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

  $$A \rightarrow B: \quad g^a$$
  $$B \rightarrow A: \quad g^b$$

  - Shared secret (with someone)
    - A deduces:

      $$Knows(Y, g^{ab}) \supset (Y = A) \vee Knows(Y,b)$$
  - Authentication

Component 2

- Challenge Response:

$$A \rightarrow B: \; m, A$$
$$B \rightarrow A: \; n, sig_B\{m, n, A\}$$
$$A \rightarrow B: \; sig_A\{m, n, B\}$$

  - Shared secret (with someone)
  - Authentication
    - A deduces: Received (B, msg1) $\wedge$ Sent (B, msg2)

Composition

$m := g^a$

$n := g^b$

- ISO 9798-3 protocol:

$$A \rightarrow B: \; g^a, A$$

$$B \rightarrow A: \; g^b, \text{sig}_B\{g^a, g^b, A\}$$

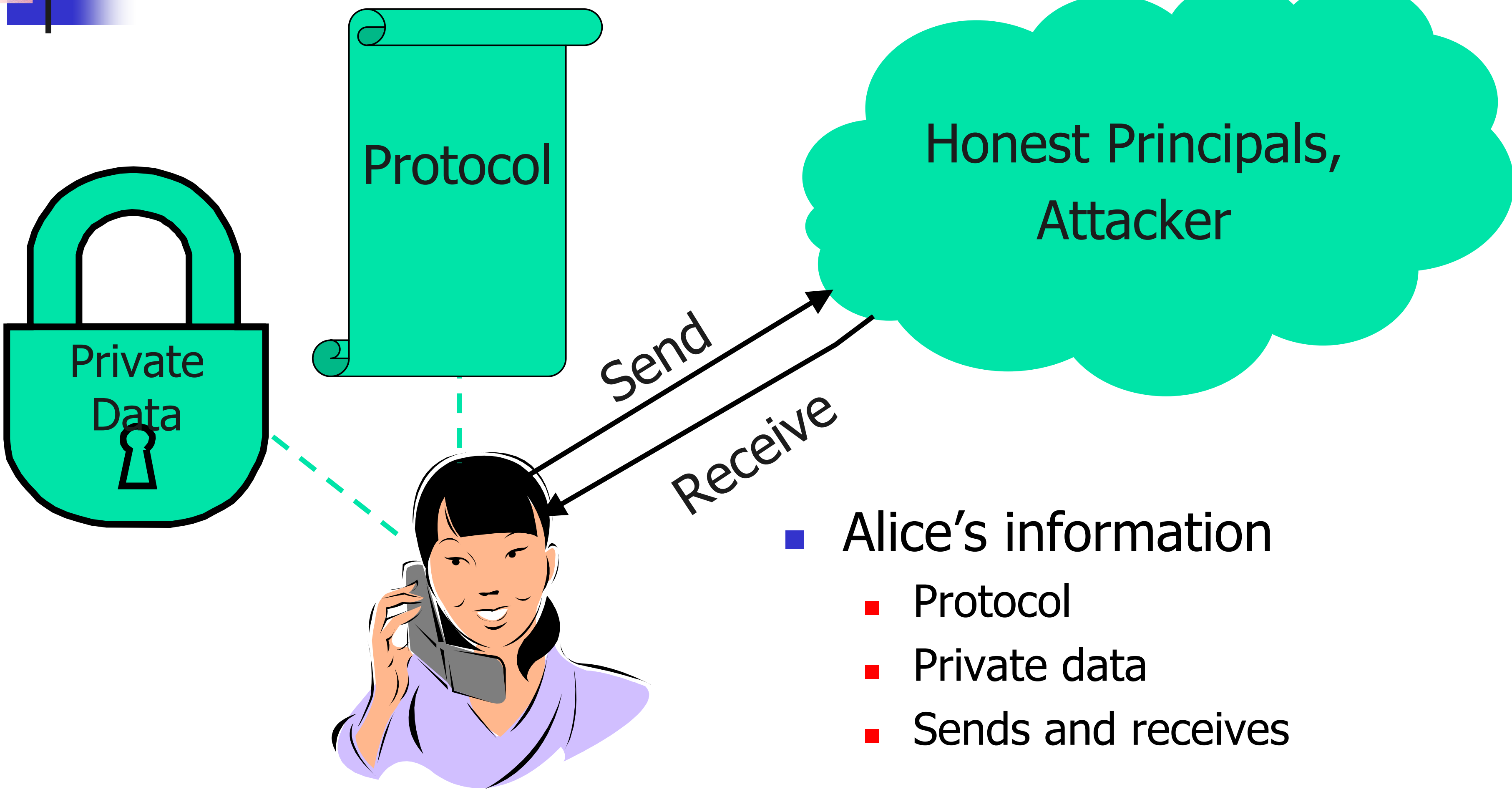
$$A \rightarrow B: \; \text{sig}_A\{g^a, g^b, B\}$$

