Secure Agents

Patrick Lincoln and Carolyn Talcott
SRI International

HCSS 1-3 April 2003

The Team

Pat Lincoln

Drew Dean

Jon Millen

Vitaly Shmatikov

Carolyn Talcott

Project overview in a nutshell

- past/present/future access control
- tracking mobile agents
- privacy models
- semantic framework

Challenges for secure agents

- mobility of computation, agents, and devices
- agent autonomy
- heterogeneous communication media
  - wired and wireless connections
  - dynamic (possibly virtual) network topology
- heterogeneous goals
  - multipolar security domains
  - stakeholders with diverse goals and concerns
  - federations, collaboration, information sharing

Framework Objectives

- Specify and analyze
  - secure agent architectures
  - secure agent systems

- Represent and reason about
  - information transformation and flow
  - stealth, privacy, anonymity
  - security goals, policies, enforcement mechanisms
  - relationships across domains

Secure agent system model

Elements

- Nodes (hosts) --- possibly mobile
- Communication media (networks)
- Agents --- possibly mobile
- Messages

Nodes

- Exist in a communication environment
- Encapsulate and manage a set of resources
  - runtime, communication, directories, data storage ...
- Provide services to access the resources
  - execution environment
  - communication
  - brokers
- Service availability/quality may depend on location or state of communication environment

Agents

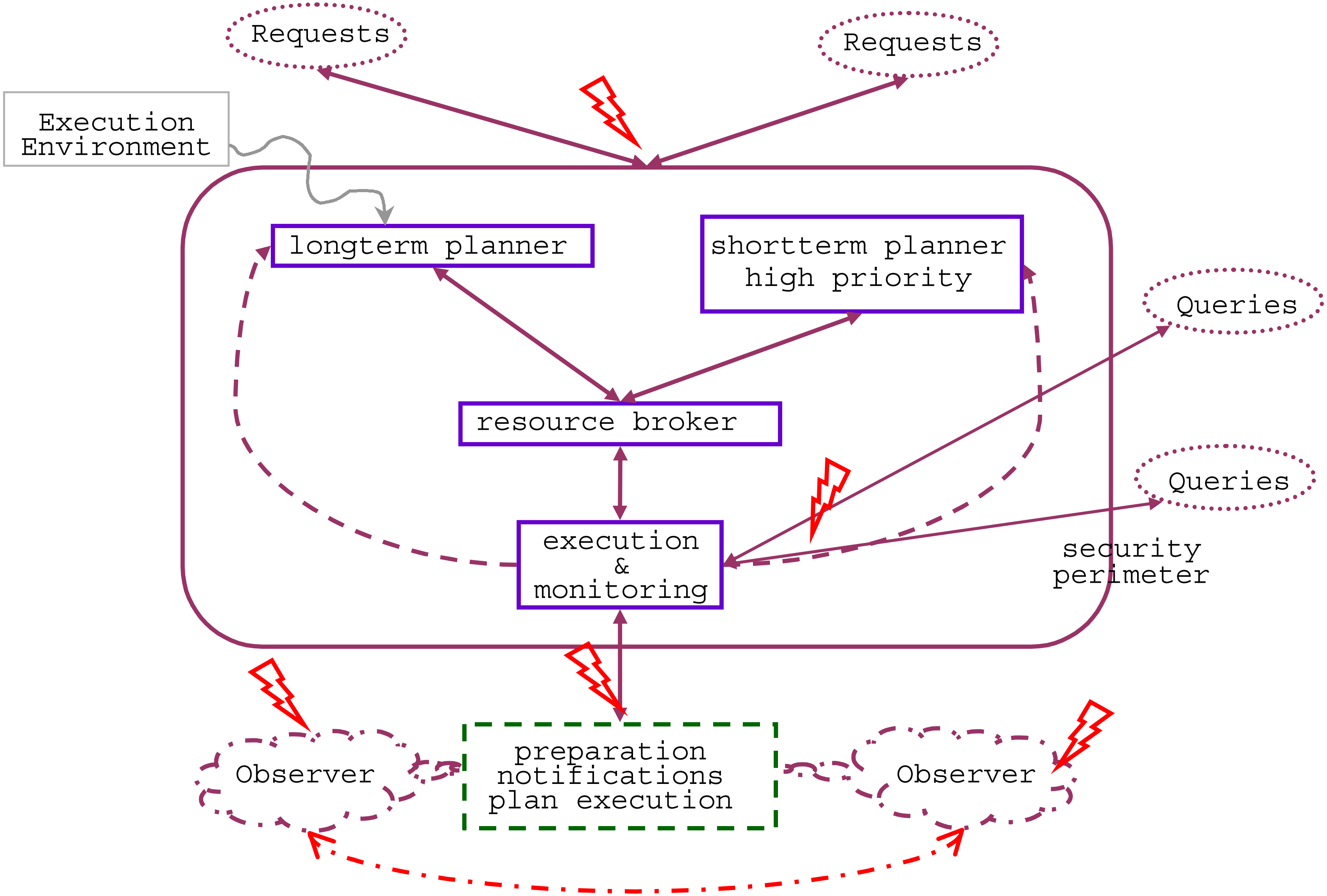
- Execute on nodes within an execution environment
- Move through the communication media
- Generate and transmit information
- Are subject to access control---what, how much/often
- Modeled by traces of service calls (event system)

