

The Anatomy of a Crypto Protocol

Joshua D. Guttman¹ John D. Ramsdell²

¹Worcester Polytechnic Institute ²The MITRE Corporation

Thanks to the [MITRE-Sponsored Research](#) program and the
[National Security Agency](#).

Symposium for Mitchell Wand
24 Aug 2009

Protocols coordinate distribute systems

Despite malicious adversaries

Allow principals to

- Agree selectively on values
- Undertake commitments involving those values
- Coordinate state changes

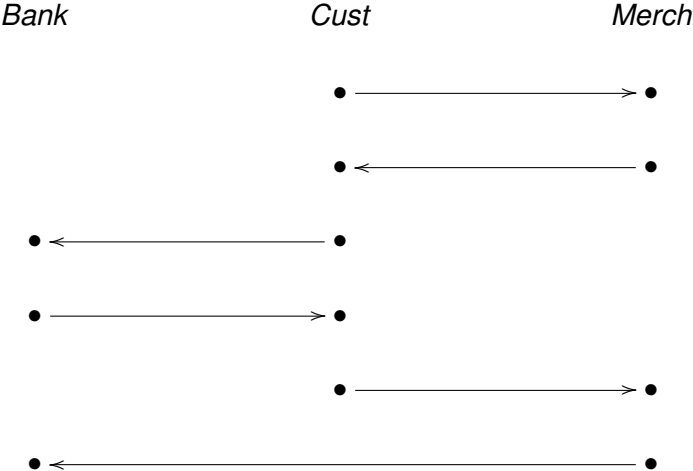
Application-specific crypto protocols

Three claims

- Central to secure distributed systems
- Analysis uses two basic principles: **authentication tests**
 - ▶ Formalized in a small denotational semantics
 - ▶ Analysis tool CPSA
- Authentication tests also suggest systematic protocol design methods

