Goal-Preserving Transformations

Joshua D. Guttman

Worcester Polytechnic Institute

Protocol Exchange
7 Oct 2009
Preserving Goals

\[ \Pi_2 = F(\Pi_1) : \Pi_2 \text{ results by transformation } F \text{ from } \Pi_1 \]
Preserving Goals

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

Need: authentication tests preserved; no new solutions to old tests

Consequence:

$H: F(A) \mapsto B$ realized implies

$J: A \mapsto A_1$ splits into $L \circ K$

$K: A \mapsto A_0$ realized

where: $A_1$ is maximal s.t. $F(A_1) \mapsto B$
Preserving Goals

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

- Need additional constraints to ensure goals of $\Pi_1$ preserved
- Need: authentication tests preserved; no new solutions to old tests
- Consequence:
  - $H: F(A) \mapsto B$ realized implies
  - $J: A \mapsto A_1$ splits into $L \circ K$
  - $K: A \mapsto A_0$ realized
  - Where: $A_1$ is maximal s.t. $F(A_1) \mapsto B$
Preserving Goals

\[ \Pi_2 = F(\Pi_1) : \Pi_2 \text{ results by transformation } F \text{ from } \Pi_1 \]

- Inclusive, low-syntax relation
- Homomorphisms among skeletons match up
- Need additional constraints to ensure goals of \( \Pi_1 \) preserved
Preserving Goals

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

- Need: authentication tests preserved; no new solutions to old tests
Preserving Goals

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

- Need: authentication tests preserved; no new solutions to old tests

- Consequence: $H: F(\mathbb{A}) \leftrightarrow \mathbb{B}$ realized implies
  - $J: \mathbb{A} \leftrightarrow \mathbb{A}_1$ splits into $L \circ K$
  - $K: \mathbb{A} \leftrightarrow \mathbb{A}_0$ realized
  - where: $\mathbb{A}_1$ is maximal s.t. $F(\mathbb{A}_1) \leftrightarrow \mathbb{B}$
Protocol Transformation $F: \Pi_1 \rightarrow \Pi_2$

$F$ determines maps:
- $\Pi_1$ skeletons $\rightarrow$ $\Pi_2$ skeletons
- $\mathcal{L}(\Pi_1) \rightarrow \mathcal{L}(\Pi_2)$

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

\[
\begin{array}{c}
\text{cs}(\phi_0) \\
F \\
\text{cs}(F(\phi_0))
\end{array}
\]
Protocol Transformation $F : \Pi_1 \rightarrow \Pi_2$

$F$ determines maps:
- $\Pi_1$ skeletons $\rightarrow \Pi_2$ skeletons
- $\mathcal{L}(\Pi_1) \rightarrow \mathcal{L}(\Pi_2)$

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

Diagram:

```
cs(\phi_0)           \mathbb{B}_{\text{real}}
\downarrow F          \downarrow F
cs(F(\phi_0))
```
Protocol Transformation $F : \Pi_1 \rightarrow \Pi_2$

$F$ determines maps:
- $\Pi_1$ skeletons $\rightarrow \Pi_2$ skeletons
- $\mathcal{L}(\Pi_1) \rightarrow \mathcal{L}(\Pi_2)$

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

\[\text{cs}(\phi_0) \xrightarrow{F} \text{cs}(F(\phi_0)) \rightarrow F(A_1) \rightarrow \mathbb{B}_{\text{real}}\]
Protocol Transformation $F : \Pi_1 \rightarrow \Pi_2$

$F$ determines maps:
- $\Pi_1$ skeletons $\rightarrow \Pi_2$ skeletons
- $\mathcal{L}(\Pi_1) \rightarrow \mathcal{L}(\Pi_2)$

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

\[
\begin{array}{c}
\text{cs}(\phi_0) \\
 F \downarrow \\
\text{cs}(F(\phi_0)) \\
 F \downarrow \\
 F(A_1) \\
 \text{B}_{\text{real}}
\end{array}
\]
Protocol Transformation $F : \Pi_1 \rightarrow \Pi_2$

$F$ determines maps:

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

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

\[
\begin{array}{c}
\text{cs}(\phi_0) \quad \text{cs}(F(\phi_0)) \\
F \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad F
\end{array}
\]
Electronic Purchase
Using a money order: *EPMO*

