

Mobile Agent Security

3 September 2002

John Marshall

1

Quote of the day

“I have never let my schooling interfere with my education.”

-Mark Twain

3 September 2002

John Marshall

2

Research Interests

- Mobile ad hoc networks
- Mobile agent security

3 September 2002

John Marshall

3

Topics of Discussion

- Ad hoc networks
- Mobile agents & their applications
- Protecting agents

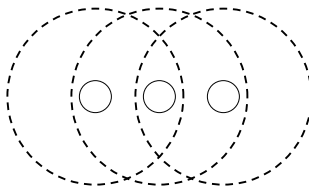
3 September 2002

John Marshall

4

Mobile Ad Hoc NETWORKS

- MANET – “infrastructure-less”
- Transmission range
- Group coordination – routing



3 September 2002

John Marshall

5

Tactical ad hoc networks

- Joint mission
- Group communication

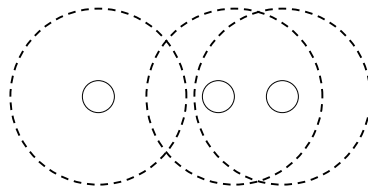
3 September 2002

John Marshall

6

Problem

- Recall, nodes are mobile
- What happens if...



3 September 2002

John Marshall

7

Issues

- Group connectivity
- Routing
- Secure communication

3 September 2002

John Marshall

8

Possible Solution

Mobile Agents

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

Trade-offs with security

3 September 2002

John Marshall

9

Other Mobile Agent Applications

- Stock-watcher
- Travel agent
- Network manager – respond to changes in network behavior
- PDAs – off-line operation

3 September 2002

John Marshall

10

Taxonomy of Mobile Agent Security

- Protecting agent platform
- Protecting agent

NIST Special Publication 800-19 (August 1999)

Wayne Jansen & Tom Karygiannis

<http://csrc.nist.gov/mobileagents/publication/sp800-19.pdf>

3 September 2002

John Marshall

11

Protecting Agent Platform

Similar to mechanisms used to thwart
malicious code (e.g. viruses):

- Isolation
- Detection
- Authenticated code

3 September 2002

John Marshall

12

Protecting Agent

“Towards Mobile Cryptography”

T. Sander & C.F. Tschudin (1998)

*Proceedings of the IEEE Symposium on
Security & Privacy: 215-224*

3 September 2002

John Marshall

13

Mobile Agents Revisited

- Mobile code
- Agent decides when & where to go
- Untrusted computing base
- Focus on non-interactivity

3 September 2002

John Marshall

14

Requirements for Agent Security

1. Code & execution integrity
2. Computing with secrets in public
3. Code privacy

3 September 2002

John Marshall

15

A Start...

Move away from cleartext code & data

“In the same sense that you can communicate some ciphmessage to another party without understanding it, we would like a computer to execute a cipherprogram without understanding it.”

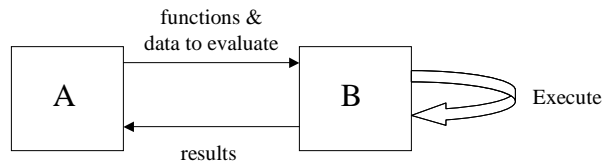
-Authors

3 September 2002

John Marshall

16

Ideal System



Goals:

1. Non-interactive evaluation
2. Minimal information leakage

3 September 2002

John Marshall

17

Whetting your mathematical appetite...

Execute $y = P(x)$

Compute the signature $z = S(y)$

Output the pair (y, z)

3 September 2002

John Marshall

18

Solution

Composition of functions

$$h := s \circ f$$

Execute $y = P(x)$

Compute the signature $z = H(x)$

Output the pair (y, z)

Problems Still Un-addressed

- Complexities introduced by self-propagation