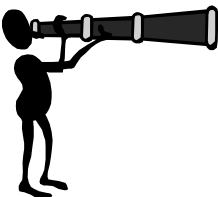


Protecting Mobile Agents

Anna Suen
suen@cs.fsu.edu
January 22, 2003



Preview

- Review:
 - Mobile Agent System Model
 - Types of Attacks
 - Agent Threats
- Techniques for protecting agents

2

Mobile Agent System Model

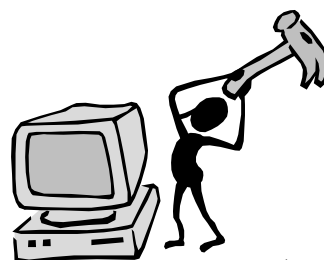
- Agent
 - code and state info needed for some computation
- Agent Platform
 - computational environment
 - Note: platform = server = host



3

Types of Attacks

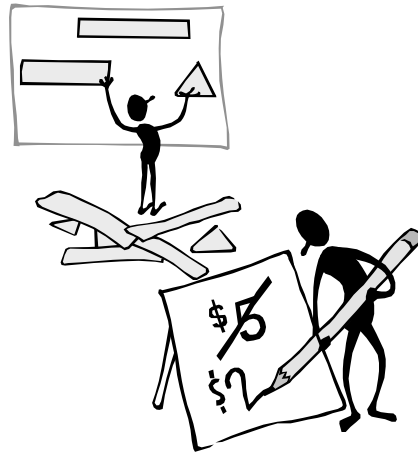
- Agent-to-Platform
- Agent-to-Agent
- Platform-to-Agent
- Other-to-Agent Platform



4

Agent Threats

- Masquerading
- Denial of Service
- Repudiation
- Eavesdropping
- Alteration



5

Prevention vs. Detection

- prevention of tampering is difficult
 - agent completely susceptible to the platform
- detection of tampering instead



6

agent

Simple Techniques

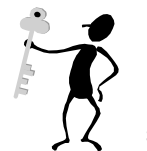
- **Jumping Beans**
 - agent always returns to secure central host before moving to next platform
- **IBM Aglets**
 - trusted network
 - only receive agents that came from a trusted platform
- These not agent systems with free-roaming agents



data

Partial Result Encapsulation

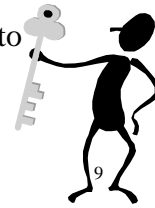
- encapsulate results at each platform visited for later verification
- **Sliding Encryption**
 - agent encrypts data with public key at each platform
 - originator decrypts with private key



data

Partial Result Authentication Code (PRAC)

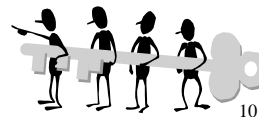
- agent and originator maintain or generate a list of secret keys
- each server:
 - summarizes results in a message
 - uses the secret key to compute an authentication tag (MAC) on the data
- agent/server destroys secret key
 - only originator has a copy of all the secret keys to verify results
- message and MAC sent to originator
 - use to check integrity of data



data

Karjoth, et al

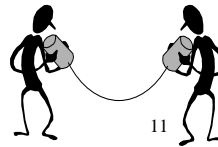
- improvement on PRAC
- server creates an encapsulation that is linked to the result
 - hash chaining
- chain of encapsulations binds each result to all previous results and the identity of the next platform to be visited



agent

Mutual Itinerary Recording

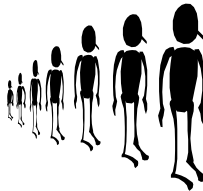
- have a cooperating agent record and track itinerary
- sends to cooperating agent last platform, current platform, and next platform info
 - authenticated channel
- agents avoid visiting platforms already visited by cooperating agent
- can be extended to more than two cooperating agents



agent

Replication and Voting

- send multiple copies of the agent
- a malicious platform may corrupt some of the agents
- enough replicates to successfully complete its task

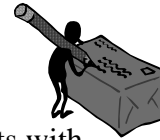


12

agent

Execution Tracing

- platforms maintain a non-repudiatable trace (log) of agent's operations
 - send receipt message to designated recipient
 - execute agent and produce corresponding trace
 - send designated recipient
 - hash of final state
 - hash of execution trace
 - send final state to originator
- if suspect tampering
 - ask for execution traces and receipts
 - simulate the agent execution and compare results with traces and receipts