**Bank**  

**Cust**  

**Merch**
Electronic Purchase
Using a money order: \textit{EPMO}

\begin{center}
\begin{tikzpicture}

\node (Bank) at (0,0) \textit{Bank};
\node (Cust) at (3,0) \textit{Cust};
\node (Merch) at (6,0) \textit{Merch};

\draw[->] (Bank) -- (Cust) node[midway,above] {query \textit{goods}};
\draw[<-] (Cust) -- (Merch);
\draw[<-] (Bank) -- (Merch);
\draw[<-] (Merch) -- (Bank);
\end{tikzpicture}
\end{center}
Electronic Purchase

Using a money order: *EPMO*

**Bank** ↔ **Cust** ↔ **Merch**

- *query goods*
- *reply price*

Guttman (WPI)  Goal-Preserving  Oct 09  4 / 25
Electronic Purchase
Using a money order: \textit{EPMO}

\begin{center}
\begin{tikzpicture}
\node (Bank) at (0,0) {? \textit{Bank}};
\node (Cust) at (3,0) {? \textit{Cust}};
\node (Merch) at (6,0) {? \textit{Merch}};

\draw[->] (Bank) -- (Cust) node [midway, above] {query \textit{goods}};
\draw[<->] (Cust) -- (Merch) node [midway, above] {reply \textit{price}};
\draw[->] (Bank) -- (Cust) node [midway, above] {cutmo acct\# \textit{price}};
\draw[<->] (Cust) -- (Bank);
\end{tikzpicture}
\end{center}
Electronic Purchase
Using a money order: *EPMO*

**Diagram:**
- **Bank**
  - cutmo *acct# price*
  - *mo*

- **Cust**
  - query *goods*
  - reply *price*

- **Merch**
  - *EPMO*
  - Bank Cust Merch
  - Query goods
  - Reply price
  - Cutmo acct# price
  - Mo
Electronic Purchase
Using a money order: EPMO

Bank

Cust

Merch

query goods

reply price

cutmo acct# price

mo

endorse mo
Electronic Purchase
Using a money order: *EPMO*

```
Bank → Cust -> Merch

query goods

reply price

cutmo acct# price

mo

endorse mo

deposit mo
```
EPMO

\[ {\{ - \}}_P \] means encr. with \( P \)'s public key

\[ {\mid - \mid}_P \] means digital signature

\[ mo = \text{[hash}(C, N_c, N_b, N_m, \text{price})]\text{]}_B \]

\text{Bank} \quad \text{Cust} \quad \text{Merch}

\[ \{ C, N_c, \text{goods} \}\text{]}_M \]

\[ \{ N_c, N_m, M, \text{price} \}\text{]}_C \]

\[ \{ C, N_c, N_m, \text{acct}\#, \text{price} \}\text{]}_B \]

\[ mo, \{ N_c, N_b \}\text{]}_C \]

\[ \text{[hash}(B, N_b, N_m)\text{]}_M \]

\[ mo, N_b \]
Customer / Merchant Agreement

\[ \{ - \}_P \] means encr. with \( P \)'s public key

\[ [-]_P \] means digital signature

\[ mo = \left\{ hash(C, N_c, N_b, N_m, price) \right\}_B \]

---

Bank

Cust

Merch

\[ \{ C, N_c, goods \} \_M \]

\[ \{ N_c, N_m, M, price \} \_C \]

\[ \{ C, N_c, N_m, acct\#, price \} \_B \]

\[ mo, \{ N_c, N_b \} \_C \]

\[ mo, N_b \]

\[ [ hash(B, N_b, N_m) ] \_M \]
Merchant / Customer Agreement

\( \{ - \}_P \) means encr. with \( P \)'s public key

\( \lbrack - \rbrack_P \) means digital signature

\( mo = \lbrack \text{hash}(C, N_c, N_b, N_m, \text{price}) \rbrack_B \)

---

**Bank**

\[ \begin{array}{c}
\{ C, N_c, \text{goods} \} \rightarrow \\
\{ C, N_c, N_m, \text{acct\#}, \text{price} \} \leftarrow \\
\text{mo, } \lbrack N_c, N_b \rbrack \rightarrow \\
\text{mo, } N_b \rightarrow \\
\lbrack \text{hash}(B, N_b, N_m) \rbrack \leftarrow \\
\end{array} \]

