Secure Protocol Composition

Anupam Datta          Ante Derek
John C. Mitchell      Dusko Pavlovic
Stanford University   Kestrel Institute
FMSE Oct 30, 2003
Motivation

- Divide-and-Conquer paradigm in security
  - IKE:
    - Phase 1: 4 sub-protocols
    - Phase 2: 2 sub-protocols
  - ISO-9798-3:
    - Secrecy
    - Authentication
Contribution

- Protocol Composition:
  - A formal logic for proving properties of security protocols from their parts
  - General composition operation, subsuming sequential and parallel composition

- Examples:
  - ISO-9798-3, NSL
  - NSL | ISO
Central Issues

- **Non-destructive Combination:**
  - Ensure that the combined parts do not degrade each other’s security
  - Assumptions about the environment
    - In logic: invariance assertions

- **Additive Combination:**
  - Accumulate security properties of combined parts, assuming they do not interfere
  - Properties achieved by individual protocol roles
    - In logic: before-after formalism
Roadmap

- Motivating Example
- Compositional Logic
- Big Picture: Protocol Derivation
- Related Work
- Conclusions
Example

Authenticated Key Agreement Problem:

Construct protocol with properties:

- Shared secret
- Authentication
Component 1

- **Diffie-Hellman**
  
  \[ \begin{align*}
  A & \rightarrow B: \quad g^a \\
  B & \rightarrow A: \quad g^b
  \end{align*} \]

- **Shared secret (with someone)**
  
  - A deduces:
    
    \[ \text{Knows}(Y, g^{ab}) \Rightarrow (Y = A) \lor \text{Knows}(Y,b) \]

- **Authentication**
Component 2

- Challenge Response:
  
  \[\begin{align*}
  &A \rightarrow B: \ m, \ A \\
  &B \rightarrow A: \ n, \ sig_B \{m, n, A\} \\
  &A \rightarrow B: \ sig_A \{m, n, B\}
  \end{align*}\]

- Shared secret (with someone)

- Authentication
  
  - A deduces: Received (B, msg1) \land Sent (B, msg2)
Composition

- ISO 9798-3 protocol:
  - $A \rightarrow B$: $g^a, A$
  - $B \rightarrow A$: $g^b, \text{sig}_B \{g^a, g^b, A\}$
  - $A \rightarrow B$: $\text{sig}_A \{g^a, g^b, B\}$

- Shared secret: $g^{ab}$
- Authentication
Roadmap

- Motivating example
- Compositional Logic
- Big Picture: Protocol Derivation
- Related Work
- Conclusions
Protocol Logic: Main idea

- Alice’s information
  - Protocol
  - Private data
  - Sends and receives

Honest Principals, Attacker

Send

Receive

Private Data

Protocol
Example: Challenge-Response

- Alice reasons: if Bob is honest, then:
  - only Bob can generate his signature. [protocol independent]
  - if Bob generates a signature of the form $\text{sig}_B \{m, n, A\}$,
    - he sends it as part of msg 2 of the protocol and
    - he must have received msg1 from Alice. [protocol specific]
- Alice deduces: Received $(B, \text{msg1}) \land \text{Sent} (B, \text{msg2})$
**Execution Model**

- **Protocol**
  - “Program” for each protocol role

- **Initial configuration**
  - Set of principals and key
  - Assignment of $\geq 1$ role to each principal

- **Run**
  
  \[ \nu X \langle \{X\}_B \rangle \]
  
  \[ \langle \{X\}_B \rangle \]
  
  \[ \langle \{Z\}_B \rangle \]

  "Position in run"
Formulas true at a position in run

- **Action formulas**
  \[ a ::= \text{Send}(P,m) \mid \text{Receive} (P,m) \mid \text{New}(P,t) \mid \text{Decrypt} (P,t) \mid \text{Verify} (P,t) \]

- **Formulas**
  \[ \varphi ::= a \mid \text{Has}(P,t) \mid \text{Fresh}(P,t) \mid \text{Honest}(N) \mid \text{Contains}(t_1, t_2) \mid \neg \varphi \mid \varphi_1 \land \varphi_2 \mid \exists x \varphi \mid \circ \varphi \mid \lozenge \varphi \]

- **Example**
  \[ \text{After}(a,b) = \lozenge(b \land \circ \lozenge a) \]
Modal Formulas

- After actions, postcondition
  \[ [\text{actions}]_P \varphi \quad \text{where} \ P = \langle \text{princ}, \text{role id} \rangle \]

- Before/after assertions
  \( \varphi \ [\text{actions}]_P \psi \)

- Composition rule
  \[ \varphi [S]_P \psi \quad \psi [T]_P \theta \quad \frac{\varphi [ST]_P \theta}{Note: \ same \ P \ in \ all \ formulas} \]
Diffie-Hellman: Property

