Software agents role for privacy and security in oppnets

Project #3
15 min. introduction presented on Sept. 28, 2006

CS6910 – Advanced Computer and Information Security (ACIS)
Fall 2006
Department of Computer Science
Western Michigan University
Instructor: Prof. Leszek T. Lilien

Group:
- Nitin Bhargava
- Harish Reddy Ravi
- Vinod Talati
Software agents

- A software agent is a piece of computer software which autonomously makes partial or complete decisions on behalf of the user.
- Many individual communicative software agents may form a multi-agent system.
Types of Software agents

- **Intelligent agents**
  - Ability to adapt and learn

- **Autonomous agents**
  - Self-contained and Independent

- **Distributed agents**
  - Multiple agent system

- **Mobile agents**
  - Agent code that moves itself to other nodes to execute

- **Fuzzy agents**
  - Software agent that implements fuzzy logic.
Examples of agents

- Buyer agents (shopping bots) ➔ Amazon.com or eBay
- Mail transfer agent ➔ For serving E-mail, such as Microsoft Outlook
- Data mining agents
Network of agents

Source: http://www.ercim.org/publication/
Possible issues with Software Agents

Security
- mobile agents

Privacy
- user data and information
Mobile Code- Security problem

- Damage to the host file system
- Excessive use of host resources e.g. cpu time and memory usage.
- Leakage of private information belonging to the hosts established users
- Can get access to the company intranet on which host is running.
How to establish trust?

- Through security policies
  - Applying security policies in open agent systems.
  - Agents should not pass the information inappropriately. They need to share and forward the correct information.
  - Agents acting for other parties will only share the necessary information.
How to establish trust?

- **Trust and reputation model.**
  - Reputation history can help in assessing the past behaviour of particular agents or users, prevent trusting on untrustworthy agents.
  - All the members in an open agent system should follow a set of rules.
  - Agents not following the rules should be blacklisted.
  - Contracts should be applied between several parties to represent and enforce agreements.

- **Users should be final authority.**
Privacy in Oppnets

- Privacy can be preserved using:
  - Encryption
  - Privacy Enhancing Technologies
Encryption

- Encryption is used to protect information stored on a host or host to host communication.
- prevent unauthorized access to communications, files, and computers.
- by preventing access it also has the effect of helping to protect privacy.
- Its not sufficient by itself.
Role of Current PET’s

- Preventing unauthorized access to communications and stored files.
- Filtering unwanted messages.
- Preventing automated data capture.
- Facilitating transactions that reveal minimal personal information.
P3P: Platform for Privacy Preferences

- Developed by World Wide Web Consortium
- Usage:
  - Users declare their privacy policy on their browsers
  - Websites register their policy with Security agencies
  - The website policy is compared with user policy and the browser makes automated decisions
- Benefits:
  - Might help uncover privacy gaps for websites
  - Can block cookies or prevent access to some sites
- Built into IE 6.0 and Netscape 7 as of July 2002
Security in Oppnets

- Security can be achieved using:
  - Cryptographic key exchange
  - Proof carrying code
    - Agent code is self contained
    - Hosts can verify agent using pre programmed information built into code
Security: Key exchange

- Host A wants to allow B to run code M
- M wants to access network resources, make contact for emergencies etc
- Simple model: A trusts B unconditionally
- A and B exchange cryptographic keys securely
- So A needs to only check B’s signature by obtaining B’s public key
Security: key exchange

- Complex model:
  - A wants to allow multiple host access.
  - Delegate cryptographic key exchange to third party: “reputation server”.
  - C provides valid public key for B to run M on A.
Security: PCC (Proof Carrying Code)

- Agents author may not be known to some or all hosts
- So use Proof Carrying Code (PCC)
- Proof enclosed with the mobile programs making them self contained allowing mobility.
Security: PCC

- For this to work each host must have common set of security properties for agents.
- Agents can then be checked by each host.
- This is not feasible on an exhaustive set of safety properties.
- Use trusted third party and delegate task of verifying agent with PCC.
PCC requirements

- Hosts rely heavily on trusted third parties.
- Creators of agents must rely on them too.
References

- Image from http://www.ercim.org/publication/Ercim_News/enw59/
  - Accessed on sept. 26th 2006

  - Available at: http://www.iis.ee.ic.ac.uk/~alfebiite/Documents/Public%20Documents/Related%20Work/oasocandnames.pdf#search=%22open%20agent%20society%22

  - Available at: http://citeseer.ist.psu.edu/feigenbaum97trust.html