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
The Protocol

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

sender of message

originator of MA

code

state

encapsulated offers

set hash value

identity of intended recipient

hash of code & state

unique session identifier

timestamp

signed by sender of message

signed by originator

Data Encapsulation

\[ \begin{align*}
& O_0 = SIG_{P_{i}}(o_i, h(r_0, P_{i+1})) \\
& O_i = SIG_{P_{i}}(o_i, h(O_{i-1}, P_{i+1}))
\end{align*} \]

\[ \begin{align*}
& \triangleright \text{recipient platform can verify any offer} \quad \triangleright \text{not encrypted} \\
& \triangleright \text{similar to PVCDSP} \quad \triangleright \text{should not infer that signer knows the content of the encrypted data it is signing} \\
& \triangleright \text{not important to encrypt offers} \quad \triangleright \text{fair competition}
\end{align*} \]
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

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

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_{i+1}(2O_{i+1}) \ldots (2O_{i+1}) \]
  - doesn’t work!
  - encapsulated offers are known
  - infeasible to do set hashing with encapsulation?
Other notes

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

Questions? Comments?