A \stackrel{K_{AB}}{\longleftrightarrow} B$

A **believes** S **controls** $A \stackrel{K_{AB}}{\longleftrightarrow} B$ (**A3**)

A **believes** S **controls fresh** $A \stackrel{K_{AB}}{\longleftrightarrow} B$ (**A5**)

$\Rightarrow$ (with **R5**, jurisdiction rule)

A **believes** $A \stackrel{K_{AB}}{\longleftrightarrow} B$

A **believes fresh** $A \stackrel{K_{AB}}{\longleftrightarrow} B$

Step 3: Proof for the third protocol step

B **sees** $\{A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{BS}}$

B **believes** $B \overset{K_{BS}}{\longleftrightarrow} S$ (**A2**)

$\Rightarrow$ (with **R1**, message meaning rule)

B **believes** S **said** $A \overset{K_{AB}}{\longleftrightarrow} B$

B **believes fresh** $A \overset{K_{AB}}{\longleftrightarrow} B$ (**A8**)

$\Rightarrow$ (with **R3**, freshness verification rule)

B **believes** S **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$

B **believes** S **controls** $A \overset{K_{AB}}{\longleftrightarrow} B$ (**A4**)

$\Rightarrow$ (with **R5**, jurisdiction rule)

B **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$

Step 3: Proof for the fourth protocol step

$A\ \textbf{sees}\ \{N_B, A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{AB}}$

$A\ \textbf{believes}\ A \overset{K_{AB}}{\longleftrightarrow} B$ (cf. **proof of the second protocol step**)

$\Rightarrow$ (with **R1**, message meaning rule)

$A\ \textbf{believes}\ B\ \textbf{said}\ \{N_B, A \overset{K_{AB}}{\longleftrightarrow} B\}$

$A\ \textbf{believes}\ \textbf{fresh}\ A \overset{K_{AB}}{\longleftrightarrow} B$ (cf. **proof of the second protocol step**)

$\Rightarrow$ (with **R2**, **R4** and **R3**, freshness verification rule)

$A\ \textbf{believes}\ B\ \textbf{believes}\ A \overset{K_{AB}}{\longleftrightarrow} B$

Step 3: Proof for the fifth protocol step

B **sees** $\{N_B, A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{AB}}$

B **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$ (cf. **proof of the third protocol step**)

$\Rightarrow$ (with **R1**, message meaning rule)

B **believes** A **said** $\{N_B, A \overset{K_{AB}}{\longleftrightarrow} B\}$

B **believes fresh** N_B (**A7**)

$\Rightarrow$ (with **R2**, **R4** and **R3**, freshness verification rule)

B **believes** A **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$

Result of the Verification

1. A **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$ (**derived from the second protocol step**)
2. B **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$ (**derived from the third protocol step**)
3. A **believes** B **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$ (**derived from the fourth protocol step**)
4. B **believes** A **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$ (**derived from the fifth protocol step**)

Annotation Rule

In order to get the first proposition, the annotation rule has to be applied

$$\{X\}$$
$$P \longrightarrow Q : Y$$
$$\{X,\ Q\,\textbf{sees}\,Y\}$$

For reasons of simplicity, we have omitted this rule application in our example

Summary and Conclusions

- BAN logic is a modal logic for analyzing security protocols
- The main source of errors is the idealization step of the real protocol
- Semantics for the BAN logic now exist, but does not solve the problem of idealization
- Various improvements have been proposed for BAN logic
- Very important: BAN logic is decideable
  - $\Rightarrow$ Therefore, the development of practical verification tools is feasible

References

- M. Burrows, M. Abadi, R.M. Needham: A Logic of Authentication. In Proceeding of the Royal Society of London A, volume 426, 1989.
- M. Abadi, M. Tuttle: A Semantics for a Logic of Authentication. In Proceeding of the Symposium on Principles of Distributed Computing, 1991.
- D. Heuzeroth: Formale Methoden zur Analyse von Authentisierungsprotokollen. Universität Karlsruhe, Fakultät Informatik, Seminararbeit 1996.