

Formal Verification of Security Protocols

Dr. Ratan Guha
Shahabuddin Muhammad
Zeeshan Furqan

Outline

- Introduction
- Problem
- Contemporary Work
- Our Contributions
 - Application
 - New Approach
- Conclusion and Future Work

Introduction

- Security Protocol
 - Sequence of messages between two or more parties in which encryption is used to provide authentication or to distribute cryptographic keys for new conversations.
 - Ensure the valid and desired working of network
 - Complexity and risk of failure

Problem

- Verification of Security Protocol
 - Complexity
 - Human interaction and expertise
 - Security leakages

Problem (cont.)

- Needham-Schroeder

$$A \rightarrow B : \{N_a \cdot A\}_{K(B)}$$

$$B \rightarrow A : \{N_a \cdot N_b\}_{K(A)}$$

$$A \rightarrow B : \{N_b\}_{K(B)}$$

Problem (cont.)

- Attack on Needham-Schroeder Protocol

$A \rightarrow P : \{N_a \cdot A\}_{K(P)} \quad P \rightarrow B : \{N_a \cdot A\}_{K(B)}$

$B \rightarrow A : \{N_a \cdot N_b\}_{K(A)}$

$A \rightarrow P : \{N_b\}_{K(P)} \quad P \rightarrow B : \{N_b\}_{K(B)}$

Problem (cont.)

- Gavin Lowe: Needham-Schroeder-Lowe (NSL)

$$A \rightarrow B : \{N_a \cdot A\}_{K(B)}$$

$$B \rightarrow A : \{N_a \cdot N_b \cdot \mathbf{B}\}_{K(A)}$$

$$A \rightarrow B : \{N_b\}_{K(B)}$$

Problem (cont.)

- Penetrator
 - Intercept and remember messages
 - Decrypt messages
 - Replay messages
 - Create messages

Contemporary Work

- Dolev-Yao
- Model Based Approaches
- Theorem Provers
- Logic Based Techniques
- Type Checking

Our Contributions

- Application of Existing Model
 - SSM
 - 802.11i
 - Limitations

Our Contributions (cont.)

- A Simplified Logic Based Approach
 - Motivation
 - Proposed Model
 - Guarantees
 - Set of Predicates
 - Inferences
 - Applications

Our Contributions (cont.)

- Model

Basic building blocks of security protocols:

- Communication Messages
- Notion of Subterm
- Freshness Rules
- Cryptographic Algebra
- Message Structure

Conclusion And Future Work

- Importance of Verification
- Complexity
- Our Contributions
- Future Directions

Questions and Comments

Thank You