  - Shared secret: g^{ab}
  - Authentication

Roadmap

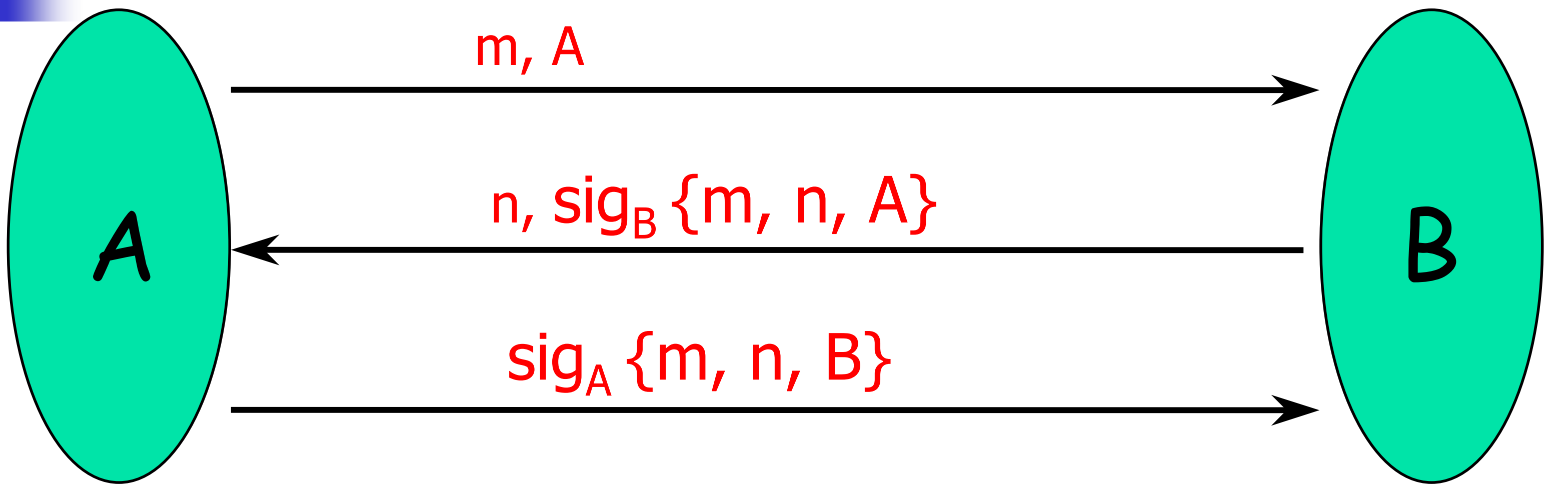
- Motivating example
- Compositional Logic
- Big Picture: Protocol Derivation
- Related Work
- Conclusions

