Goal-Preserving Transformations

Joshua D. Guttman

Worcester Polytechnic Institute

Protocol Exchange
7 Oct 2009

Preserving Goals

- $\Pi_2 = F(\Pi_1)$: Π_2 results by transformation F from Π_1

Preserving Goals

- $\Pi_2 = F(\Pi_1)$: Π_2 results by transformation F from Π_1
  - Inclusive, low-syntax relation

Preserving Goals

- $\Pi_2 = F(\Pi_1)$: Π_2 results by transformation F from Π_1
  - Inclusive, low-syntax relation
  - Homomorphisms among skeletons match up

Preserving Goals

- $\Pi_2 = F(\Pi_1)$: Π_2 results by transformation F from Π_1
  - Inclusive, low-syntax relation
  - Homomorphisms among skeletons match up
  - Need additional constraints to ensure goals of Π_1 preserved

Preserving Goals

- $\Pi_2 = F(\Pi_1)$: Π_2 results by transformation F from Π_1
  - Inclusive, low-syntax relation
  - Homomorphisms among skeletons match up
  - Need additional constraints to ensure goals of Π_1 preserved
- Need: authentication tests preserved;
  no new solutions to old tests

Preserving Goals

- $\Pi_2 = F(\Pi_1)$: Π_2 results by transformation F from Π_1
  - Inclusive, low-syntax relation
  - Homomorphisms among skeletons match up
  - Need additional constraints to ensure goals of Π_1 preserved
- Need: authentication tests preserved;
  no new solutions to old tests
- Consequence: $H\colon F(\mathbb{A}) \mapsto \mathbb{B}$ realized implies
  - $J\colon \mathbb{A} \mapsto \mathbb{A}_1$ splits into $L \circ K$
  - $K\colon \mathbb{A} \mapsto \mathbb{A}_0$ realized
  - where: $\mathbb{A}_1$ is maximal s.t. $F(\mathbb{A}_1) \mapsto \mathbb{B}$

Protocol Transformation $F\colon \Pi_1 \longrightarrow \Pi_2$

F determines maps:

- Π_1 skeletons $\longrightarrow$ Π_2 skeletons
- $\mathcal{L}(\Pi_1) \longrightarrow \mathcal{L}(\Pi_2)$

When does F preserve $\mathcal{L}(\Pi_1)$-goals $\quad \forall \vec{x} \,.\, (\phi_0 \supset \exists \vec{y} \,.\, \bigvee_{1 \leq i \leq j} \phi_i)$?

$$\begin{array}{c} \mathrm{cs}(\phi_0) \\ {\scriptstyle F}\big\downarrow \\ \mathrm{cs}(F(\phi_0)) \end{array}$$

Protocol Transformation $F\colon \Pi_1 \to \Pi_2$

F determines maps:

- Π_1 skeletons $\to$ Π_2 skeletons
- $\mathcal{L}(\Pi_1) \to \mathcal{L}(\Pi_2)$

When does F preserve $\mathcal{L}(\Pi_1)$-goals $\quad \forall \vec{x} \,.\, (\phi_0 \supset \exists \vec{y} \,.\, \bigvee_{1 \le i \le j} \phi_i)$?

$$
\begin{tikzcd}
\mathrm{cs}(\phi_0) \arrow[d, "F"'] & \\
\mathrm{cs}(F(\phi_0)) \arrow[r, bend right, mapsto] & \mathbb{B}_{\mathrm{real}}
\end{tikzcd}
$$

Protocol Transformation $F\colon \Pi_1 \to \Pi_2$

F determines maps:

- Π_1 skeletons $\to$ Π_2 skeletons
- $\mathcal{L}(\Pi_1) \to \mathcal{L}(\Pi_2)$

When does F preserve $\mathcal{L}(\Pi_1)$-goals $\quad \forall \vec{x} \,.\, (\phi_0 \supset \exists \vec{y} \,.\, \bigvee_{1 \le i \le j} \phi_i)$?

$$
\begin{tikzcd}
\mathrm{cs}(\phi_0) \arrow[d, "F"'] & & \\
\mathrm{cs}(F(\phi_0)) \arrow[r, mapsto] \arrow[rr, mapsto, bend right] & F(\mathbb{A}_1) \arrow[r, mapsto] & \mathbb{B}_{\mathrm{real}}
\end{tikzcd}
$$

Protocol Transformation $F \colon \Pi_1 \to \Pi_2$

F determines maps:

