

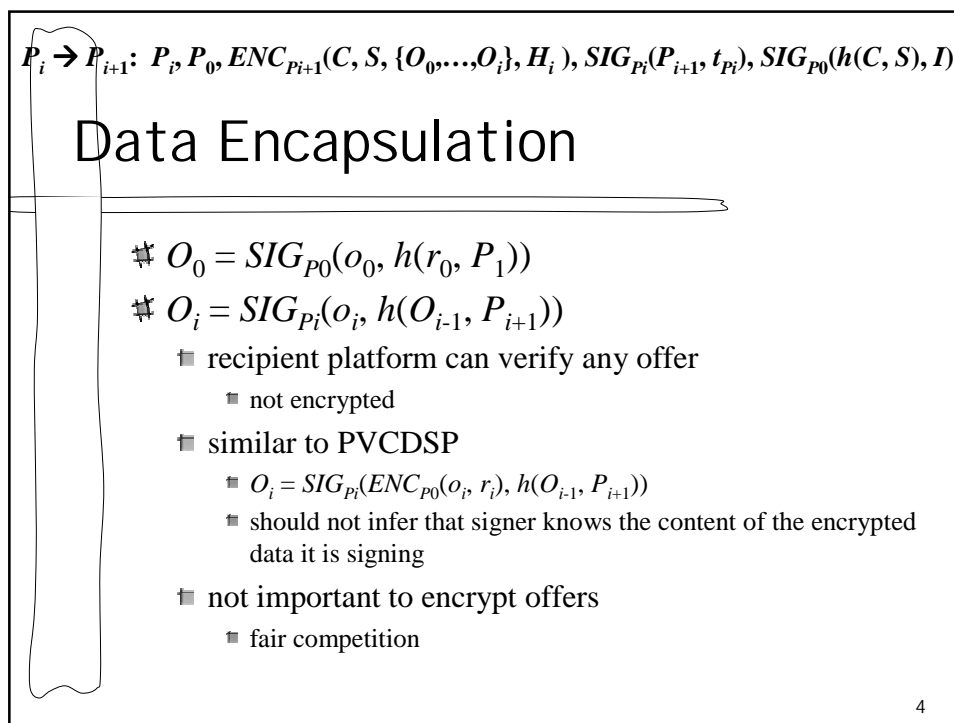
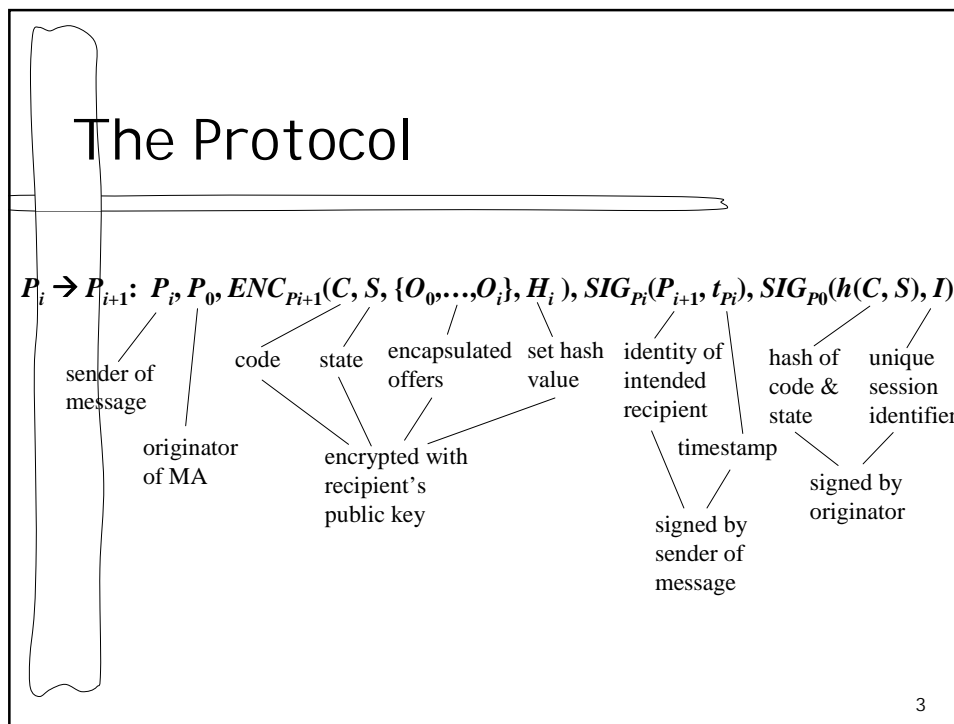
Protecting Mobile Agents with Data Encapsulation and Execution Tracing