**Cust**

\[ \begin{array}{c}
\{ C, N_c, \text{goods} \} \rightarrow \\
\{ N_c, N_m, M, \text{price} \} \leftarrow \\
\end{array} \]

**Merch**

\[ \begin{array}{c}
\{ C, N_c, N_m, \text{acct\#}, \text{price} \} \leftarrow \\
\end{array} \]
Customer / Bank Agreement

\[ \{ - \}_P \] means encr. with \( P \)'s public key

\[ [ - ]_P \] means digital signature

\[ mo = \left[ \text{hash}(C, N_c, N_b, N_m, \text{price}) \right]_B \]

**Bank**

\[ \{ C, N_c, \text{goods} \} \_M \]

\[ \{ C, N_c, N_m, acct\#, \text{price} \} \_B \]

\[ mo, \{ N_c, N_b \} \_C \]

\[ mo, N_b \]

\[ \left[ \text{hash}(B, N_b, N_m) \right]_M \]

**Cust**

\[ \{ C, N_c, goods \} \_M \]

\[ \{ N_c, N_m, M, \text{price} \} \_C \]

\[ \{ C, N_c, N_m, acct\#, \text{price} \} \_B \]

\[ mo, \{ N_c, N_b \} \_C \]

\[ mo, N_b \]

**Merch**

\[ \left[ \text{hash}(B, N_b, N_m) \right]_M \]
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

\( \{ \cdot - \cdot \}_P \) means encr. with \( P \)'s public key

\( \{ - \}_P \) means digital signature

\( mo = \left\lbrack \text{hash}(C, N_c, N_b, N_m, \text{price}) \right\rbrack_B \)

\( \{ C, N_c, \text{goods} \}_M \)

\( \{ N_c, N_m, M, \text{price} \}_C \)

\( \{ C, N_c, N_m, \text{acct\#}, \text{price} \}_B \)

\( mo, \{ N_c, N_b \}_C \)

\( mo, N_b \)

\( \left\lbrack \text{hash}(B, N_b, N_m) \right\rbrack_M \)
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

Bank

Cust

Merch

Guttman (WPI)
Goal-Preserving

Oct 09 12/25
Simplification: Customer-merchant subprotocol

Bank → Cust ↓ Merch

Guttman (WPI) Goal-Preserving Oct 09 13/25
EPMO customer-merchant subprotocol

**Cust**

\[ \{C, N_c, x \}_{M} \]

\[ \{N_c, N_m, M, y \}_{C} \]

\[ N_m \]

**Merch**

\[ \{C, N_c, x \}_{M} \]

\[ \{N_c, N_m, M, y \}_{C} \]

\[ N_m \]
Needham-Schroeder-Lowe

\[ \{ C, N_c \} \rightarrow M \]

\[ \{ N_c, N_m, M \} \rightarrow C \]

\[ \{ C, N_c \} \rightarrow M \]

\[ \{ N_c, N_m, M \} \rightarrow C \]

\[ N_m \]

\[ N_m \]
EPMO: How customer tests merchant

\[
\begin{align*}
\text{Cust} & \rightarrow \{ C, N_c, x \}_M \downarrow \downarrow \{ N_c, N_m, M, y \}_C \\
& \text{N}_m \\
\text{Merch} & \leftarrow \{ C, N_c, x \}_M \\
& \text{N}_m
\end{align*}
\]
EPMO: How merchant tests customer

\[ \{ C, N_c, x \} \rightarrow \{ N_c, N_m, M, y \} \]

\[ \{ C, N_c, x \} \rightarrow \{ N_c, N_m, M, y \} \]

\[ \{ N_c, N_m, M, y \} \rightarrow \{ C, N_c, x \} \]

\[ \{ N_c, N_m, M, y \} \rightarrow \{ C, N_c, x \} \]

\[ N_m \rightarrow N_m \]

\[ N_m \rightarrow N_m \]
Nonce sent encrypted

Authentication test pattern

- When a freshly chosen value $N$ is:
  - Sent inside encryptions $S = \{ \{ \cdots N \cdots \}^S_{K_1}, \ldots, \{ \cdots N \cdots \}^S_{K_i}\}$
  - Received later outside these forms
- Infer: either
  - Some decryption key $K_i^{-1}$ is compromised, or else
  - A regular participant received some
    $$\{ \cdots N \cdots \}^S_{K_i}$$
    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

\[ \{ C, N_c, x \} \xrightarrow{M} \{ N_c, N_m, M, y \} \xrightarrow{C} \{ N_c, N_m, M, y \} \xrightarrow{M} \{ C, N_c, x \} \]
Merchant / Customer Agreement