Electronic Purchase

Using a money order: *EPMO*



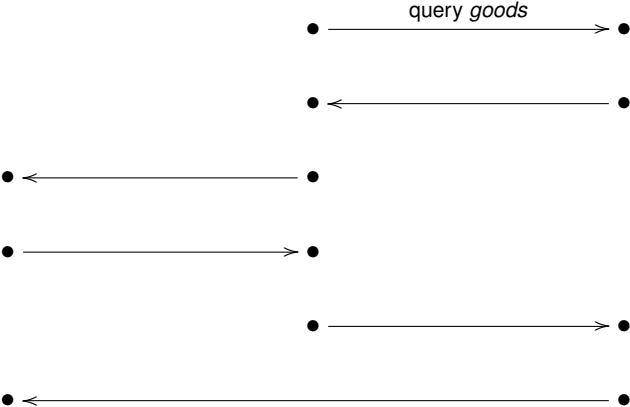
Electronic Purchase

Using a money order: *EPMO*

Bank

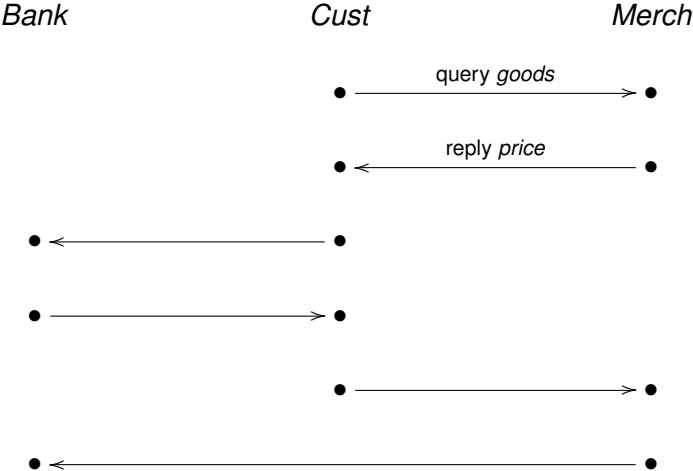
Cust

Merch



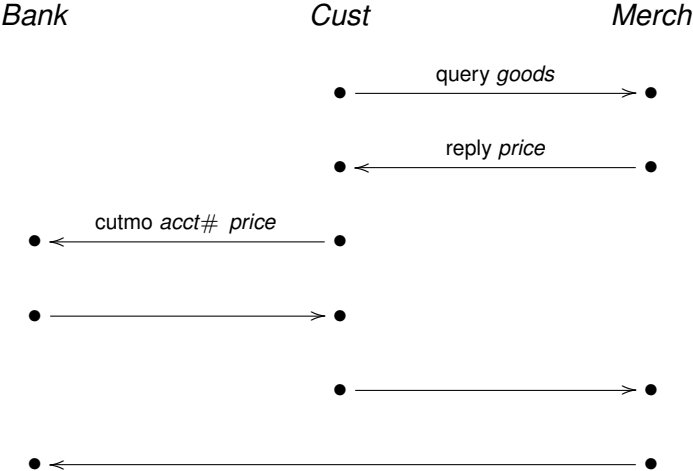
Electronic Purchase

Using a money order: *EPMO*



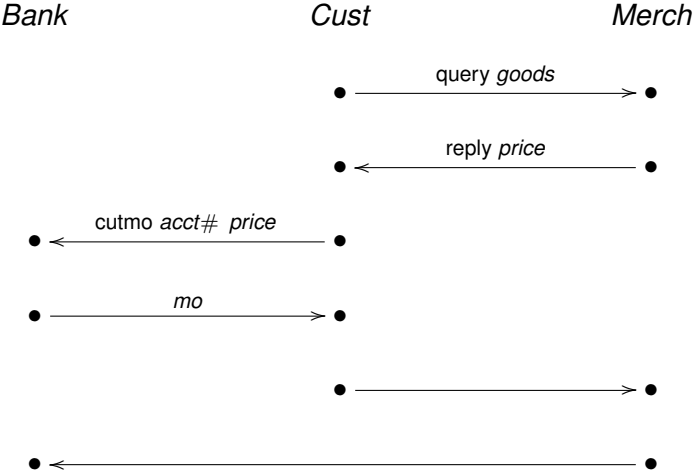
Electronic Purchase

Using a money order: *EPMO*



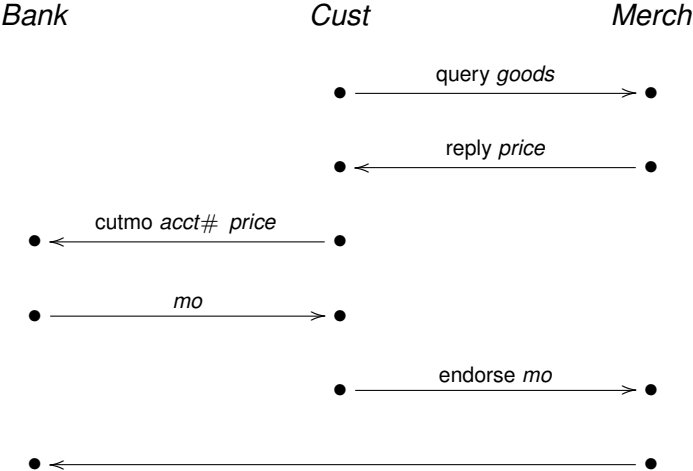
Electronic Purchase

Using a money order: *EPMO*



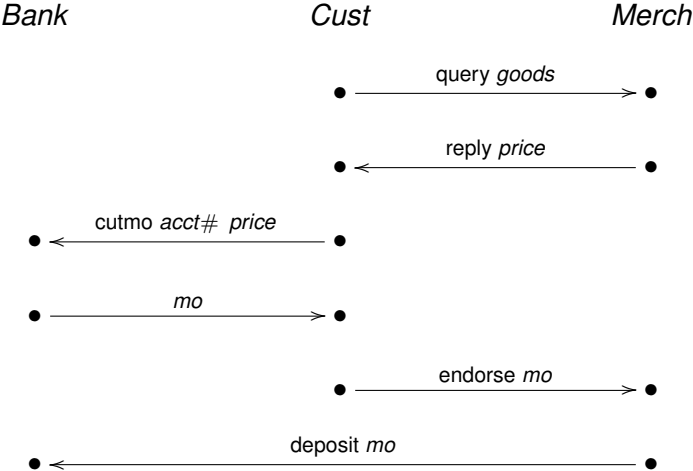
Electronic Purchase

Using a money order: *EPMO*



Electronic Purchase

Using a money order: *EPMO*



EPMO Goals

- *Cust, Merch, Bank* agree on:
 - ▶ principal identities
 - ▶ *price*
- *Cust, Merch* agree on *goods*
- *Cust, Bank* agree on *acct#*
