

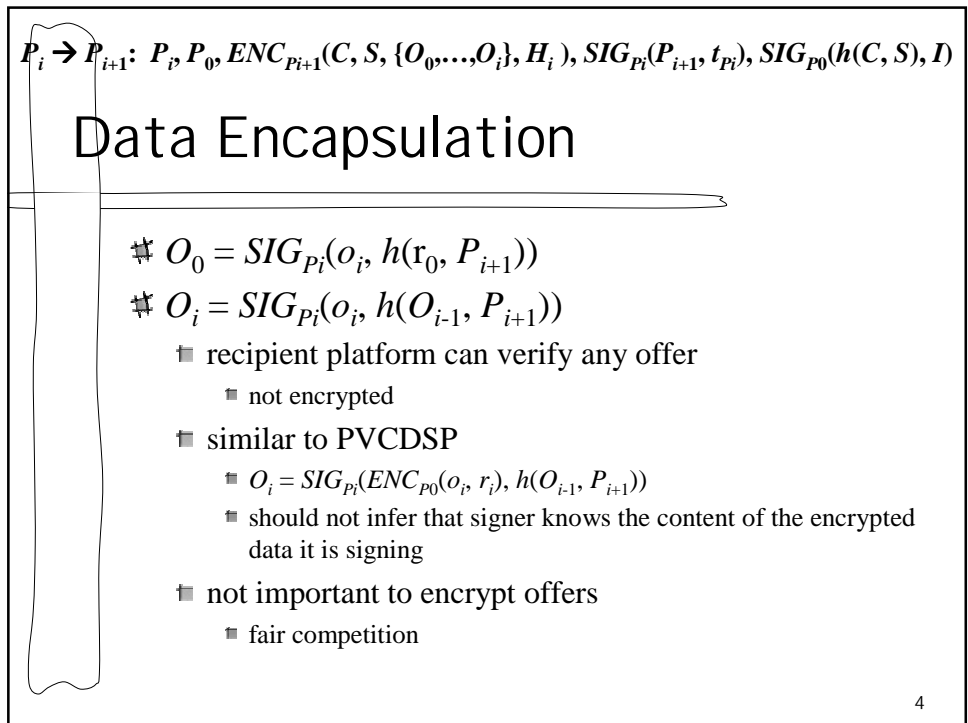
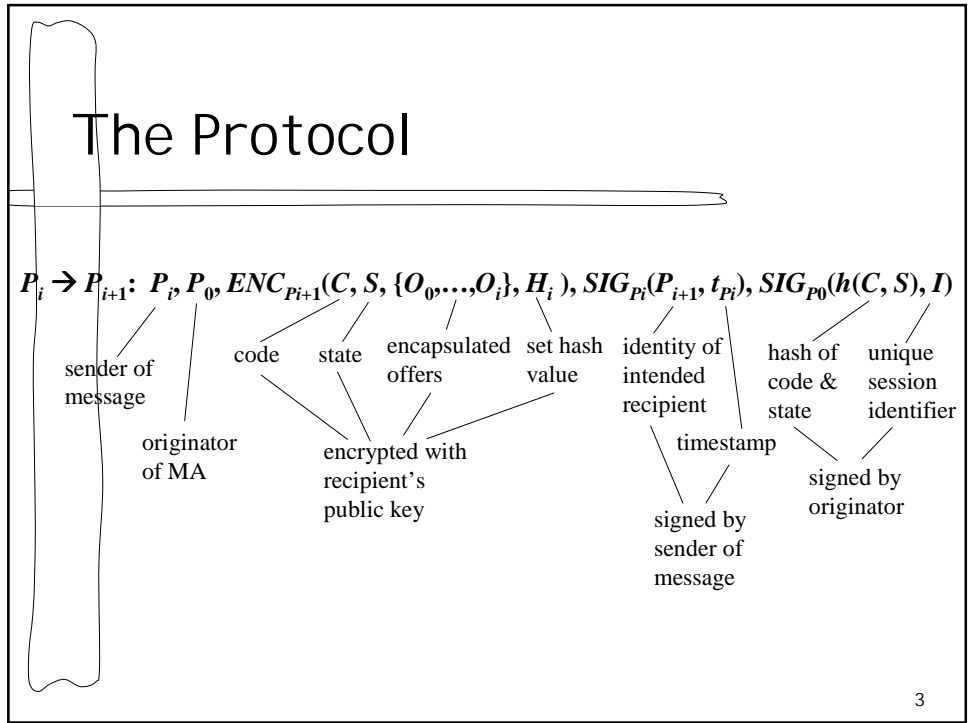
Protecting Mobile Agents with Data Encapsulation and Execution Tracing



Anna Suen
suen@cs.fsu.edu
April 7, 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 or replace an encapsulated offer
 - can truncate

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

Questions? Comments?



8