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
The Protocol

\[ P_i \rightarrow P_{i+1}: P_i, P_0, \text{ENC}_{P_i+1}(C, S, \{O_0, \ldots, O_i\}, H_i), \text{SIG}_{P_i}(P_{i+1}, t_{P_i}), \text{SIG}_{P_0}(h(C, S), I) \]

sender of message

receiver platform can verify any offer

not encrypted

similar to PVCDSP

\[ O_i = \text{SIG}_{P_i}(\text{ENC}_{P_0}(o_i, r), h(O_{i-1}, P_{i+1})) \]

should not infer that signer knows the content of the encrypted data it is signing

not important to encrypt offers

fair competition
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

\[
\begin{align*}
O_{i+1} &= (o_{i+1}, h(O_{i+1}, P_i)) \\
O_i &= (o_i, h(O_{i-1}, P_{i+1})) \\
O_{i-1} &= (o_{i-1}, h(O_{i-2}, P_i))
\end{align*}
\]

Set Hashing

- use set hashing to verify set of encapsulated offers
- updating
  - hard with chaining – can’t simply replace an offer
  - no updating

\[
H_i = g^{(2O_1+1)(2O_2+1)\ldots(2O_{i+1})}
\]

- doesn’t work!
  - encapsulated offers are known
  - infeasible to do set hashing with encapsulation?
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

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
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

$O_0 \neq O'_0 = \text{SIG}_{P_4}(o_0, h(r_{P_4} P_1))$

$O_0 = \text{SIG}_{P_0}(o_0, h(r_{P_1} P_1))$

Can’t replace entire set of encapsulated offers
- $O_0$ contains a secret random number known only to the originator
- dummy offer

$O_0 \neq O'_0 = \text{SIG}_{P_4}(o_0, h(r_{P_4} P_1))$
Protecting Mobile Agents

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

\[ P_i \rightarrow P_{i+1}: P_i, P_0, ENCP_{i+1}(C, S, \{O_0, \ldots, O_i\}, H_i), SIG_{P_i}(P_{i+1}, t_{P_i}), SIG_{P_0}(h(C, S), I) \]

Analysis - 4

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

\[ P_i \rightarrow P_{i+1}: P_i, P_0, ENCP_{i+1}(C, S, \{O_0, \ldots, O_i\}, H_i), SIG_{P_i}(P_{i+1}, t_{P_i}), SIG_{P_0}(h(C, S), I) \]

Anna Suen
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

Questions? Comments?