- Beyond that, full confidentiality

EPMO₁

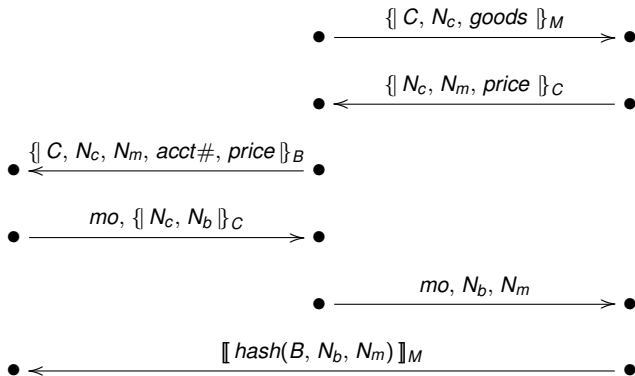
$\{ - \}_P$ means encr. with P 's public key
 $\llbracket - \rrbracket_P$ means digital signature

$mo = \llbracket hash(C, N_c, N_b, N_m, price) \rrbracket_B$

Bank

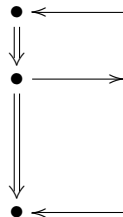
Cust

Merch

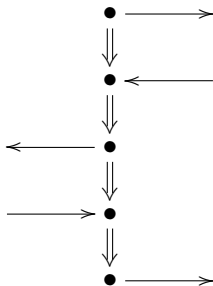


The Strand Space point of view

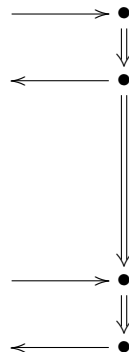
Bank



Cust



Merch

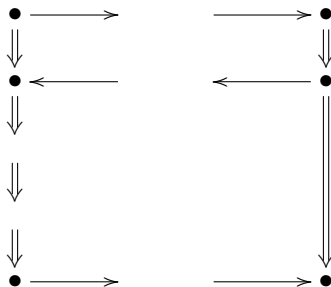


Simplification: Customer-merchant subprotocol

Bank

Cust

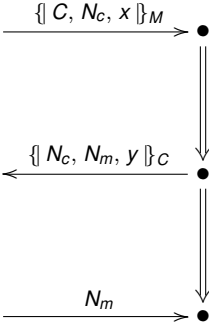
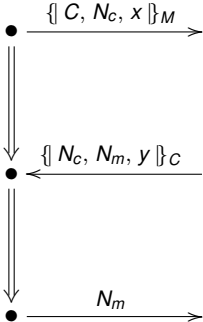
Merch



$EPMO_1$ customer-merchant subprotocol

Cust

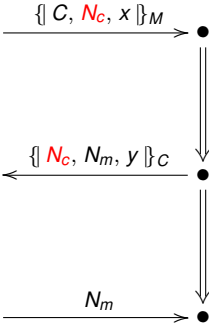
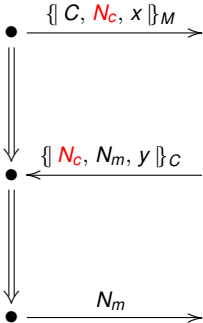
Merch



