Multi-Dimensional Analysis of SSL3.0

Zhenxiao Yang & Ali Ebnenasir
Computer Science Department
Michigan State University
December 2002

Outline

- Motivations
- Problem
- Our Approach
  - Temporal-Belief Logic
  - Two-Dimensional Model Checking Using SPIN
- Analysis Approach
- Comparison
- Conclusions and Future work
Motivations

- Why Secure Socket Layer Protocol?
  - A de facto standard for the security of transport layer
  - Results affect a large number of e-commerce users
  - Applicability of formal methods in the analysis of security protocols

- What is Multi-Dimensional Analysis and why?
  - Multiple semantic model to capture different dimensions of a protocol
  - Each formal method has limited expressiveness
  - The semantic model of each formal method filters some details that are not expressible in its language

Problem

- Formal analysis of SSL3.0
- Related work
  - Wagner and Schneier, 1996
    - An informal analysis
    - No analysis for the state of beliefs
    - Experience-based approach
  - Mitchell et al., 1997
    - A finite-state model checker (Murphi)
    - A low-level modeling language for a complex protocol
    - No analysis for the state of beliefs
Problem (continued)

- Related work (continued)
  - Dietrich, 1997
    - A formal analysis using Belief logic
    - The analysis of passive attacks
    - No formal model for the intruder
    - No automatic analysis

- Common shortcoming?
  - Single semantic model

Our Approach

Specification(s) → Properties → Analysis

Model 1 → Model 2 → Model 3

Instantiation
Our Approach (continued)

- Security protocols
  - Distributed programs
  - Inter-Participant communication mechanism: *Message passing*
  - Each action affects the beliefs of the participants

Timeline structure: an interleaving of participants actions

![Timeline diagram]

Temporal-Belief Semantic models

- Temporal-Belief analysis
- Specification: Temporal-Belief Logics
- What do we mean by Belief?
  - A logical language for the internal representation of the beliefs of each participant
  - A formal belief model is pair (\(\Delta_i, R_i\))
    - \(\Delta_i\): a set of observations of participant \(i\)
    - \(R_i\): a relation from a set of observations to a new observation (a.k.a reasoning ability of \(i\)).

Wooldridge & Fisher 94
Belief Model Constraints

- Assumptions:
  - The reasoning ability of a participant does not change over time
  - The beliefs of a participant may change over time

Wooldridge & Fisher 94

Analysis Approach

- One instance, one session
  - Specify the protocol in TBL language
  - Specify an intruder model in TBL
  - Translate the specification into a modeling language (e.g., Promela)
  - Find the flaws and possible attacks using a model checker (e.g., SPIN) as long as your computational resources allow
  - Fix your model by improving the Specification
Example

- An step of a simplified protocol

  ClientHello: \( C \rightarrow S : C, Ver_C, Suite_C \)

  TBL Specification:

  \[
  BC(\text{clientName} = C) \\
  BC(\text{clientVersion} = \text{Ver}_C) \\
  BC(\text{clientSuite} = \text{Suite}_C) \\
  IC(\text{BS}(\text{clientName} = C) \land (\text{clientVersion} = \text{Ver}_C) \land \\
  (\text{clientSuite} = \text{Suite}_C))
  \]

Comparison of TBL and CAPSL

- A sample property:
  - It is always the case that both client and server cannot roll back to version 2.0

\[
(\square \neg ((BC(\text{Ver}_C = 2.0)) \land (BS(\text{Ver}_S = 2.0))))
\]
Conclusions

- Advantages
  - A methodology for inductive analysis of security protocols
  - Our approach have the potential to be automated
  - The expressiveness of TBL with respect to CAPSL

- Disadvantages
  - The more expressive, the more complex (computational and human resources)

Future Work

- Automatic generation of TBL specification from CAPSL specification

- Automatic translation of TBL specification into a modeling language (e.g., Promela)

- Use a model checker (e.g., SPIN) to analyze the protocol
References


Formal Belief Model

A belief model $M$ is a pair $(\Delta, R)$, where

- $\Delta \subseteq \text{Form}(\mathcal{L})$, where Form($\mathcal{L}$) is the set of all formulae in $\mathcal{L}$.

- $R \subseteq ((\text{PowerSet(Form} (\mathcal{L})) \times \text{Form}(\mathcal{L}))$, where $R$ is a finite enumerable binary relation that has the following properties:

  - If $(\Delta_0, \alpha) \in R$ then $\forall \varphi : \varphi \in \Delta_0 : (\Delta_0, \varphi) \in R$ (Reflexivity).
  - If $(\Delta_0, \alpha) \in R$, $(\Delta_1, \beta) \in R$, and $\Delta_0 \subseteq \Delta_1$ then $(\Delta_1, \alpha) \in R$ (Monotonicity).
  - If $(\Delta_0, \alpha) \in R$ and $(\{\alpha\}, \beta) \in R$ then $(\Delta_0, \beta) \in R$ (Transitivity).
Temporal-Belief Logic - Syntax

- Symbols
  
  - Every symbol of $\mathcal{L}_r$, where $\mathcal{L}_r$ is the language of propositional logic.
  
  - A set $\text{Par} = \{P_1, \cdots, P_n\}$ that contains the names of participants.
  
  - The symbols $B$ and $I$.
  
  - The temporal connectives $X$ (i.e., next operator) and $U$ (i.e., until operator).

---

Temporal-Belief Logic – Syntax (Cont’d)

- Formulae
  
  - If $\alpha \in \mathcal{F}_r$ then $\alpha$ is a formula, where $\mathcal{F}_r$ is the set of well-formed formulae in propositional logic.
  
  - If $\alpha$ is a formula and $P_i$ is a participant then $B P_i \alpha$ is also a formula.
  
  - If $\alpha$ is a formula and $P_i$ is a participant then $I P_i \alpha$ is also a formula.
  
  - If $\alpha$ is a formula then $\neg \alpha$, $X \alpha$, and $(\alpha)$ are also formulae.
  
  - If $\alpha$ and $\beta$ are formulae then $\alpha \land \beta$ and $\alpha U \beta$ are also formulae.
Temporal-Belief Logic - Semantics

Temporal operators semantics.

\[ \langle M, x \rangle \models X \alpha \iff \langle M, x + 1 \rangle \models \alpha \]
\[ \langle M, x \rangle \models (\alpha U \beta) \iff \exists y : (y \in N) \land (x \leq y) : \]
\[ (\langle M, x \rangle \models \beta) \land (\forall z : z \in N : (y \leq z < x) \Rightarrow (\langle M, z \rangle \models \alpha) \]

Wooldridge & Fisher 94

Temporal-Belief Logic – Semantics (Cont’d)

The semantics of propositional and belief operators

\[ \langle M, x \rangle \models \text{true} \]
\[ \langle M, x \rangle \models p \iff Val(x, p) = T, \text{ where } p \text{ is an atomic proposition.} \]
\[ \langle M, x \rangle \models \neg \alpha \iff \langle M, x \rangle \not\models \alpha \]
\[ \langle M, x \rangle \models \alpha \land \beta \iff \langle M, x \rangle \models \alpha \text{ and } \langle M, x \rangle \models \beta \]
\[ \langle M, x \rangle \models BP_i \alpha \iff \alpha \in Bel(L(x, P_i), R_i) \]
\[ \langle M, x \rangle \models IP_i \alpha \iff \langle M, x \rangle \models (BP_i(true \land (BP_i \alpha)) \]

Wooldridge & Fisher 94