Reasoning

- Executable models (Maude)
  - agent behaviors
  - hostile environments
  - mechanisms for control, detection, and protection
- Multi-view specification
  - end-to-end ---principals, goals, messages -- event trace sets
  - system-wide---resources, access, network -- state transition
  - local behavior---agents, node-level services
    - rewrite rules, service call traces
- Justify Coherency
  - mapping between views
  - conditions for S to imply S'

Plan/Execute/Monitor Example

(MAC)



Plan+Execute+Monitor Architecture

Security Issues I

- Validity of monitoring data
- What damage could bad data cause
  - aborted/revoked plans, physical damage

- Are negotiated permissions (access to external resources) trustworthy?
- What happens if a schedule is based on false assumptions regarding such permissions?

- Who should be allowed to make what queries?

Security Issues II

- What can external observers learn?
  - combining information about permissions given by different resource controllers
  - from permissions denied
  - observing activities -- from multiple points
- To what extent are planning and resource allocation strategies known to external agents?
- Can adversary manipulate overall resource assignments to prevent a task from being carried out?

Security Issues III

- Sometimes it is essential to share information
  - the FAA has to be told flight plans
  - permission must be negotiated to fly through foreign airspace
- How much and when?
- How can the resource broker/scheduler select distribution of external resources and usage dependancy to support delayed release of time sensitive information?
- How can such properties be specified and checked?

Infosphere (JBI) Example

The right information
to the right person
at the right time

Information management

Repositories of

- information objects
- metadata schema
- information policies
- information transformers

Interaction model

- publish
- subscribe/notify
- query/retrieve

Information sources (publishers)

- Remote sensors or observers
- Weather stations
- External data repositories
    - inventories
    - intelligence
- Data analysis systems
- Approved users
- Fuselets
    - transform published information objects
    - monitor and publish alerts,
    - assemble and publish reports

Infosphere Security Challenges

- Sensitive Information
  - capabilities, plans, intelligence
- Sharing
  - collaboration
  - coalitions
- Information validation
  - source
  - processing