$EPMO_1$: How customer tests merchant

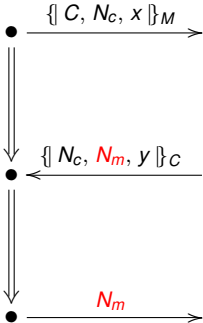
Cust

Merch

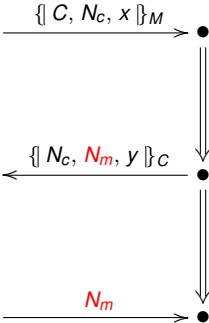


$EPMO_1$: How merchant tests customer

Cust



Merch



Nonce sent encrypted

Authentication test pattern

- When a freshly chosen value N is:

- ▶ Sent inside encryption

$$\{ \dots N \dots \}_K$$

- ▶ Received later outside this form

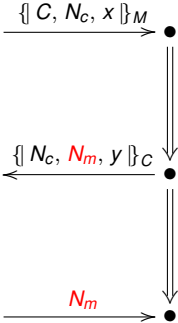
- Infer: either

- ▶ Decryption key K^{-1} is compromised, or else
- ▶ A regular participant received

$$\{ \dots N \dots \}_K$$

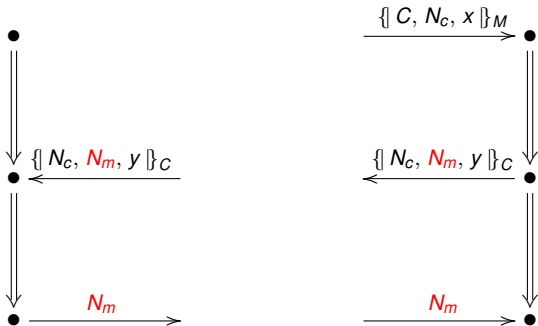
and retransmitted N in another form

$EPMO_1$: What does the merchant learn?



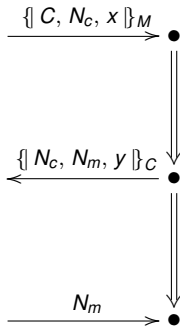
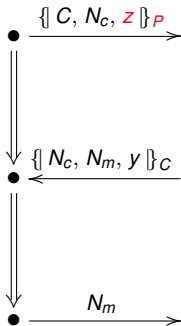
$EPMO_1$: What does the merchant learn?

If N_m freshly chosen, C 's decryption key uncompromised

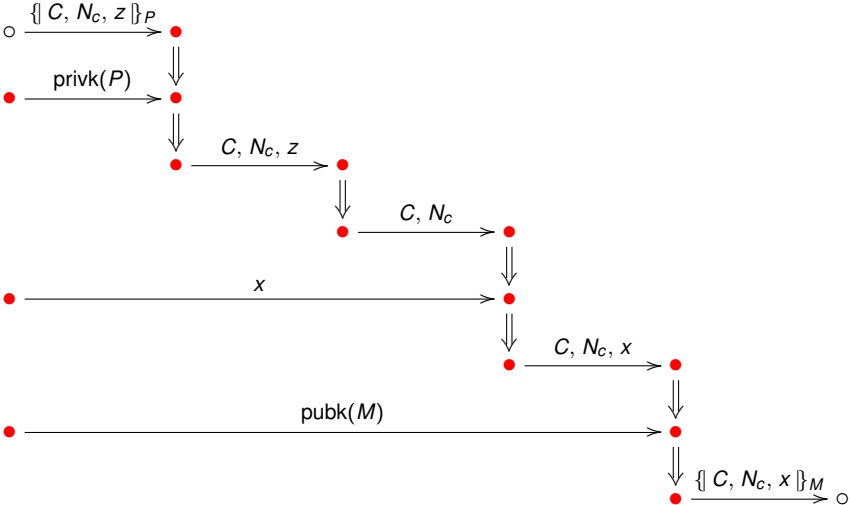


$EPMO_1$: What does the merchant learn?