- Π_1 skeletons $\to$ Π_2 skeletons
- $\mathcal{L}(\Pi_1) \to \mathcal{L}(\Pi_2)$

When does F preserve $\mathcal{L}(\Pi_1)$-goals $\quad \forall \vec{x} \,.\, (\phi_0 \supset \exists \vec{y} \,.\, \bigvee_{1 \le i \le j} \phi_i)$?

$$
\begin{tikzcd}
\mathrm{cs}(\phi_0) \arrow[r, mapsto, bend left] \arrow[d, "F"'] & \mathbb{A}_1 \arrow[d, "F"] & \\
\mathrm{cs}(F(\phi_0)) \arrow[r, mapsto] \arrow[rr, mapsto, bend right] & F(\mathbb{A}_1) \arrow[r, mapsto] & \mathbb{B}_{\mathrm{real}}
\end{tikzcd}
$$

Protocol Transformation $F\colon \Pi_1 \rightarrow \Pi_2$

F determines maps:

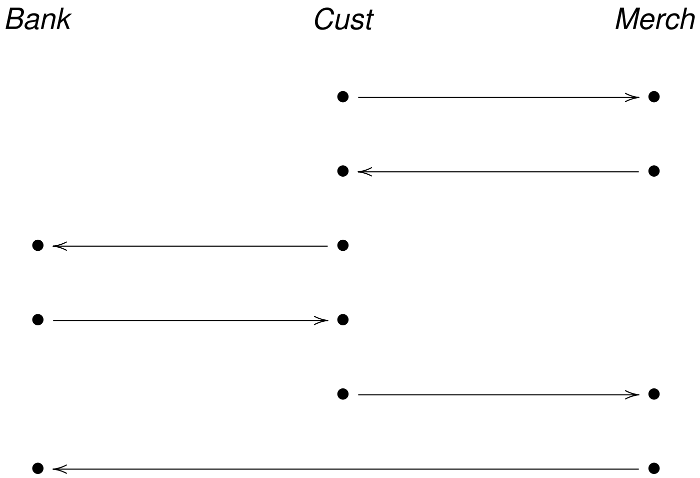
- Π_1 skeletons $\rightarrow$ Π_2 skeletons
- $\mathcal{L}(\Pi_1) \rightarrow \mathcal{L}(\Pi_2)$

When does F preserve $\mathcal{L}(\Pi_1)$-goals $\quad \forall \vec{x} \,.\, (\phi_0 \supset \exists \vec{y} \,.\, \bigvee_{1 \leq i \leq j} \phi_i)$?

$$
\begin{tikzcd}
\mathrm{cs}(\phi_0) \arrow[r, mapsto, "?"'] \arrow[rr, mapsto, bend left] \arrow[d, "F"'] & \color{red}{\mathbb{A}_{\mathrm{real}}} \arrow[r, mapsto, "?"'] & \mathbb{A}_1 \arrow[d, "F"] & \\
\mathrm{cs}(F(\phi_0)) \arrow[rr, mapsto] \arrow[rrr, mapsto, bend right] & & F(\mathbb{A}_1) \arrow[r, mapsto] & \mathbb{B}_{\mathrm{real}}
\end{tikzcd}
$$

