Modelling and Analysing of Security Protocol: Lecture 5

BAN logic

Tom Chothia
CWI
Introduction

• So far you have learn:
  – the “vocabulary” of protocols and
  – to “look hard at it to see if its right”.

• This is a lot more than most people know!

• But how can we be sure that a protocol is correct?

• This lecture: BAN logic - A formal logic of security protocols.
SecureComm

Lots of state-of-the-art protocol research including:

– “VANET”: Vehicular Ad-hoc NETworks

– “Rural area networks”: Put the routers on bus - hours of delays between messages.

A BitTorrent DoS attack

Target
A BitTorrent DoS attack
A BitTorrent DoS attack
OpenFire

• Open up the network:
  – so that people attack decoy machines,
  – not the real machines.
Kerberos

A protocol for key establishment and authentication used in Windows, MacOS, Apache, OpenSSH, ...

1. \( A \rightarrow S : A,B,N_A \)
2. \( S \rightarrow A : \{K_{AB},B,L,N_A,..\}_{K_{AS}},\{K_{AB},A,L,..\}_{K_{BS}} \)
3. \( A \rightarrow B : \{A,T_A\}_{K_{AB}},\{K_{AB},A,L,..\}_{K_{BS}} \)
4. \( B \rightarrow A : \{T_A+1\}_{K_{AB}} \)
Kerberos Assumption

- A and S share the key $K_{AS}$
- B and S share the key $K_{AS}$
- A trusts S to generate a new key
- B trusts S to generate a new key
- N is a nonce, T is a timestamp and L is an expiration time.
What Do We Mean By Correct?

• “Good Key” and “Key Confirmation”:
  – A believes that $K_{AB}$ is a good key to communicate with B
  
  – B believes that $K_{AB}$ is a good key to communicate with A
  
  – A believes that B believes that $K_{AB}$ is a good key to communicate with A
  
  – A believes that B believes that $K_{AB}$ is a good key to communicate with A
Why “A” Believes in the Key?

A’s belief in the key comes from the message:

2. \( \{K_{AB,B,L,N_A,..}\}_{K_{AS}}, \{K_{AB,A,L,..}\}_{K_{BS}} \)

This line and the assumptions are all “A” needs.
Why “A” Believes in the Key?

Step 1: A sees the message part \( \{K_{AB}, B, L, N_A, ..\}_KAS \)

As the key \( K_{AS} \) is only shared with A and S the part of the message \( (K_{AB}, B, L, N_A) \) must have come from S.

Rule: If A and S share a key K and A sees a message \( \{ M \}_K \) (not from A) then A can conclude that S said “M” at some point.
Why “A” Believes in the Key?

Step 1: A believes that S said \((K_{AB}, B, L, N_A)\) at some point

\(N_A\) is A’s nonce therefore this cannot be an old message therefore A can conclude that S said \((K_{AB}, B, L, N_A)\) as part of the current run of the protocol.

Rule: If A believe that S once said M and M includes a nonce then A can conclude that S currently believes M
Why “A” Believes in the Key?

Step 1: A believes that S currently believes \((K_{AB}, B, L, N_A)\) and in particular \(K_{AB}\) as a key for A and B.

A trusts S to make keys for A and B, therefore A can accept \(K_{AB}\) as a key with B.

Rule: If A trusts S to produce keys and A believes that S believes in a key then A believe in the key.
Verify this Argument

• There are 4 parts to this argument:
  – The assumptions.
  – The protocol messages.
  – The rules.
  – The application of the rules.

• If the check each of these parts you can be sure the whole proof is correct.
Logic

• A “logic” is a formal system of reasoning. They specify rules for knowledge, e.g.

Rule: If you know that “A implies B” and you know “A” then you may conclude “B”

• General Idea: the logic fixes the rules and you or a computer applies them. If the rules lead your goal then you know it’s true.
Logic

Classic Logic uses: and rules like:

- $A \land B$ and
- $A \lor B$ or
- $\neg A$ not
- $A \Rightarrow B$ implies
- $\forall x. A(x)$ For all
- $\exists x. A(x)$ Exist

\[
\begin{align*}
A \land B & \quad \text{and} \\
A \lor B & \quad \text{or} \\
\neg A & \quad \text{not} \\
A \Rightarrow B & \quad \text{implies} \\
\forall x. A(x) & \quad \text{For all} \\
\exists x. A(x) & \quad \text{Exist}
\end{align*}
\]
Proof Trees

- All men are mortal, Plato is a man, therefore Plato is mortal.

∀ x. Man(x) → Mortal(x)

\[
\begin{align*}
\text{Man(Plato)} & \rightarrow \text{Mortal(Plato)} \\
\text{Man(Plato)} & \\
\hline
\text{Mortal(Plato)}
\end{align*}
\]
Logics

• A logic is “sound” if everything you can deduce from the rules is true.

• And “complete” if everything that is true can be deduced.

• There is no sound and complete logic for mathematics ... if there was all mathematicians would be out of a job!
BAN logic

• See paper and JAPE demo
Wide Mouth Frog Protocol

• A light weight key establishment protocol:

1. $A \rightarrow S : A, \{Ta, B, K_{ab}\}_{K_{as}}$
2. $S \rightarrow B : \{Ts, A, K_{ab}\}_{K_{bs}}$

What are the assumption?
Conclusion

• BAN logic give us a formal way to reason about protocols.

• It’s not “sound” or “complete” but it is very effective.

• If you have time to a BAN proof of your protocol. If you don’t think about the rules.