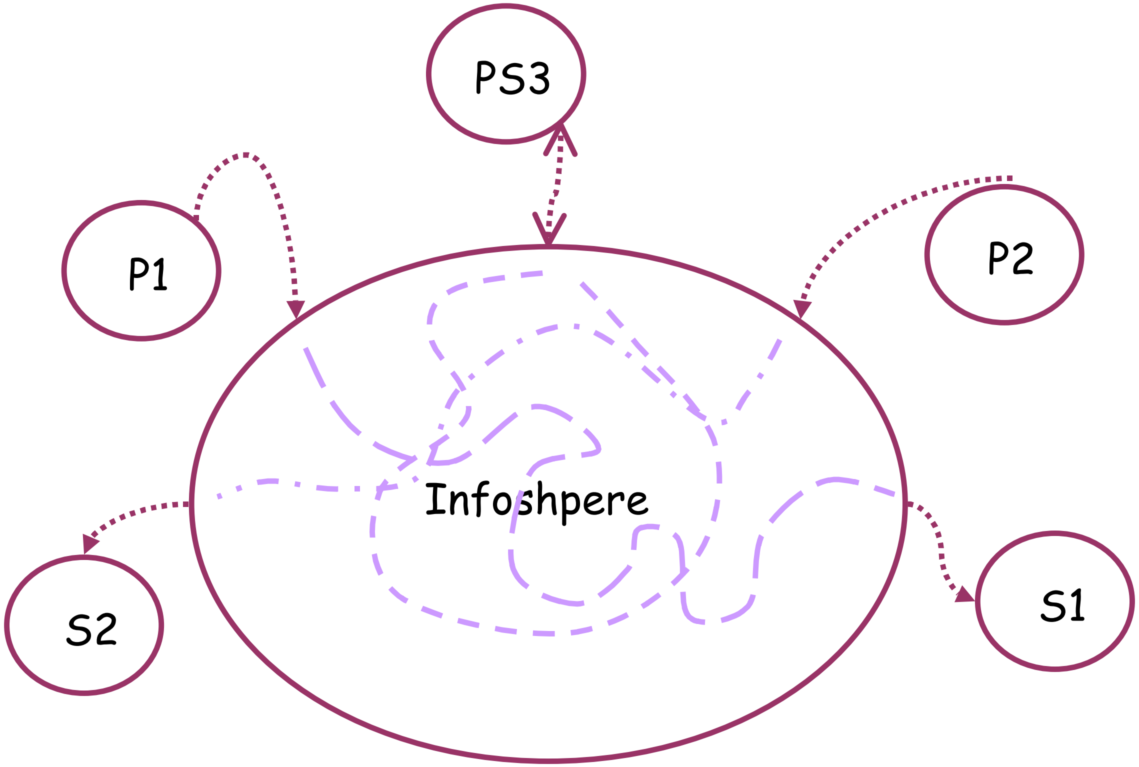
Infosphere

Specification Views

Infosphere end-2-end view

- External Agents -- authenticated clients
- Infosphere is black box / murky pool
- Semantic model -- sets of interaction traces
  - publish, subscribe, query, notify, and retrieve events.

Infosphere end-2-end view



Infosphere end-2-end requirements

- Classify events according to information object

- Specify information flow requirements using closure conditions on trace sets (ala Mantel)

- Example: information must not flow from domain d to domain d' means that if we omit d events, then the resulting trace is also a possible behavior.