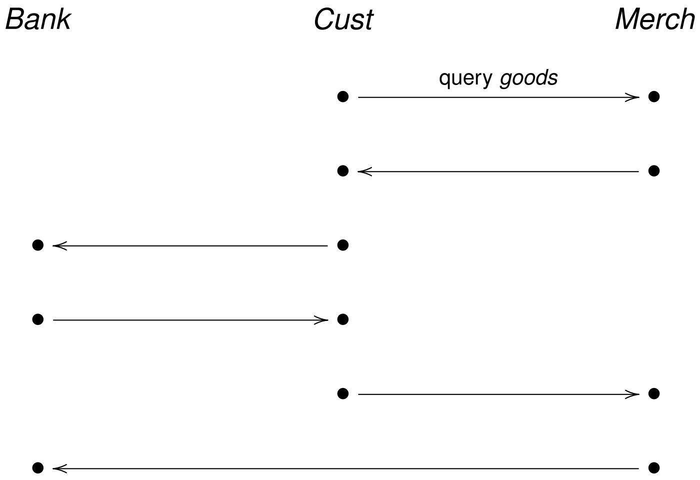
Electronic Purchase

Using a money order: *EPMO*



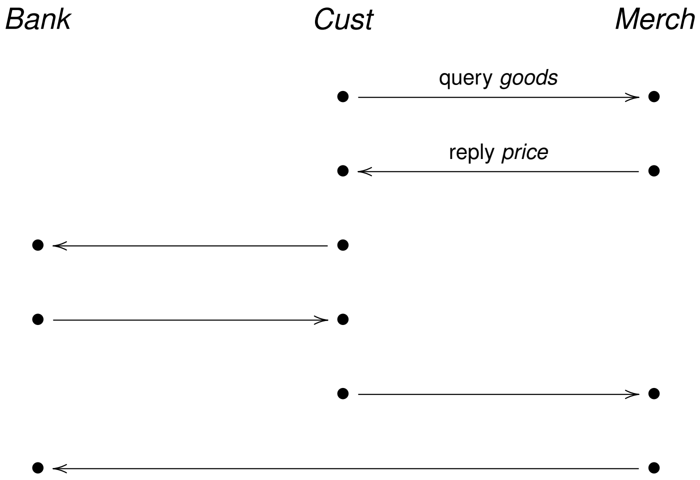
Electronic Purchase

Using a money order: *EPMO*



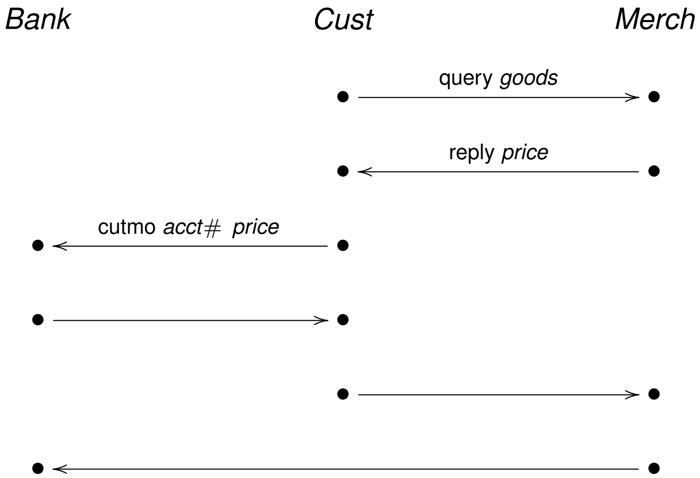
Electronic Purchase

Using a money order: *EPMO*



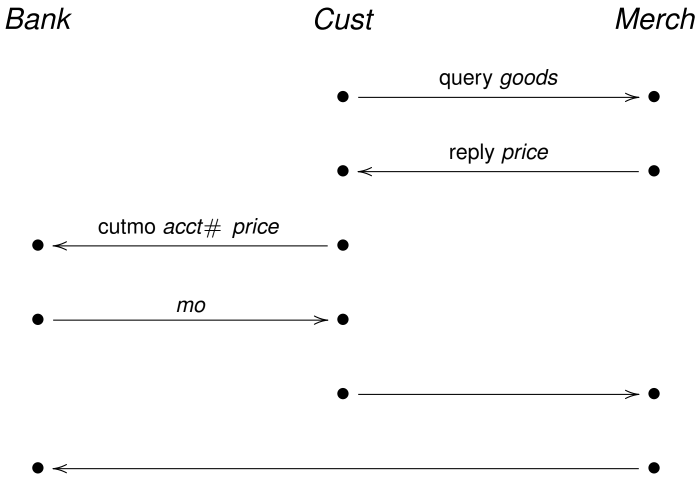
Electronic Purchase

Using a money order: *EPMO*



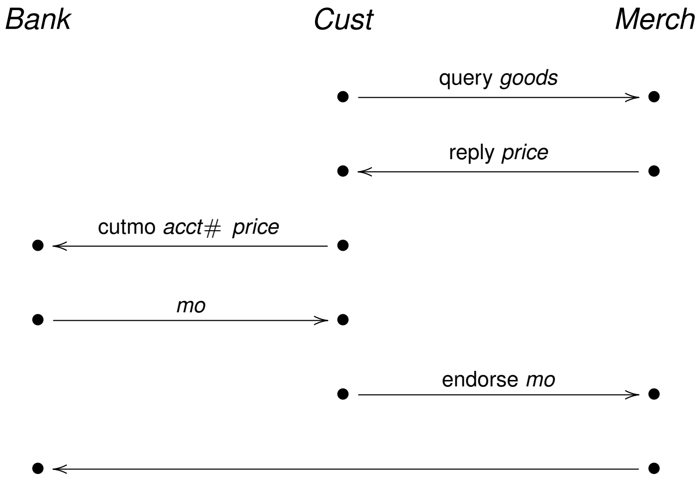
Electronic Purchase

Using a money order: *EPMO*



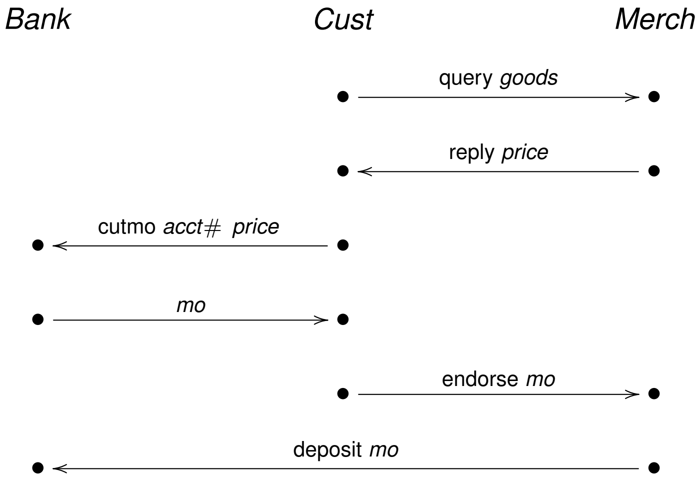
Electronic Purchase

Using a money order: *EPMO*



Electronic Purchase

Using a money order: *EPMO*



