



# Strand Space Model: Formal Analysis of Security Protocols

Deidre W. Evans

Ratan K. Guha

Zeeshan Furqan

Shahabuddin Muhammad



# Outline

- ◆ Security Protocols
- ◆ Needham-Schroeder (NS) Protocol
- ◆ Security Protocol Verification
- ◆ Strand Space Model
- ◆ Notion of Correctness
- ◆ NSL and SSM
- ◆ Propositions and Lemmas for NSL
- ◆ Proving NSL in SSM
- ◆ Issues in SSM



# Security Protocol

## ◆ Definition

- Sequence of messages between two or more parties in which encryption is used to provide authentication or to distribute cryptographic keys for new conversations.



# Security Properties

- ◆ Secrecy - intruder unable to deduce anything about the legitimate user's activity
- ◆ Authentication of Origin - message that purports to be from a party was indeed originated by that party.
- ◆ Entity Authentication - confident that the claimed identity of an agent with whom one is interacting is correct.
- ◆ Integrity - data can not be corrupted or at least any such corruption will always be detected



# Security Properties

- ◆ Authenticated Key Exchange - enable authenticated communication by setting up key between users.
- ◆ Non-repudiation – protect a participant against cheating by the other
- ◆ Fairness – prevent one participant from gaining an advantage by halting protocol part-way through (e.g. electronic contact signing)
- ◆ Availability – achieve some desired goal



# Security Protocol Vulnerabilities

- ◆ Man-in-the-middle - intruder imposes himself between the communication between two honest users
- ◆ Reflection – bounce messages back to an agent to fool him into revealing correct response to his message
- ◆ Oracle - honest agent is induced to perform some steps of a protocol in a way that helps him to get some data



# Security Protocol Vulnerabilities

- ◆ Replay - intruder monitors partial run of protocol and at some later time replays one or more of the messages to fool honest agent
- ◆ Interleave - intruder contrives for two or more runs of the protocol to overlap (e.g. Needham-Schroeder)
- ◆ Failure of Forward Secrecy – compromised keys and messages are used in future



# Needham-Schroeder (NS) Protocol

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

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

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



# An Attack on NS Protocol

## ◆ Interleaving

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

A thinks he shares secret with P

B thinks he shares secret with A



# An Attack on NS Protocol

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

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

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

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



# Security Protocol Verification

- ◆ “Protocols such as those developed here are prone to extremely subtle errors that are unlikely to be detected in normal operations. The need for techniques to verify the correctness of such protocols is great, and we encourage those interested in such problems to consider this area”<sup>1</sup>

<sup>1</sup>Using Encryption for Authentication in Large Networks of Computers  
by Needham and Schroeder



# Security Protocol Verification

- ◆ Complexity
- ◆ Human interaction and expertise
- ◆ Security leakages



# Current Approaches

- ◆ Dolev-Yao Model – laid foundation by presenting basic intruder model; words follow some rules such as those for a symmetric encryption; intruder's task is to discover secret word(s); protocol security problem becomes a search based on a term-rewrite system; drawback: can only detect protocol deficiencies
- ◆ FDM and InaJo – predicate calculus extension; specify definitions, initial conditions, transforms, axioms, and criteria (specify critical requirements for a secure state); specifications are executed and verified by related tools; successful in locating both active and passive attack flaws since intruder is a separate entity in the model's mathematical
- ◆ NRL Analyzer framework - prototype verification tool that assist in verification of security properties of cryptographic protocols or in detection of security flaws; takes same approach as Dolev and Yao, but treats protocol as a machine for producing words, beliefs, and events; each participant has a set of beliefs which are created and modified as result of receiving messages made up of words, while messages are sent depending upon both beliefs and messages received; events represent state transitions in which new words are generated and beliefs are modified.



# Current Approaches

- ◆ B-method Approach
- ◆ Non-interference Approach
- ◆ Inductive Approach
- ◆ Spi Calculus
- ◆ Provable Security



# Intruder Model

- Intercept and remember messages
- Decrypt messages
- Replay messages
- Create messages
- Kill messages
- Sniff messages
- Reroute messages
- Delay messages
- Fake messages



# Strand Space Model (SSM)

- ◆ Formal way to verify correctness
- ◆ Clear semantics about data freshness
- ◆ Exact causal relation information
- ◆ Explicit model for penetrator
- ◆ Notion of correctness
- ◆ Simple and informative proof



# Strand Space Model

- ◆ Strand
  - Sequence of events that a single principal may engage in
- ◆ Strand Space
  - Set of strands
  - All legitimate executions of protocol plus all the actions of penetrator
- ◆ Bundle
  - Particular execution of a protocol