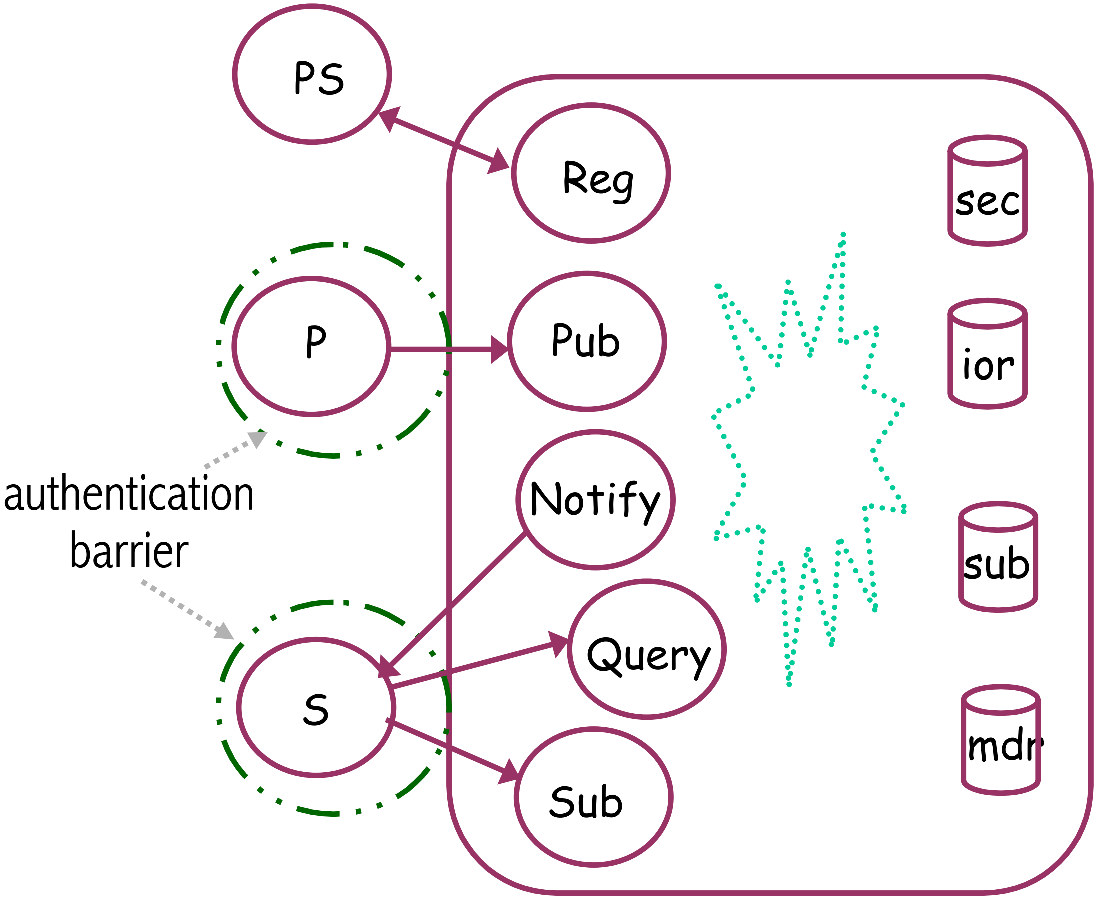
Infosphere system view

- System state -- data repositories:
  - security policy rules---access control, trust management, ...
  - information objects repository
  - metadata schemas
  - subscriptions

- Services
  - interaction -- publish, subscribe, query
  - notification service -- interaction helper
  - registration service (agent admission control)

- Authentication barrier
  - remote execution environment

Infosphere system view



Infosphere system requirements

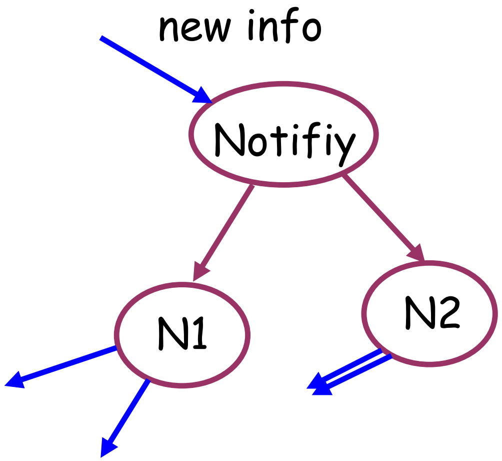
Require:

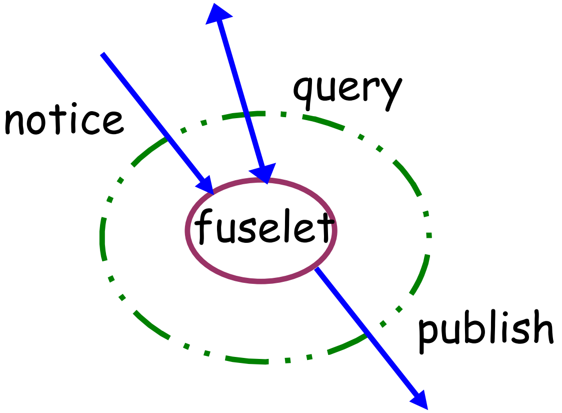
- security policy rules ensure end-to-end requirements
- admitted client service requests obey security policy
- ...

Show:

- satisfaction of system requirements implies that end-to-end information flow requirements are met.

Infosphere behavior fragments





Infosphere: a notification behavior

Rules

- classify subscriptions
  - group subscriptions
  - high sensitivity subscriptions
  - ...
- delegate notification to class specific helpers

Requirements:

- group join for a particular group subscription constrained to enforce the security policy.
- additional authentication and information protection for sensitive information subcriptions

Infosphere: fuselet behavior

- Specify
  - Subscription
  - Rules for information transformation
    - may involve additional queries
  - Information flow properties
- Show rules imply specified flow properties

- Execution environment controls
  - queries and publications
  - access to runtime resources

Show combined behaviors meet system requirements!!

- under suitable conditions

Whither Next

- Devil is in the details
  - what are the right security domains
  - what information flow policies are appropriate
  - composing properties and/or domains
  - effects of transformation

- What is information?

- Modeling temporal aspects
  - value of information depends on time / past future events

- Disinformation?   Stealth?