EPMO

$\{\!|\, - \,|\!\}_P$ means encr. with P's public key

$[\![-]\!]_P$ means digital signature

$$mo = [\![\, hash(C,\ N_c,\ N_b,\ N_m,\ price)\,]\!]_B$$

Bank — *Cust* — *Merch*

$Cust \xrightarrow{\{\!|\, C,\ N_c,\ goods \,|\!\}_M} Merch$

$Cust \xleftarrow{\{\!|\, N_c,\ N_m,\ M,\ price \,|\!\}_C} Merch$

$Bank \xleftarrow{\{\!|\, C,\ N_c,\ N_m,\ acct\#,\ price \,|\!\}_B} Cust$

$Bank \xrightarrow{mo,\ \{\!|\, N_c,\ N_b \,|\!\}_C} Cust$

$Cust \xrightarrow{mo,\ N_b} Merch$

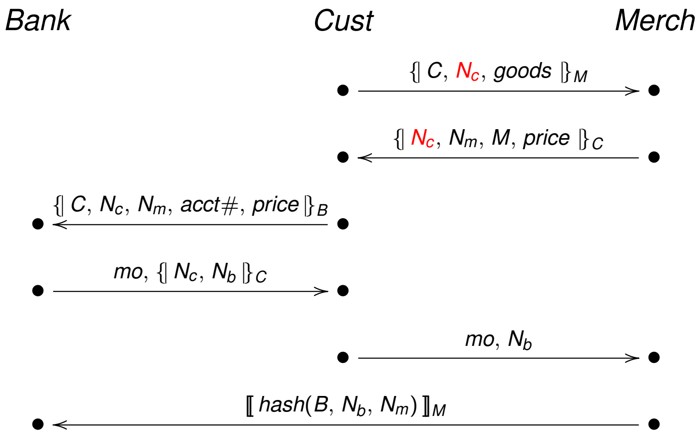
$Bank \xleftarrow{[\![\, hash(B,\ N_b,\ N_m)\,]\!]_M} Merch$

