Modelling and Analysing of Security Protocol: Lecture 5

BAN logic

Tom Chothia
CWI

Introduction

• So far you have learned:
  – the "vocabulary" of protocols and
  – to "look hard at it to see if it's 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 Ah-hoc NETworks
– "Rural area networks": Put the routers on bus - hours of delays between messages.

A BitTorrent DoS attack

Target
Tracker

A BitTorrent DoS attack

Target
Tracker
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. $S \rightarrow A : \{K_{AB}, B, L, N_A, \ldots\}_{K_{AS}}\{K_{AB}, A, L, \ldots\}_{K_{BS}}$
3. $A \rightarrow B : \{A, T_A\}_{K_{AB}}\{K_{AB}, A, L, \ldots\}_{K_{BS}}$
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 $K_{BS}$
• 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. $\{K_{AB}, B, L, N_A, \ldots\}_{K_{AS}}\{K_{AB}, A, L, \ldots\}_{K_{BS}}$

This line and the assumptions are all “A” needs.

Why “A” Believes in the Key?

Step 1: A sees the message part $(K_{AB}, B, L, N_A, \ldots)_{K_{AS}}$

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 \(M\)

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

Classic Logic uses: and rules like:

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

Proof Trees

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

\[
\forall x. \text{Man}(x) \Rightarrow \text{Mortal}(x) \\
\text{Man(Plato) \Rightarrow Mortal(Plato)} \\
\text{Man(Plato)} \\
\text{Mortal(Plato)}
\]
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 → S : A, {Ta, B, K_{ab}K_{as}}
2. S → 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.