- **Formula**
  - $[\text{new } a ]_A \text{Fresh}(A, g^a)$

- **Explanation**
  - Modal form: $[\text{actions }]_P \varphi$
  - Actions: $[\text{new } a ]_A$
  - Postcondition: $\text{Fresh}(A, g^a)$
Challenge Response: Property

- Modal form: $\varphi \ [ \text{actions} ]_P \psi$
  - precondition: $\text{Fresh}(A,m)$
  - actions: $[ \text{Initiator role actions} ]_A$
  - postcondition:
    $\text{Honest}(B) \implies \text{ActionsInOrder}(\text{send}(A, \{A,B,m\}),\text{receive}(B, \{A,B,m\}),\text{send}(B, \{B,A,\{n, \text{sig}_B \{m, n, A\}\}\}),\text{receive}(A, \{B,A,\{n, \text{sig}_B \{m, n, A\}\}\}))$
Composition: DH+CR = ISO-9798-3

- DH postcondition matches CR precondition
- Combination:
  - Substitute $g^a$ for $m$ in CR to obtain ISO.
  - Apply composition rule, persistence.
  - ISO initiator role inherits CR authentication.
- DH secrecy is also preserved
  - Proved using another application of composition rule.

Additive Combination
Critical issues

- Reasoning about honest principals
  - Invariance rule, called "honesty rule"
- Preservation of invariants under composition
  - If we prove Honest(X) ⊨ φ for protocol 1 and compose with protocol 2, is formula still true?
Honesty Rule

- **Definition**
  - A basic sequence of actions begins with receive, ends before next receive

- **Rule**
  
  \[
  \begin{align*}
  \text{[ } \varphi \text{ ]}_X \\
  \forall B \in \text{BasicSeq}(Q). \varphi [B]_X \varphi \\
  Q \gg \text{Honest}(X) \Rightarrow \varphi
  \end{align*}
  \]

- **Example**
  
  \[
  \text{CR \gg Honest}(X) \Rightarrow \\
  (\text{Sent}(X, m_2) \Rightarrow \text{Recd}(X, m_1))
  \]
Combining protocols

$\Gamma \vdash$ Honest($X$) $\supset \ldots$

$\Gamma \mid \rightarrow$ Secrecy

$\Gamma \cup \Gamma' \mid \rightarrow$ Secrecy

$\Gamma' \vdash$ Honest($X$) $\supset \ldots$

$\Gamma' \mid \rightarrow$ Authentication

$\Gamma \cup \Gamma' \mid \rightarrow$ Authentication

$\exists \cup \Gamma' \mid \rightarrow$ Secrecy $\land$ Authentication [additive]

DH $\bullet$ CR $\triangleright\triangleright \Gamma \cup \Gamma'$ [nondestructive]

ISO $\triangleright$ Secrecy $\land$ Authentication
Composition Rules

- Invariant weakening rule
  \[ \Gamma |- \varphi [\ldots]_p \psi \]
  \[ \Gamma \cup \Gamma' |- \varphi [\ldots]_p \psi \]

- Sequential Composition
  \[ \Gamma |- \varphi [S]_p \psi \]
  \[ \Gamma |- \psi [T]_p \theta \]
  \[ \Gamma |- \varphi [ST]_p \theta \]

- Prove invariants from protocol
  \[ Q \triangleright \Gamma \quad Q' \triangleright \Gamma \]
  \[ Q \cdot Q' \triangleright \Gamma \]
Roadmap

- Motivating example
- Compositional Logic
- **Big Picture: Protocol Derivation**
- Related Work
- Conclusions
Derivation Framework

- Protocols are constructed from:
  - components

  by applying a series of:
  - composition, refinement and transformation operations.

- Properties accumulate as a derivation proceeds.

- Examples in previous paper [DDMP; CSFW03]:
  - STS, ISO-9798-3, JFKi, JFKr, IKE
Roadmap

- Motivating example
- Compositional Logic
- Big Picture: Protocol Derivation
- Related Work
- Conclusions
Previous Work

- **Formal Model:**
  - Disjoint Encryption [THG99]
  - Environmental Requirements [CMS03]

- **Computational Model:**
  - Probabilistic Polytime Process Calculus [LMMS98]
  - Probabilistic Polytime I/O Automata [PW01]
  - Probabilistic Polytime TM’s: UC [C01]
Roadmap

- Motivating example
- Compositional Logic
- Big Picture: Protocol Derivation
- Related Work
- Conclusions
Conclusions

- Successfully extended protocol logic to compositional reasoning

- **Central Issues:**
  - Additive combination *before-after assertions*
  - Nondestructive combination *invariants*

- **Examples:**
  - ISO = DH; CR
  - NSL = NSL(init); NSL(KE)
  - NSL | ISO

- Part of bigger program on protocol derivation
Questions?