Customer / Merchant Agreement

$\{\!| - |\!\}_P$ means encr. with P's public key

$[\![-]\!]_P$ means digital signature

$$mo = [\![\, hash(C,\ N_c,\ N_b,\ N_m,\ price) \,]\!]_B$$

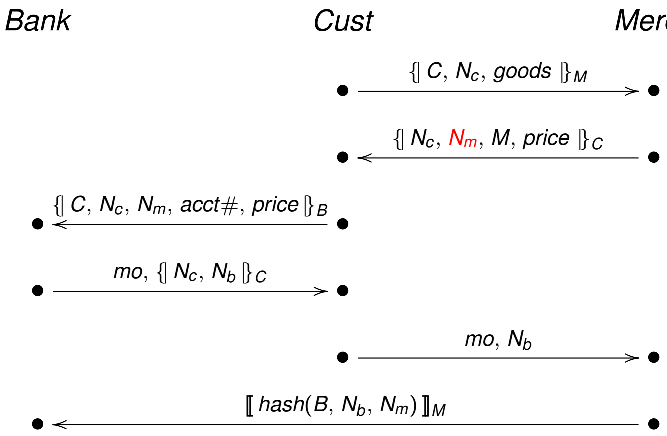


Merchant / Customer Agreement

$\{\!|\ -\ |\!\}_P$ means encr. with P's public key

$[\![\ -\ ]\!]_P$ means digital signature

$$mo = [\![\ hash(C,\ N_c,\ N_b,\ N_m,\ price)\ ]\!]_B$$

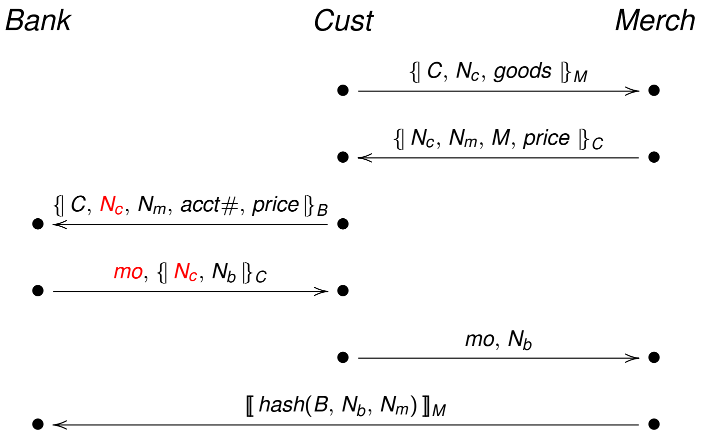


Customer / Bank Agreement

$\{\!|\ -\ |\!\}_P$ means encr. with P's public key

$[\![\ -\ ]\!]_P$ means digital signature

$$mo = [\![\, hash(C,\ N_c,\ N_b,\ N_m,\ price)\,]\!]_B$$



Nonce sent encrypted

Authentication test pattern

- When a freshly chosen value N is:
  - Sent inside encryptions $S =$

$$\{\, \{\!|\, \cdots N \cdots \,|\!\}_{K_1}, \ldots, \{\!|\, \cdots N \cdots \,|\!\}_{K_i} \,\}$$

  - Received later outside these forms
- Infer: either
  - Some decryption key K_i^{-1} is compromised, or else
  - A regular participant received some

$$\{\!|\, \cdots N \cdots \,|\!\}_{K_i}$$

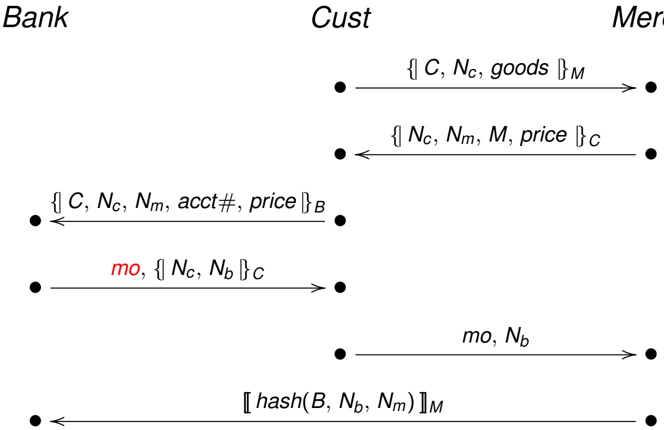
    and retransmitted N in another form

Merchant / Bank Agreement

$\{\!| - |\!\}_P$ means encr. with P's public key

$[\![-]\!]_P$ means digital signature

$mo = [\![\, hash(C,\ N_c,\ N_b,\ N_m,\ price)\,]\!]_B$



Encrypted message received

The second authentication test pattern

- If encrypted value $c = \{\!|\, t \,|\!\}_{K_0}$ is received outside forms $S =$

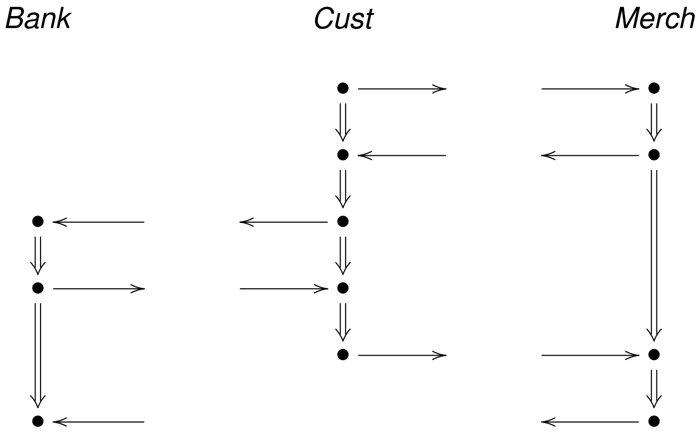
$$\{\{\!|\, \cdots c \cdots \,|\!\}_{K_1}, \ldots, \{\!|\, \cdots c \cdots \,|\!\}_{K_i}\}$$