\( \{ - \}_P \) means encr. with \( P \)'s public key

\( \lceil - \rceil_P \) means digital signature

\[ mo = \lceil \text{hash}(C, N_c, N_b, N_m, \text{price}) \rceil_B \]

---

**Diagram**

**Bank**

\( \{ C, N_c, \text{goods} \}_M \)

\( \{ N_c, N_m, M, \text{price} \}_C \)

\( \{ C, N_c, N_m, \text{acct}\#, \text{price} \}_B \)

**Cust**

\( mo, \{ N_c, N_b \}_C \)

**Merch**

\( mo, N_b \)

\[ \lceil \text{hash}(B, N_b, N_m) \rceil_M \]
Translating a Test

- **Subprotocol test:**
  - Critical value: $N_m$
  - Escape set: $S_0 = \{ \{ N_c, N_m, M, y \} \}$

- **EPMO test $T(c, S_0)$:**
  - Critical value: $N_m$
  - Escape set: $S_0 \cup \{ \{ C, N_c, N_m, acct\#, price \} \}_{B} : \text{acct\# is an acct} \} \cup \{ \{ hash(C, N_c, N_b, N_m, price) \} \}_{B} : B \text{ is a bank}\}$
Translating a Test

- **Subprotocol test:**
  - Critical value: $N_m$
  - Escape set: $S_0 = \{ \{ N_c, N_m, M, y \} \}$

- **EPMO test $T(c, S_0)$:**
  - Critical value: $N_m$
  - Escape set: $S_0 \cup \{ \{ C, N_c, N_m, \text{acct}\#, \text{price} \} : \text{acct}\# \text{ is an acct} \} \cup \{ \{ \text{hash}(C, N_c, N_b, N_m, \text{price}) \} : B \text{ is a bank} \}$

- Solutions to subprotocol test in $A$
  vs. Solutions to subprotocol test in $A$
Protocol Transformation \( F: \Pi_1 \to \Pi_2 \)

\( F \) determines maps:
- \( \Pi_1 \) skeletons \( \to \Pi_2 \) skeletons
- \( \mathcal{L}(\Pi_1) \to \mathcal{L}(\Pi_2) \)

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

\[
\begin{align*}
\text{cs}(\phi_0) & \xrightarrow{F} \text{A}_{\text{real}} \\
\text{A}_{\text{real}} & \xrightarrow{?} \text{A}_1 \\
\text{cs}(F(\phi_0)) & \xrightarrow{F} \text{B}_{\text{real}}
\end{align*}
\]
Two Conditions
Sufficing for goal preservation

- If $A$ has unsolved test $c, S$, then $F(A)$ has unsolved test $T(c, S)$

- If step $F(A) \xrightarrow{T(c,S)} B$ in $\Pi_2$, then $B = F(A_1)$ and $A \xrightarrow{c,S} A_1$
Two Conditions
Sufficing for goal preservation

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

$$F(A) \xrightarrow{T(c,S)} B$$

in $\Pi_2$, then $B = F(A_1)$ and

$$A \xrightarrow{c,S} A_1$$

I.e. test solution LTS in $\Pi_1$ simulates $\Pi_2$ relative to $F$ for skeletons of the form $F(A)$ and steps of the form $T(c, S)$
Preserving Goals

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

- Need: authentication tests preserved; no new solutions to old tests

- Consequence: $H: F(\mathbb{A}) \mapsto \mathbb{B}$ realized implies
  - $J: \mathbb{A} \mapsto \mathbb{A}_1$ splits into $L \circ K$
  - $K: \mathbb{A} \mapsto \mathbb{A}_0$ realized
  - where: $\mathbb{A}_1$ is maximal s.t. $F(\mathbb{A}_1) \mapsto \mathbb{B}$