

Mobile Agent Security

NIST Special Publication 800-19 (August 1999)
Wayne Jansen & Tom Karygiannis
<http://csrc.nist.gov/mobileagents/publication/sp800-19.pdf>

26 February 2002

John Marshall

1

Quotes of the day

Nobody will ever win the battle of the sexes.
There's too much fraternizing with the enemy.
-Henry Kissinger

Put-down:

I like you, but I wouldn't want to see you working
with subatomic particles.
-unknown

26 February 2002

John Marshall

2

From Last Time

- Tactical ad hoc networks
- Issues
- Proposed solution

26 February 2002

John Marshall

3

Tactical ad hoc networks

- Mobile nodes
- Joint mission
- Group communication

26 February 2002

John Marshall

4

Issues

- Group connectivity
- Routing
- Secure communication

26 February 2002

John Marshall

5

Proposed Solution

Mobile Agents

- autonomous
- work on someone's behalf
- well-defined mission
- self-propagating

Trade-offs with security

26 February 2002

John Marshall

6

Taxonomy of Mobile Agent Security

- Protecting agent platform
- Protecting agent

26 February 2002

John Marshall

7

Protecting Agent Platform

- Isolation
- Safe code
- Authenticated code
- Path history

26 February 2002

John Marshall

8

Isolation

- Protect platform from agents
- Protect agents from each other
- Idea of isolated, trusted domains
- “Sandboxing” with virtual address space

26 February 2002

John Marshall

9

Safe Code

- Interpreted language implementation (eg. Java)
- Mobility
- “Harmful” commands denied to agents
- Implementation dependent (not built-in)

26 February 2002

John Marshall

10

Authenticated Code

- Digital signatures
- Provides authorship & integrity
- No guarantee of fault-free execution

26 February 2002

John Marshall

11

Path History

- Platforms visited
- Resource constraints* (eg. CPU utilization)
- Path entry integrity

* Pandey, Hashii & Lal. “Secure Execution of Mobile Programs.” *Proc. of DISCEX (1) 2000*: pp 362-76

26 February 2002

John Marshall

12

Taxonomy of Mobile Agent Security

- Protecting agent platform
- Protecting agent

26 February 2002

John Marshall

13

Protecting Agent

- Partial result encapsulation
- Replicate agents & voting
- Execution trace
- Environmental key generation

26 February 2002

John Marshall

14

Partial Result Encapsulation

- Protect agent's actions at platform for future verification
- Who performs encapsulation?
- How results encapsulated?
- Who verifies?

26 February 2002

John Marshall

15

Replicate Agents & Voting

- Multiple agent copies
- Independent paths
- Increased likelihood one will reach destination by avoiding encounter with malicious platform
- Assumes few malicious platforms

26 February 2002

John Marshall

16

Execution Trace

- Log of agent behavior on platform
- Hashed—fingerprint
- Size & number of logs problematic

26 February 2002

John Marshall

17

Environmental Key Generation

- Trigger event when environmental condition holds
- Key generated to unlock portion of code
- Assumes platform cannot uncover triggering message from agent's code (eg. hashed)
- Platform may restrict agent from dynamically creating code (viewed as malicious)

26 February 2002

John Marshall

18

Mobile Agent Applications

- Work on someone's behalf (delegation)
- Network management
 - adaptive response to network events
- PDAs
 - off-line operation

26 February 2002

John Marshall

19

Further Considerations for Tactical Ad Hoc Networks

- Downward scalability
- Group management
- Next time: routing

Broch, Maltz, Johnson, Hu & Jetcheva. "A performance comparison of multi-hop wireless ad hoc network routing protocols." *Proc. of the 4th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98)*, October 25-30, 1998, Dallas, TX.

26 February 2002

John Marshall

20