- Infer: either
  - Encryption key K_0 is compromised, or else
  - Some decryption key is compromised, or else

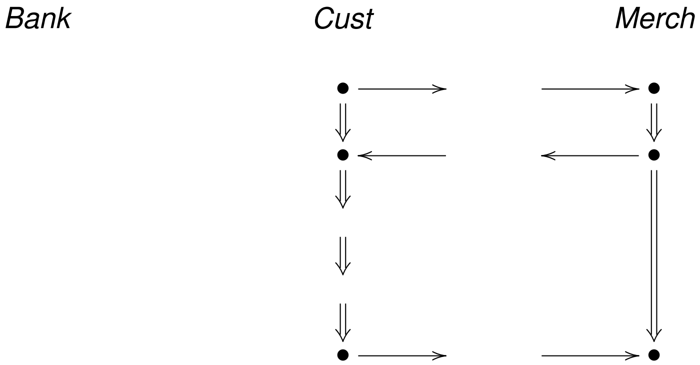
$$K_j^{-1} \text{ for } 1 \leq j \leq i$$

  - Regular participant received c only within S, if at all, transmitted c outside

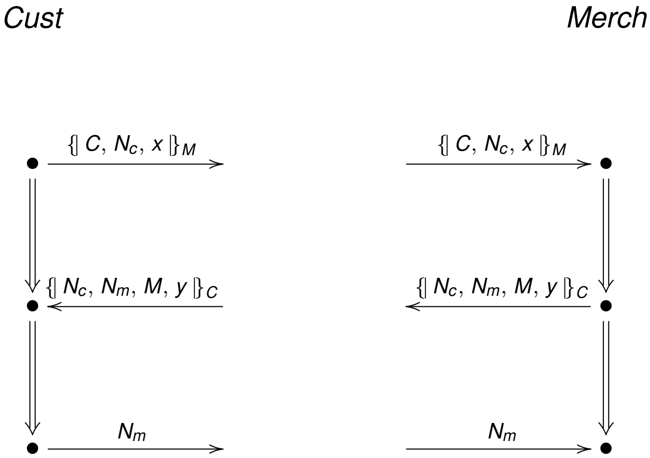
The Strand Space point of view



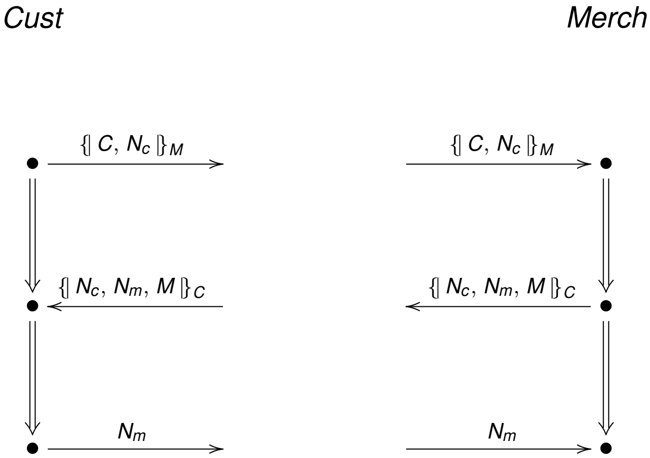
Simplification: Customer-merchant subprotocol



