

Using Detection Objects to Detect Attacks on Mobile Agents

Anna Suen
suen@cs.fsu.edu

October 17, 2002

Preview

- Mobile Agents
- Security
- Detection Objects
- Example
- Problems with Detection Objects
- My thoughts & ideas...thesis?

2

Mobile Agents

- program instances (or processes)
- capable of moving within the network under their own control

3

Mobile Agents - Security

- Two aspects:
 - protect host systems from attacks by mobile agents
 - protect mobile agents from attacks by host systems
 - detection objects

4

Detection Objects

- dummy data items
 - not modified by agent or host system
- if not modified, then can be confident that legitimate data are not corrupted
- agent and host systems must not be aware of detection objects

5

Example

- agent's mission
 - to query various databases to find the cheapest flight from A to B
 - rank the flights by price
- a dummy flight is stored in its database
- after agent returns
 - search through list to see if the dummy flight was modified

6

Problems with D.O.

- very application-specific
 - d.o. that works for one type of query may not work for another
- need to update d.o. often
 - so can't guess which is the d.o. by comparing the results of several queries over time

7

Problems with D.O.

- need to pay attention to the construction of queries and objects
 - query needs to return the detection object
 - flight example...
- d.o. must be plausible enough to fool host systems, but not so plausible that it affects the results of the query

8

Problems with D.O.

- not applicable to all types of queries
 - could be useful for repeated queries
 - worthwhile to determine the best way to generate detection objects

9

Thesis Ideas...

- *using detection objects to protect data on an agent collecting data from various host systems*
 - apply only to mobile agents that have a database
- to determine what the most suitable query type is
- detection objects can be used for both the mobile agent and host system to detect attacks

10

My Thoughts

- Why does the query need to return the detection object?
 - Why not just take the result and store it in the database?
- Should encrypt the database?
 - so host systems can't steal the data and use it to their own advantage

11

Questions?



12

References

- Hohl, Fritz. "Mobile Agents and Active Networks."
- Meadows, Catherine. "Detecting Attacks on Mobile Agents."
- Sander, Tomas & Tschudin, Christian F. "Protecting Mobile Agents Against Malicious Hosts."