13

agent

Environmental Key Generation

- allows agent to take predefined action when some environmental condition is true
- when agent encounters an environmental condition a key is generated
 - use key to unlock executable code
- environmental condition is hidden



14

agent

Computing with Encrypted Functions

- platform execute a program with an embedded function without revealing the original function



15

agent

Obfuscated Code

- scrambled code
 - no one can completely understand the function
 - cannot modify resulting code without detection

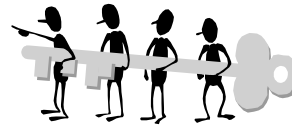


16

data

Data Collection Protocol

- shared key between originator and each server
- each server computes an integrity proof value and integrates it into the overall integrity proof value
 - set hashing: method to hash together a set of data blocks in an order-independent fashion
- agent returns to originator:
 - set of collected data
 - overall integrity proof value
- originator verifies integrity of data with overall integrity proof value

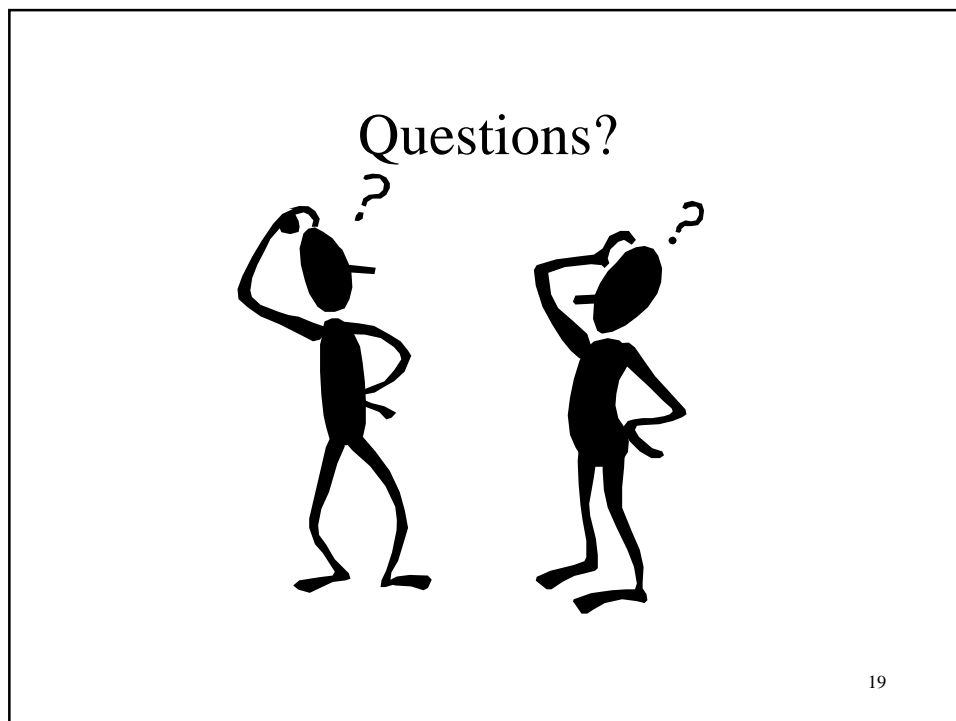



17




- Partial Result Encapsulation
- Mutual Itinerary Recording
- Replication and Voting
- Execution Tracing
- Environmental Key Generation
- Computing with Encrypted Functions
- Obfuscated Code
- Data Collection Protocol

18






References



- Wayne Jansen & Tom Karygiannis. "Mobile Agent Security." NIST Special Publication 800-19. September 1999.
- G. Karjoh, N. Asokan, and C. Gulcu. "Protecting the Computation Results of Free-roaming Agents." Lecture Notes in Computer Science 1477, pgs 195-207. 1998.
- Sergio Loureiro, Refik Molva, and Alain Pannetrat. "Secure Data Collection with Updates." Electronic Commerce Research Journal. Vol 1, No 2. February/March 2001.
- Giovanni Vigna. "Protecting Mobile Agents through Tracing." Proceedings of the 3rd ECOOP Workshop on Mobile Object Systems. Jyväskylä, Finland. June 1997.
- Bennet S. Yee. "A Sanctuary for Mobile Agents." UC San Diego, Department of Computer Science and Engineering. April 28, 1997.



20