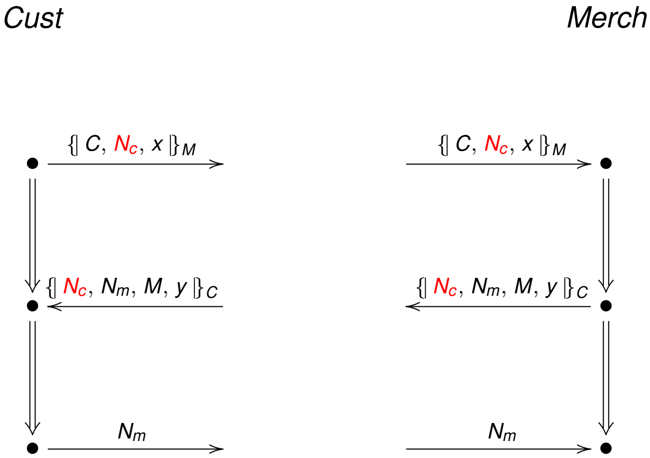
EPMO customer-merchant subprotocol



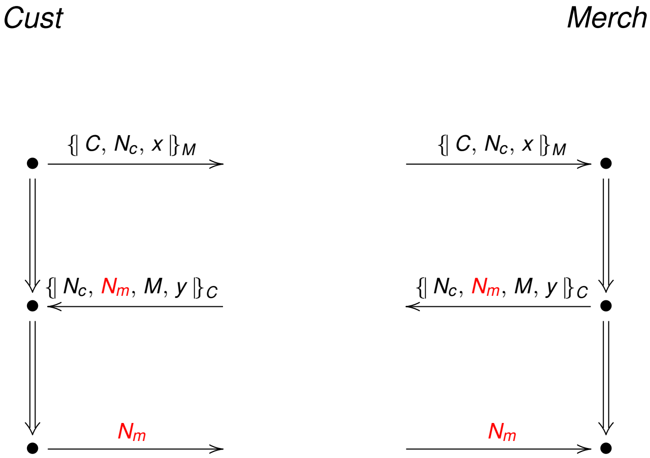
Needham-Schroeder-Lowe



EPMO: How customer tests merchant



EPMO: How merchant tests customer



Nonce sent encrypted

Authentication test pattern

- When a freshly chosen value N is:
  - Sent inside encryptions $S =$

$$\{ \{\!| \cdots N \cdots |\!\}_{K_1}, \ldots, \{\!| \cdots N \cdots |\!\}_{K_i} \}$$

  - Received later outside these forms
- Infer: either
  - Some decryption key K_i^{-1} is compromised, or else
  - A regular participant received some

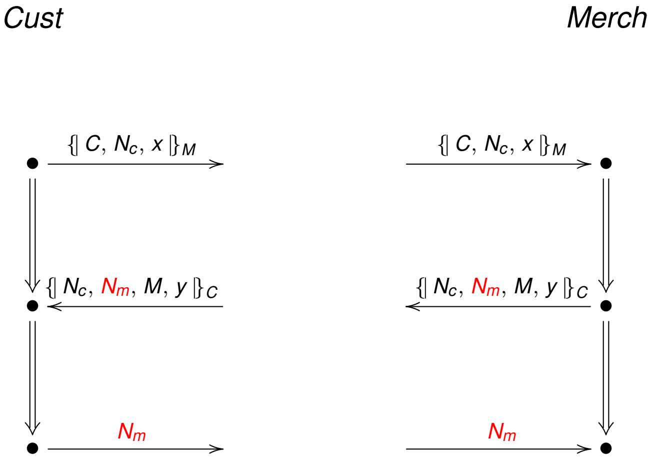
$$\{\!| \cdots N \cdots |\!\}_{K_i}$$

    and retransmitted N in another form

Translating tests

- Test consists of:
  - Critical value c, e.g. N_m
  - Escape set S, e.g. $\{ \{\!| N_c, N_m, M, y |\!\}_C \}$
- Solution could be
  - Compromised decryption key C^{-1}
  - Regular edge that receives N_m only within S, retransmits N_m outside S

EPMO: How merchant tests customer

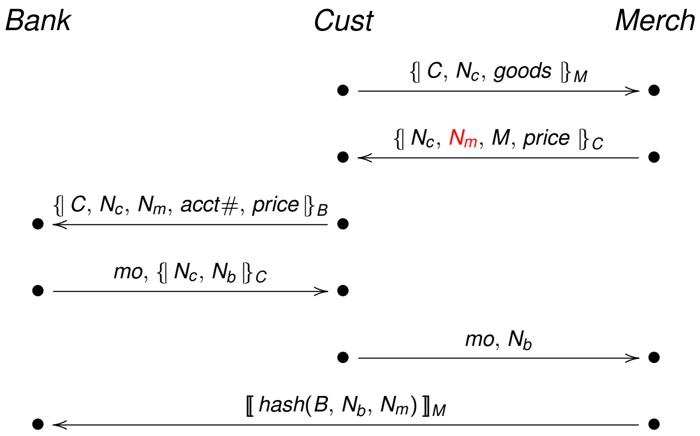


Merchant / Customer Agreement

$\{\!|\ -\ |\!\}_P$ means encr. with P's public key

$[\![\ -\ ]\!]_P$ means digital signature

$mo = [\![\ hash(C,\ N_c,\ N_b,\ N_m,\ price)\ ]\!]_B$



Translating a Test

- Subprotocol test:
  - Critical value: N_m
  - Escape set: $S_0 = \{ \{\!| N_c, N_m, M, y |\!\}_C \}$
- EPMO test $T(c, S_0)$:
  - Critical value: N_m
  - Escape set: $S_0 \cup$

