Overview

- BAN Logic – Burrows, Abadi, and Needham
- GNY – Gong, Needham, Yahalom
- RV
- AT – Abadi and Tuttle
- VO – van Oorschot
- SVO – Syverson and van Oorschot
- Wenbo Mao – “Mao”
- Comparison
- Conclusion

BAN Logic – 1989

- Goal: Offer a formalization of the description and analysis of authentication protocols over distributed computer systems
  - State what is accomplished by the protocol
  - Allow reasoning about, and comparisons of, protocol assumptions
  - Draw attention to unnecessary actions that can be removed from a protocol
  - Highlight any encrypted messages that could be sent in clear text
- Tool: SPEAR
  - Model analyzer for BAN Logic and GNY
  - Developed for security protocols
BAN (cont.)

- Advantages
  - Introduced a simple and powerful notation
  - Logic postulates (ie. Nonce-verification rule) are straightforward to apply for deriving BAN beliefs

- Disadvantages
  - Idealization step can cause analysis problems
  - No formal syntax or semantics
  - Does not account for improper encryption
  - A principal’s beliefs cannot be changed at later stages of the protocol
  - Logic limited to analyze authentication protocols
  - Honesty and trust in other principals is not addressed

Foundation of Each Logic

<table>
<thead>
<tr>
<th></th>
<th>BAN</th>
<th>GNY</th>
<th>GS</th>
<th>AT</th>
<th>VO</th>
<th>XVO</th>
<th>M-tabs</th>
<th>RV</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GNY</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VO</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XVO</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M-tabs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RV</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Read across - States which logic(s) were used to design the new logic
Read down - States which logic(s) extended from the logic
Logics listed in increasing year of publication

GNY - 1990

- Goal: Gain ability to analyze more protocols in a more consistent manner
- Extends and reformulates BAN
  - Notions are expanded
  - New rules and constructs
  - Eliminate some of BAN’s universal assumptions
- Tools:
  - SPEAR
    - Model analyzer for BAN Logic and GNY
    - Developed for security protocols
  - Pattern scanner used as a parser for “not-originated-here” notion
GNY (cont.)
- Advantages
  - Multiple levels of trust can be used in reasoning
  - More protocols can be analyzed
  - Making some BAN assumptions explicit allows for generality
- Disadvantages
  - R6 is unsound
  - Combining rules can result in unsound conclusions
  - The set of rules is incomplete
  - Some rules have redundant premises
  - E.g. I2

RV – 1996
- Goal: Provide a logic of belief, based on BAN for use with a theory generator
- Extension of BAN
  - Explicit interpretation
    - Idealization step
      - Fails to consider other interpretations
      - Hidden assumptions about safety of message
  - Responsibility
    - Account for principal’s irresponsible behavior
- Tool: RVChecker
  - Theory Generator

RV (cont.)
- Advantages
  - Maintains the original simplicity of BAN
  - Has tool support
  - Addresses principal responsibility and the idealization step
- Disadvantages
  - No formal syntax or semantics
  - Unable to specify full range of protocols
AT – 1991

• Goal: Find a natural semantic model for BAN
• Extensions:
  – Provides formal syntax and semantics
  – Simplifies existing BAN inference rules
  – Reformulates inference rules as axioms
  – Removes need for honesty

AT (cont.)

• Advantages
  – Formal syntax and semantics
  – Addresses question of principal honesty
  – More elegant proof system owing to rules of BAN being rewritten as axioms
• Disadvantages
  – No tool support
  – Assumes perfect encryption
  – Does not address idealization step

VO – 1993

• Goal: Extend BAN family of logics in a manner that allows authenticated key agreement protocols to be analyzed, and to better examine goals and beliefs in the protocols.
• Extensions
  – Refine the BAN construct “shares the good crypto key”
  – Define new key confirmation primitive
  – Define new postulates for use with reasoning about “jointly established” keys
VO (cont.)

• Advantages
  – Accomplishes analysis of a new set of protocols
  – Allows for a closer analysis of the goals and beliefs of the new set of protocols

• Disadvantages
  – Time is ignored
  – Message ordering is not addressed

SVO – 1994

• Goal: Unification of BAN, GNY, AT, & VO
• Extensions:
  – Include public keys
  – New functions
  – Message comprehensibility

SVO (cont.)

• Advantages
  – Proved to be sound

• Disadvantages
  – Not suited for tool support
    • SVD revamped SVO: developed to be compatible with Isabelle theorem prover
Mao – 1995

- **Goal:** Formalize the idealization step
- **Extension:**
  - Rule-based idealization technique
  - Remove need for perfect encryption assumption

Mao (cont.)

- **Advantages**
  - Formalization of idealization technique
  - Eliminates assumption of perfect cryptography
- **Disadvantages**
  - No tool support
  - No proof of soundness for idealization rules

Comparison Table Part 1

<table>
<thead>
<tr>
<th>System</th>
<th>Formal Syntax</th>
<th>Formal Semantics</th>
<th>Separation of Semantics and Syntax</th>
<th>Minimize Universal Assumptions</th>
<th>Increase Number of Protocols Analyzed</th>
<th>Adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAN</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>GNY</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>RV</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>AT</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>VO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>SVO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Mao</td>
<td>Formal</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>
Comparison Table Part 2

<table>
<thead>
<tr>
<th>Assumptions</th>
<th>Perfect Cryptography</th>
<th>Idealization</th>
<th>Address honesty</th>
<th>Other Levels of Trust</th>
<th>Tool Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAN</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>GNY</td>
<td>YES</td>
<td>YES</td>
<td>- not originated here</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>RV</td>
<td>YES</td>
<td>YES</td>
<td>- comes up with interpretation rules</td>
<td>YES</td>
<td>NO - done with legit rules</td>
</tr>
<tr>
<td>VA</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES - done with legit rules</td>
<td>YES</td>
</tr>
<tr>
<td>VNV</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES - done with legit rules</td>
<td>NO</td>
</tr>
<tr>
<td>Mao</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

Conclusions

• BAN gave a very good foundation to expand upon
• BAN-like logics do not need to be limited to authentication protocols
• No one logic can or will cover all aspects of protocol analysis
• More tool support is needed

Possible Future Work

• Possible extensions to our work:
  – Include other BAN-like logics
    • Gaarder Snekkenes - GS
    • Sigrid Gurgens – SG
    • Mao and Boyd
    • SVD – An extension of SVO
  – Design and develop tool support
References


Relationships Among Logics