Protocol Logic: Main idea



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

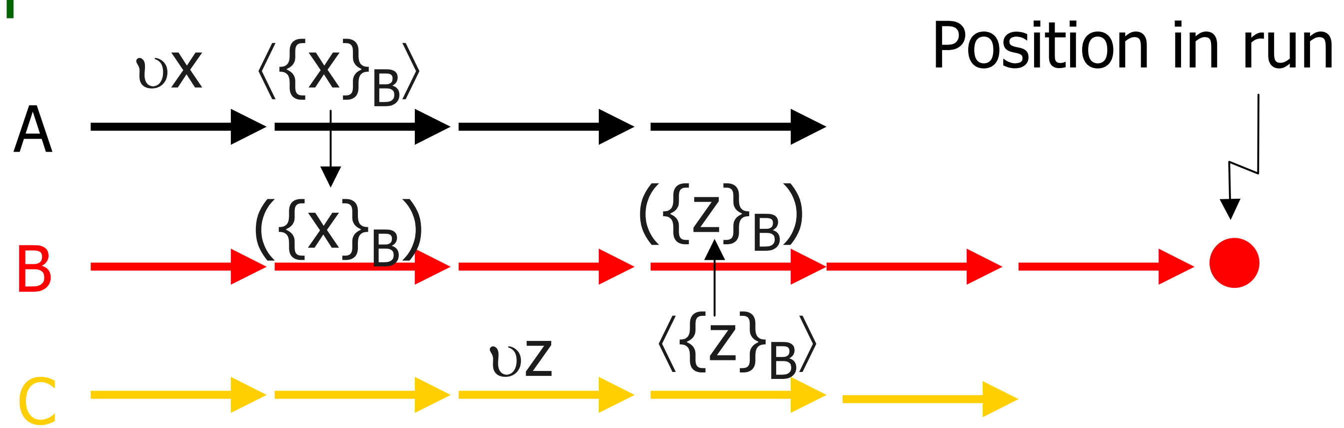
Example: Challenge-Response



- Alice reasons: if Bob is honest, then:
  - only Bob can generate his signature. [protocol independent]
  - if Bob generates a signature of the form 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, msg1) $\wedge$ Sent (B, msg2)

Execution Model

- Protocol
  - "Program" for each protocol role
- Initial configuration
  - Set of principals and key
  - Assignment of ≥1 role to each principal
- Run



Formulas true at a position in run

- Action formulas

  a ::= Send(P,m) | Receive (P,m) | New(P,t)

  | Decrypt (P,t) | Verify (P,t)

- Formulas

  φ ::= a | Has(P,t) | Fresh(P,t) | Honest(N)

  | Contains(t_1, t_2) | $\neg\varphi$ | $\varphi_1 \wedge \varphi_2$ | $\exists x\ \varphi$

  | $\mathrm{o}\varphi$ | $\Diamond\varphi$

- Example

  After(a,b) = $\Diamond(b \wedge \mathrm{o}\Diamond a)$

Modal Formulas

- After actions, postcondition

  $[\text{ actions }]_P\ \varphi$ where P = ⟨princ, role id⟩

- Before/after assertions

  $\varphi\ [\text{ actions }]_P\ \psi$

- Composition rule

$$\frac{\varphi\,[\,S\,]_P\,\psi \qquad \psi\,[\,T\,]_P\,\theta}{\varphi\,[\,ST\,]_P\,\theta}$$

Note: same P *in all formulas*

Diffie-Hellman: Property

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

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

Challenge Response: Property

- Modal form: φ [actions]$_P$ ψ
  - precondition: Fresh(A,m)
  - actions: [Initiator role actions]$_A$
  - postcondition:

    Honest(B) $\supset$ ActionsInOrder(
    send(A, {A,B,m}),
    receive(B, {A,B,m}),
    send(B, {B,A,{n, sig$_B$ {m, n, A}}}),
    receive(A, {B,A,{n, 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) $\supset \varphi$ 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

$$\frac{[\ ]_X\ \varphi \qquad \text{For all } B \in \text{BasicSeq}(Q).\ \varphi\ [B]_X\ \varphi}{Q \blacktriangleright \text{Honest}(X) \supset \varphi}$$

- Example

$$CR \blacktriangleright \text{Honest}(X) \supset (\text{Sent}(X, m_2) \supset \text{Recd}(X, m_1))$$

Combining protocols

$\overbrace{}^{\Gamma}$ $\overbrace{}^{\Gamma'}$

DH ▶ Honest(X) $\supset$ … CR ▶ Honest(X) $\supset$ …

Γ |- Secrecy Γ' |- Authentication

$\Gamma \cup \Gamma'$ |- Secrecy $\Gamma \cup \Gamma'$ |- Authentication

$\Gamma \cup \Gamma'$ |- Secrecy $\wedge$ Authentication [additive]

DH • CR ▶ $\Gamma \cup \Gamma'$ [nondestructive]

=

ISO ▶ Secrecy $\wedge$ Authentication

Composition Rules

- Invariant weakening rule

$$\frac{\Gamma \mid\!\text{-}\ \varphi\,[\ldots]_P\,\psi}{\Gamma \cup \Gamma' \mid\!\text{-}\ \varphi\,[\ldots]_P\,\psi}$$

- Sequential Composition

$$\frac{\Gamma \mid\!\text{-}\ \varphi\,[\,S\,]_P\,\psi \qquad \Gamma \mid\!\text{-}\ \psi\,[\,T\,]_P\,\theta}{\Gamma \mid\!\text{-}\ \varphi\,[\,ST\,]_P\,\theta}$$

- Prove invariants from protocol

$$\frac{Q \blacktriangleright \Gamma \qquad Q' \blacktriangleright \Gamma}{Q \bullet Q' \blacktriangleright \Gamma}$$

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?