

Protecting Mobile Agent Data with Data Encapsulation and Cryptographic Tracing

Anna Suen
suen@cs.fsu.edu
March 19, 2003

Preview

★Background Review

- Execution Tracing
- Data Encapsulation
 - publicly verifiable chained digital signature protocol
 - chained MAC protocol
 - data collection protocol

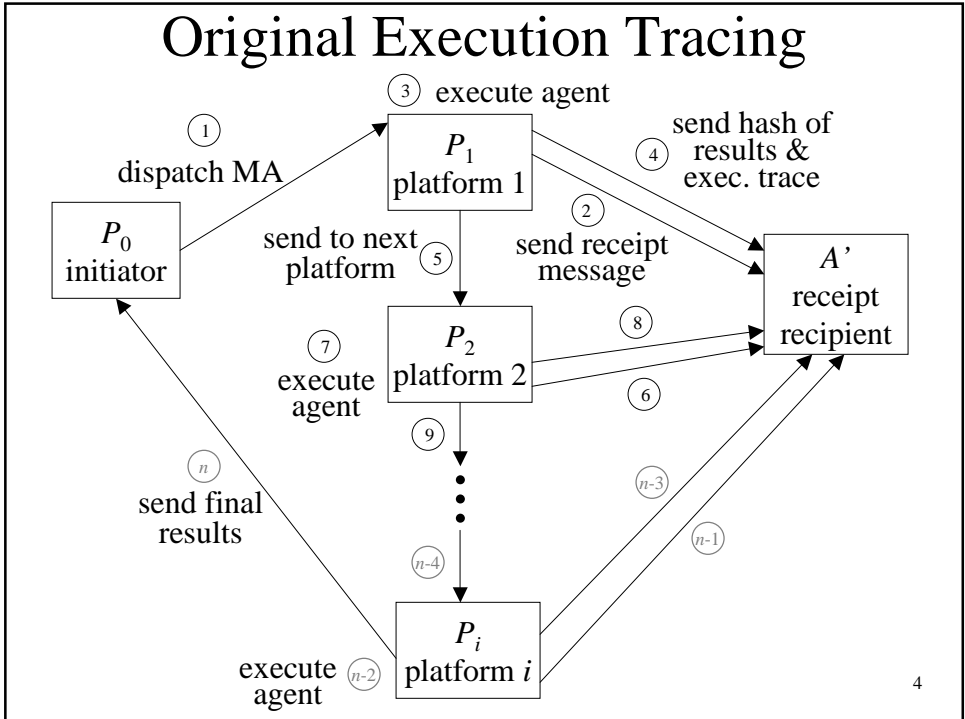
★My Protocol

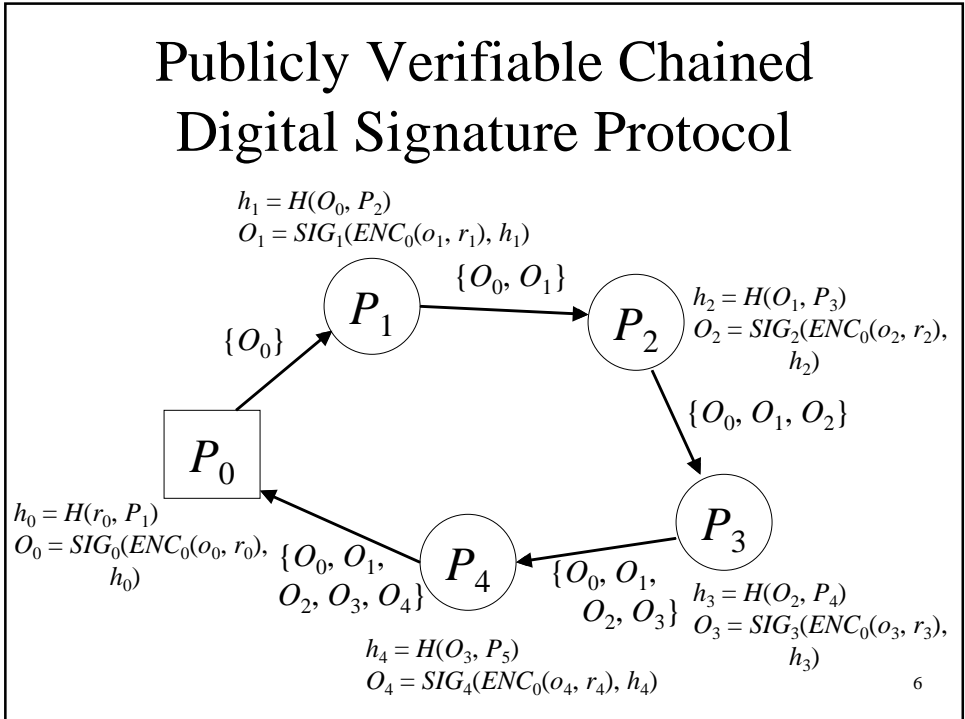
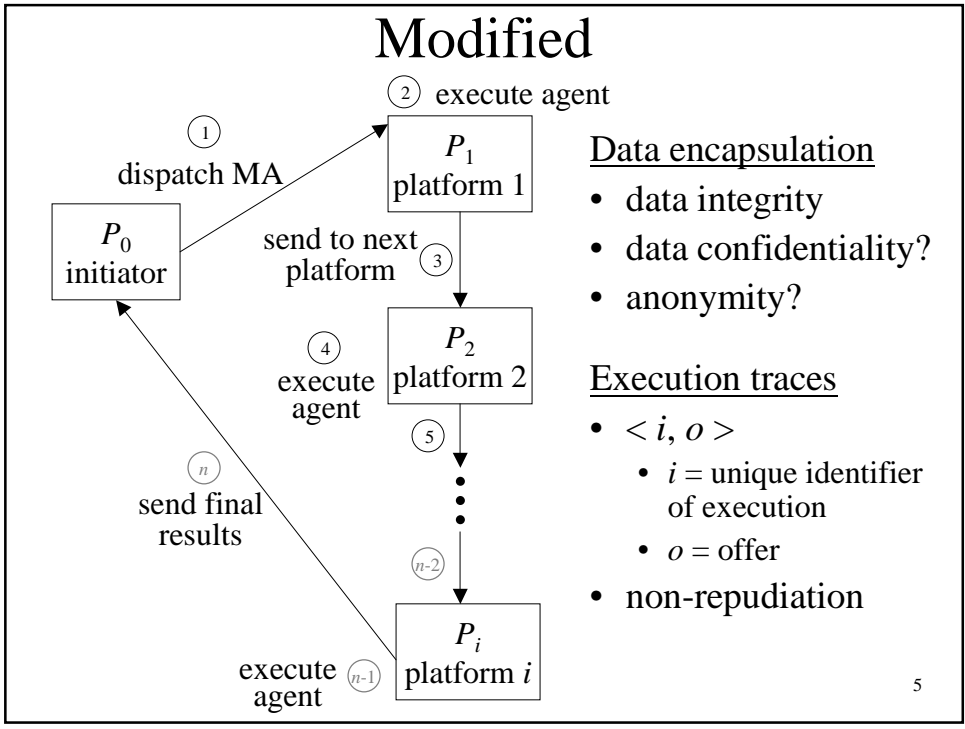
- critique, please!