If N_m freshly chosen, C 's decryption key uncompromised

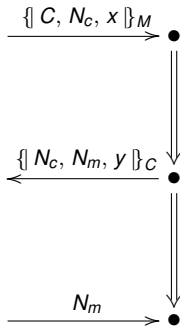
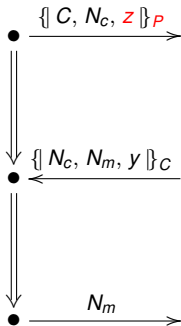


EPMO₁: How this is possible



$EPMO_1$: What does the merchant learn?

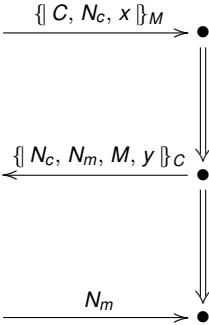
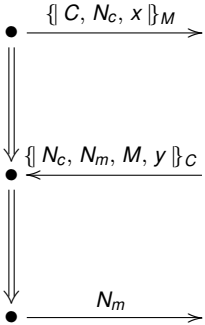
If N_m freshly chosen, C 's decryption key uncompromised



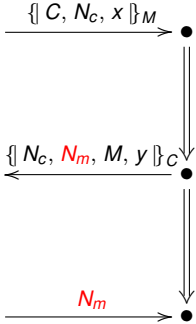
*EPMO*₂ customer-merchant subprotocol

Cust

Merch

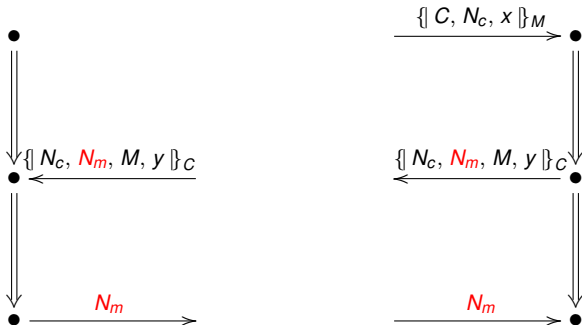


$EPMO_2$: What does the merchant learn?



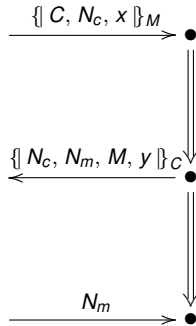
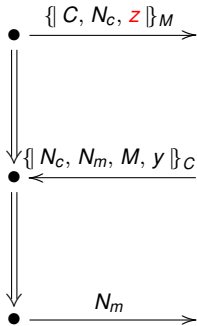
$EPMO_2$: What does the merchant learn?

If N_m freshly chosen, C 's decryption key uncompromised



$EPMO_2$: What does the merchant learn?

If N_m freshly chosen, C 's decryption key uncompromised



EPMO₂

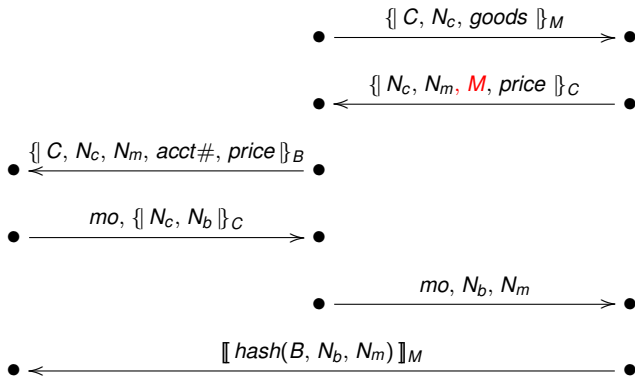
$\{ - \}_P$ means encr. with P 's public key
 $\llbracket - \rrbracket_P$ means digital signature

$$mo = \llbracket hash(C, N_c, N_b, N_m, price) \rrbracket_B$$

Bank

Cust

Merch



Small denotational semantics

For crypto protocols

- Skeletons \mathbb{A} :
 - ▶ Partial executions (see previous slides)
 - ▶ Some skeletons are *realized*