Anna Suen
suen@cs.fsu.edu
April 9, 2003

Preview

- # The Protocol
- # Data Encapsulation
- # Set Hashing
- # Other Notes



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

Data Encapsulation

- only originator knows random number
 - only one who can verify the chain
- offers are chained
 - can't delete, replace, or truncate an encapsulated offer

5

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

Set Hashing

- ⌘ use set hashing to verify set of encapsulated offers
- ⌘ updating
 - hard with chaining – can't simply replace an offer
 - no updating
- ⌘ $H_i = g^{(2O_1+1)(2O_2+1)\dots(2O_i+1)}$
 - doesn't work!
 - encapsulated offers are known
 - infeasible to do set hashing with encapsulation?

6

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

Other notes

- # no way to prevent malicious host from
 - replacing originator identity (2nd field) with his own
 - replace encapsulated offers with his own
 - replacing unique session id with his own
 - signing hash of code & state with own signature
- # MA will never return to originator

7

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

Analysis - 1

- # can't change code/state and sign it as his own (and insert collected offers into original message)
 - O_0 is signed by originator
 - signature on O_0 and on last field won't match

8

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

Analysis - 1.5

⚡ Why not just resign O_0 with his own signature?

- ruins the chain
- can't just recompute the entire chain
 - doesn't know who next platform is

P_3
 \downarrow
 $P_3, P_0, ENC_{P_4}(C, S, \{O_0, O_1, O_2, O_3\}, H_3), SIG_{P_3}(P_4, t_3), SIG_{P_0}(h(C, S), I)$
 P_4
 \downarrow
 $P_4, P_4, ENC_{P_5}(C', S', \{O'_0, O_1, O_2, O_3, O_4\}, H_4), SIG_{P_4}(P_5, t_4), SIG_{P_4}(h(C', S'), I)$
 P_5

$O_0 \neq O'_0 = SIG_{P_4}(o_0, h(r_0, P_1))$

9

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

Analysis - 2

⚡ can't replace entire set of encapsulated offers

- O_0 contains a secret random number known only to the originator
- dummy offer

P_3
 \downarrow
 $P_3, P_0, ENC_{P_4}(C, S, \{O_0, O_1, O_2, O_3\}, H_3), SIG_{P_3}(P_4, t_3), SIG_{P_0}(h(C, S), I)$
 P_4
 \downarrow
 $P_4, P_0, ENC_{P_5}(C, S, \{O_4\}, H_4), SIG_{P_4}(P_5, t_4), SIG_{P_0}(h(C, S), I)$
 P_5

$O_0 = SIG_{P_0}(o_0, h(r_0, P_1))$

10

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

Analysis - 3

- # can't truncate
 - 1st field is the identity of the sender
 - 4th field signed by sender
 - these should match signer of last encapsulated offer

11

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

Analysis - 4

- # can't truncate and add own offer
 - breaks chain

12

Conclusion

- # don't need set hashing because the chaining mechanism (and signatures) prevents tampering
- # intermediate platforms can't see other offers because don't know who signed encapsulated offer
 - can't deduce signer from signature
 - only originator can unlock the chain with knowledge of his secret number and first platform
- # no updating

13

Questions? Comments?



14