# Strand Space Model

- ◆ Signed term
  - A pair  $\langle \sigma, a \rangle$ ,  $\sigma \in \{+, -\}$ ,  $a \in A = \{\text{set of terms}\}$
- ◆ Strand Space over  $A$ 
  - A set  $\Sigma$  with trace mapping  $\text{tr}: \Sigma \rightarrow (\pm A)^*$
- ◆ Node
  - A pair  $n = \langle s, i \rangle$ ,  $s \in \Sigma$ ,  $1 \leq i \leq \text{length}(\text{tr}(s))$
  - $\text{index}(n) = i$ ,  $\text{strand}(n) = s$ ,  $\text{term}(n) = (\text{tr}(s))_i$
- ◆ Edge
  - $n_1 \rightarrow n_2$  iff  $\text{term}(n_1) = +a$ ,  $\text{term}(n_2) = -a$ ,  $a \in A$
  - $n_1 \Rightarrow n_2$  if  $n_1 = \langle s, i \rangle$ ,  $n_2 = \langle s, i+1 \rangle$
  - $n' \Rightarrow^+ n$ ,  $n'$  precedes  $n$  on same strand



# Strand Space Model

## ◆ Penetrator strands

- M. text message:  $\langle +t \rangle$ ,  $t \in$  set of terms
- F. flushing:  $\langle -g \rangle$
- T. tee:  $\langle -g, +g, +g \rangle$
- C. concatenation:  $\langle -g, -h, +gh \rangle$
- S. separation:  $\langle -gh, +g, +h \rangle$
- K. key:  $\langle +K \rangle$   $K \in K_p$
- E. encryption:  $\langle -K, -h, +\{h\}_k \rangle$
- D. decryption:  $\langle -K^{-1}, -\{h\}_k, +h \rangle$



# Notion of Correctness

## ◆ Agreement Property

- Each time a participant B completes a run of the protocol as responder using  $x$ , apparently with A, then there is a unique run of the protocol with the principal A as initiator using  $x$ , apparently with B

## ◆ Secrecy

- a value  $x$  is secret in a bundle  $C$  if for every  $n \in C$ ,  $\text{term}(n) \neq x$

# NSL and SSM

Resp[A,B,N<sub>a</sub>,N<sub>b</sub>]

$\langle - \{N_a \cdot A\}_{K(B)} \rangle$  ←



$\langle + \{N_a \cdot N_b \cdot B\}_{K(A)} \rangle$  →



$\langle - \{N_b\}_{K(B)} \rangle$  ←

Init[A,B,N<sub>a</sub>,N<sub>b</sub>]

$\langle + \{N_a \cdot A\}_{K(B)} \rangle$



$\langle - \{N_a \cdot N_b \cdot B\}_{K(A)} \rangle$



$\langle + \{N_b\}_{K(B)} \rangle$



# Propositions and Lemmas for NSL

- ◆ Given a responder strand, bundle  $C$  contains initiator strand of the same height.
- ◆ If  $C$  is a bundle. Then  $\leq_c$  is partial order.
- ◆ Every non-empty subset of the nodes in  $C$  has  $\leq_c$ -minimal members.
- ◆ If  $n$  is a  $\leq_c$ -minimal member of  $S$ , then sign of  $n$  is positive, where  $S$  is subset of set of bundle.
- ◆ If node  $n \in C$  is a  $\leq_c$ -minimal element of  $\{m \in C: t \text{ appears in } \text{term}(n)\}$ , then  $n$  is originating occurrence of  $t$ .



# Proving NSL using SSM

- ◆ Let  $\Sigma$  is NSL space,  $C$  is a bundle in  $\Sigma$  and  $s$  is a responder strand with  $C$ -height 3;
- ◆  $\text{Inv}(K_A)$  is not in  $K_P$
- ◆  $N_A$  is not equal to  $N_B$
- ◆  $N_B$  is uniquely originating
- ◆ Then  $C$  contains an initiator strand with  $C$ -height 3.

# Proving NSL using SSM

Resp[A,B,N<sub>a</sub>,N<sub>b</sub>]

$\langle - \{N_a \cdot A\}_{K(B)} \rangle$



$\langle + \{N_a \cdot N_b \cdot B\}_{K(A)} \rangle \quad (n_0)$



$n_2 \dots N_b \dots \rightarrow$

$\langle - \{N_b\}_{K(B)} \rangle \quad (n_3)$



# Proving NSL using SSM

## ◆ Lemmas

- $N_b$  originates at  $n_0$ .
- $n_2$  is regular and the sign of  $n_2$  is positive.
- A node  $n_1$  precedes  $n_2$  and  $\text{term}(n_1) = \{N_a \cdot N_b \cdot B\}_{K(A)}$
- The regular strand containing  $n_1$  and  $n_2$  is an initiator strand and is contained in  $C$ .
- If  $N_a$  is uniquely originating in  $\Sigma$ , there is at most one strand  $t \in \text{Init}[A, B, N_a \cdot N_b]$



# Issues in SSM

- ◆ In ideal cryptosystem, free-algebra assumption is not true, i.e.
  - $\{m\}_k = \{m'\}_k$ , does not necessarily mean that  $m=m'$  and  $k=k'$
- ◆ SSM can not handle such penetrators with power to cryptanalyze old session keys and hence benefit from some kind of replay attacks.
- ◆ We can incorporate more stringent notion of secrecy, e.g. information flow security properties into the protocols.