$$\{ \{\!| C, N_c, N_m, acct\#, price |\!\}_B : acct\# \text{ is an acct } \} \quad \cup$$

$$\{ [\![hash(C, N_c, N_b, N_m, price)]\!]_B : B \text{ is a bank } \}$$

Translating a Test

- Subprotocol test:
  - Critical value: N_m
  - Escape set: $S_0 = \{ \{\!| N_c, N_m, M, y |\!\}_C \}$
- EPMO test $T(c, S_0)$:
  - Critical value: N_m
  - Escape set: $S_0 \cup$

$$\{ \{\!| C, N_c, N_m, acct\#, price |\!\}_B : acct\# \text{ is an acct } \} \quad \cup$$

$$\{ [\![hash(C, N_c, N_b, N_m, price)]\!]_B : B \text{ is a bank } \}$$

- Solutions to subprotocol test in $\mathbb{A}$
  vs. Solutions to subprotocol test in $\mathbb{A}$

Protocol Transformation $F : \Pi_1 \to \Pi_2$

F determines maps:

- Π_1 skeletons $\to$ Π_2 skeletons
- $\mathcal{L}(\Pi_1) \to \mathcal{L}(\Pi_2)$

When does F preserve $\mathcal{L}(\Pi_1)$-goals $\quad \forall \vec{x} \,.\, (\phi_0 \supset \exists \vec{y} \,.\, \bigvee_{1 \le i \le j} \phi_i)$?

$$
\begin{tikzcd}
\mathrm{cs}(\phi_0) \arrow[r, mapsto, "?"'] \arrow[rr, mapsto, bend left] \arrow[d, "F"'] & \color{red}{\mathbb{A}_{\mathrm{real}}} \arrow[r, mapsto, "?"'] & \mathbb{A}_1 \arrow[d, "F"] & \\
\mathrm{cs}(F(\phi_0)) \arrow[rr, mapsto] \arrow[rrr, mapsto, bend right] & & F(\mathbb{A}_1) \arrow[r, mapsto] & \mathbb{B}_{\mathrm{real}}
\end{tikzcd}
$$

Two Conditions

Sufficing for goal preservation

- If $\mathbb{A}$ has unsolved test c, S,
  then $F(\mathbb{A})$ has unsolved test $T(c, S)$
- If step

$$F(\mathbb{A}) \stackrel{T(c,S)}{\longrightarrow} \mathbb{B}$$

  in Π_2, then $\mathbb{B} = F(\mathbb{A}_1)$ and

$$\mathbb{A} \stackrel{c,S}{\longrightarrow} \mathbb{A}_1$$

Two Conditions

Sufficing for goal preservation

- If $\mathbb{A}$ has unsolved test c, S, then $F(\mathbb{A})$ has unsolved test $T(c, S)$
- If step
$$F(\mathbb{A}) \stackrel{T(c,S)}{\longrightarrow} \mathbb{B}$$
in Π_2, then $\mathbb{B} = F(\mathbb{A}_1)$ and
$$\mathbb{A} \stackrel{c,S}{\longrightarrow} \mathbb{A}_1$$
I.e. test solution LTS in Π_1 simulates Π_2 relative to F for skeletons of the form $F(\mathbb{A})$ and steps of the form $T(c, S)$

Preserving Goals

- $\Pi_2 = F(\Pi_1)$: Π_2 results by transformation F from Π_1
  - Inclusive, low-syntax relation
  - Homomorphisms among skeletons match up
  - Need additional constraints to ensure goals of Π_1 preserved
- Need: authentication tests preserved;
  no new solutions to old tests
- Consequence: $H\colon F(\mathbb{A}) \mapsto \mathbb{B}$ realized implies
  - $J\colon \mathbb{A} \mapsto \mathbb{A}_1$ splits into $L \circ K$
  - $K\colon \mathbb{A} \mapsto \mathbb{A}_0$ realized
  - where: $\mathbb{A}_1$ is maximal s.t. $F(\mathbb{A}_1) \mapsto \mathbb{B}$