Small denotational semantics

For crypto protocols

- Skeletons \mathbb{A} :
 - ▶ Partial executions (see previous slides)
 - ▶ Some skeletons are *realized*
- Homomorphisms H :
Structure-preserving maps

$$H: \mathbb{A} \mapsto \mathbb{B}$$

Small denotational semantics

For crypto protocols

- Skeletons \mathbb{A} :
 - ▶ Partial executions (see previous slides)
 - ▶ Some skeletons are *realized*
- Homomorphisms H :
Structure-preserving maps

$$H: \mathbb{A} \mapsto \mathbb{B}$$

- Test-solving transition relation:

$$\mathbb{A} \rightsquigarrow \mathbb{B}$$

Small denotational semantics

For crypto protocols

- Skeletons \mathbb{A} :
 - ▶ Partial executions (see previous slides)
 - ▶ Some skeletons are *realized*
- Homomorphisms H :
Structure-preserving maps

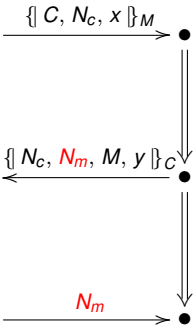
$$H: \mathbb{A} \mapsto \mathbb{B}$$

- Test-solving transition relation:

$$\mathbb{A} \rightsquigarrow \mathbb{B}$$

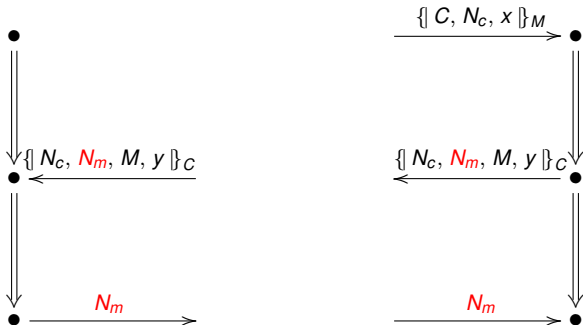
\mathbb{A} is realized iff every test in \mathbb{A} is solved

$EPMO_2$: What does the merchant learn?



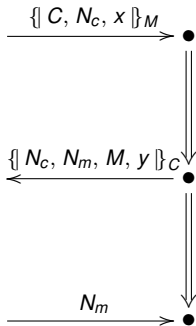
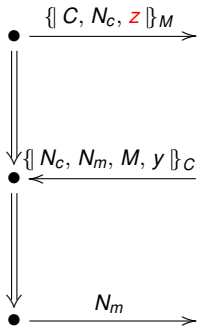
$EPMO_2$: What does the merchant learn?

If N_m freshly chosen, C 's decryption key uncompromised



$EPMO_2$: What does the merchant learn?

If N_m freshly chosen, C 's decryption key uncompromised



Three key facts

- $A \rightsquigarrow B$ implies

$$H: A \mapsto B$$

for some H

Three key facts

- $A \rightsquigarrow B$ implies

$$H: A \mapsto B$$

for some H

- A is realized implies in LTS

$$A \sim / \rightsquigarrow$$

Three key facts

- $A \rightsquigarrow B$ implies

$$H: A \mapsto B$$

for some H

- A is realized implies in LTS

$$A \sim / \rightsquigarrow$$

- Suppose $A_0 \mapsto A$ and A is realized.
Then for some realized A_1 ,

$$A_0 \rightsquigarrow^* A_1 \quad \text{and} \quad A_1 \mapsto A$$

Application-specific crypto protocols

Three claims

- Central to secure distributed systems
- Analysis uses two basic principles: **authentication tests**
 - ▶ Formalized in a small denotational semantics
 - ▶ Analysis tool CPSA
- Authentication tests also suggest systematic protocol design methods