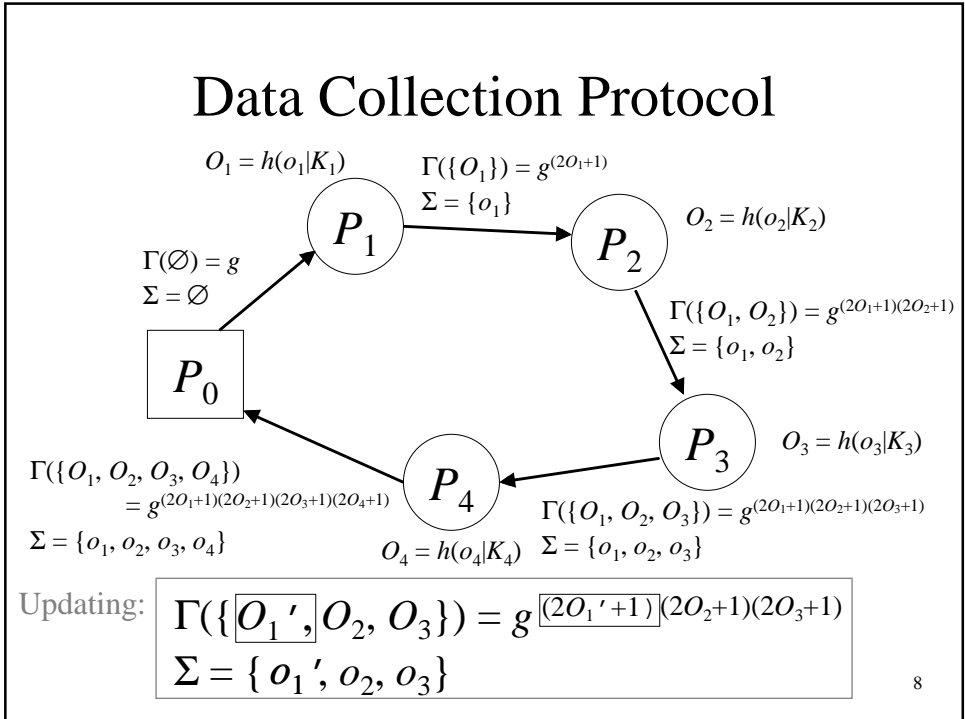
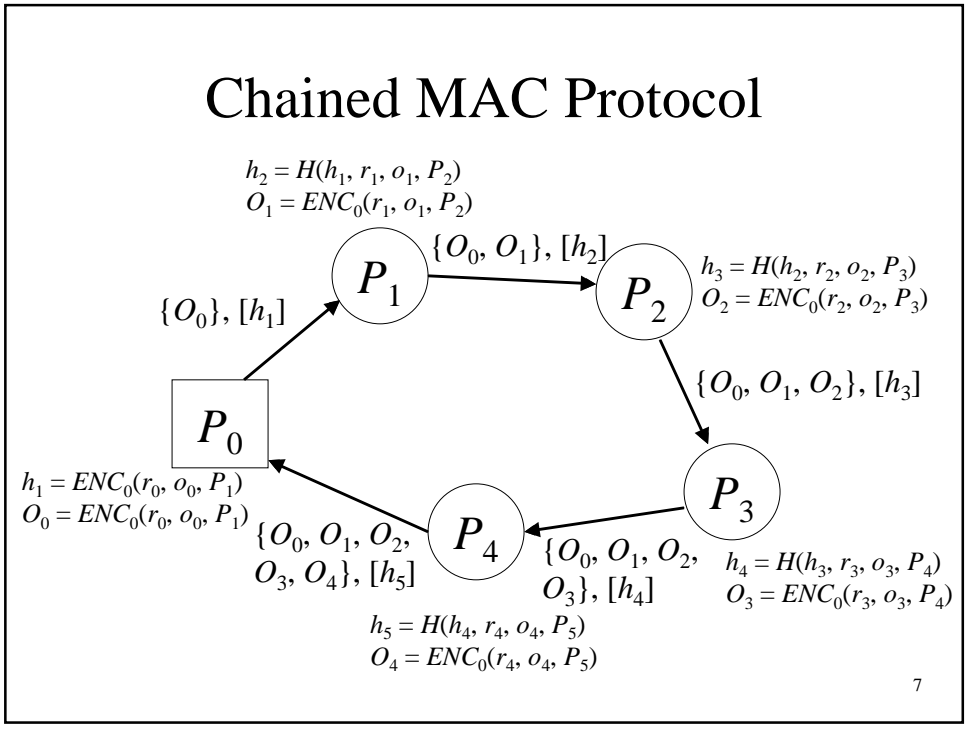
2

Notation

C	Code	
S	State	
P_0	Originator	creator of the mobile agent
$P_{i>0}$	Platform	computational environment for the mobile agent
o_i	Offer	the data that platform P_i submits
O_i	Encapsulated offer	the offer o_i encrypted or hashed together with some other information
H_i	Set hash value	
K_{P_i}	Public key of P_i	
K'_{P_i}	Secret key of P_i	
$ENC_{P_i}(m)$	Encryption	encryption of message m with the public key of P_i
$SIG_{P_i}(m)$	Signature	signing of message m with the secret key of P_i
$h(m)$	Hash	one-way hash of message m
t_{P_i}	Timestamp	the timestamp provided by P_i
i	Identifier	the unique identifier of the mobile agent session ³







Data Encapsulation Summary

★Publicly Verifiable Chained Digital Signature Protocol:

$$- O_i = SIG_{P_i}(ENC_{P_0}(o_i, r_i), h(O_{i-1}, P_{i+1}))$$

★Chained MAC Protocol:

$$- O_i = ENC_{P_0}(r_i, o_i, P_{i+1})$$

★Data Collection Protocol

$$- O_i = h(o_i|K_i)$$

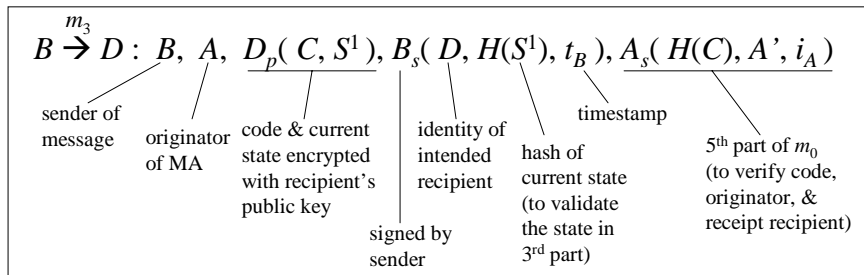
9

B sends the MA to D – what I had

- Original message by Vigna:

$$B \xrightarrow{m_0} D : B, A, D_p(C, S^1), B_s(H(S^1), D), A_s(H(C), H(S^0), B, A', t_A, i_A))$$

- Altered message:



Changes:

- B includes a new timestamp for freshness.
- eliminated extraneous info

10

Protocol I had (with TTP):

- new notation

$P_i \rightarrow P_{i+1}$:

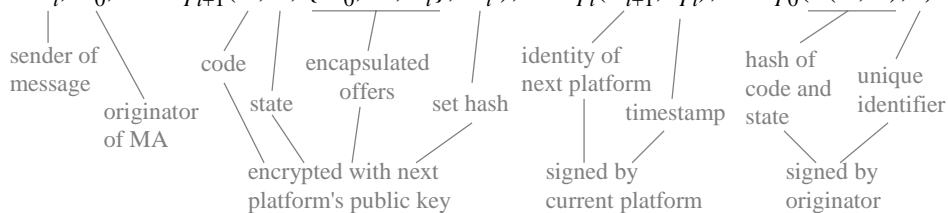
$P_i, P_0, ENC_{P_{i+1}}(C, S), SIG_{P_i}(P_{i+1}, h(S), t_{P_i}), SIG_{P_0}(h(C), P'_0, i_{P_0})$

Protocol I'm working on:

- no TTP
- static state

$P_i \rightarrow P_{i+1}$:

$P_i, P_0, ENC_{P_{i+1}}(C, S, \{O_0, \dots, O_i\}, H_i), SIG_{P_i}(P_{i+1}, t_{P_i}), SIG_{P_0}(h(C, S), i)$



11

My Assumptions

- ★ PKI
- ★ static code & state
- ★ code & state are separate entities
- ★ each platform has a unique identifier
- ★ tamper-proof, non-repudiable execution trace file stored at each platform
- ★ platforms will always provide the correct answer, if it executes the code non-maliciously
- ★ originator always trusted
- ★ no collusion?
- ★ universally controlled timestamp?

12

New Protocol

$P_i \rightarrow P_{i+1}:$

$P_i, P_0, ENC_{P_{i+1}}(C, S, \{O_0, \dots, O_i\}, H_i), SIG_{P_i}(P_{i+1}, t_{P_i}), SIG_{P_0}(h(C, S), i)$

$O_i = h(O_{i-1}, o_i, P_{i+1}, t_{P_i})$
 $O_i = SIG_{P_i}(o_i)$ - anyone can verify offer
 $O_i = ENC_{P_0}(o_i)$ - data is confidential
 $O_i = SIG_{P_i}(P_{i+1}, t_{P_i}, o_i)$
 $O_i = ENC_{P_i}(o_i, O_{i-1}, P_{i+1})$

$H_i = g^{(2O1+1)(2O2+1)\dots(2O_i+1)}$ - set hash of the offers

13

Execution Tracing

- ★ maintained and stored by each platform
- ★ non-repudiable
- ★ $\langle i, o \rangle$
 - i = unique identifier of execution
 - o = offer
- ★ who logs?
 - sender – right before sending
 - receiver – immediately upon receipt
 - both?
 - like sending receipt

14

Conclusion

- ★ Data Encapsulation
 - data integrity
 - data confidentiality
- ★ Chaining
 - only intended recipient can make next offer
- ★ Set Hashing
 - check integrity of set of encapsulated offers
 - updating offer
- ★ Execution Tracing
 - non-repudiation

15

Questions?
Comments?

16

References

- * G. Karjoth, N. Asokan, C. Gulcu. "Protecting the computation results of free-roaming agents." *Proceedings of the Second International Workshop, Mobile Agents 98*. Springer-Verlag Lecture Notes in Computer Science 1477, pages 195-207. Springer, 1998.
- * Sergio Loureiro, Refik Molva, Alain Pannetrat. "Secure Data Collection with Updates." *Electronic Commerce Research Journal*. 1/2: 119-130. February/March 2001.
- * Giovanni Vigna. "Protecting Mobile Agents through Tracing." *Proceedings of the 3rd ECOOP Workshop on Mobile Object Systems*. Jyväskylä, Finland. June 1997.