Intrusion Detection in the Large:
Distributed Detection of Distributed Attacks

Douglas B. Moran
Artificial In telligencc Center
SRI International
moran@ai.sri.com
http://www.ai.sri.com/~moran/

Distributed Attacks

- **Distributed Target**
  - Distributed System
    - Distributed File System
    - Database
    - Agent Systems
  - Shared privilege
- **Distributed Source**
- **Distributed over time**
- **Data Fusion Problem**
  - Loose clusters
  - Massive overlap
  - No hierarchy: flexible & dynamic organizations
    - task force
    - business process re-engineering
    - out-sourcing
- **Task Model**
- **Human Factors**

Distributed Detection

- **Partial Evidence per Intrusion**
- **Merge Evidence from Multiple Sites**
  - Matching incidents
  - Reliability/Competence of reporter
  - Terminological and procedural uncertainty and inconsistency
- **Sites Under Attack Directly Communicate**
- **Reporting Problems**
  - Confidentiality/Sanitize
  - Security
  - Feedback to cracker
  - Under-reporting

Improved Reporting

- Create Automated Security Manual (shortage of human expertise)
- Catalogue of Known Intrusion Scenarios and Techniques
  - Confidentiality issue
- Customizable to Site
  - Better diagnosis
  - Reduced consistency

Goals of Project:

- Short-term Goal
  - Improved diagnosis
  - Assisted recovery
- Long-term Goal
  - Automated report generation
  - Multilevel reports
    - trustworthiness of recipient
    - current situation

AI Technology

- Reactive (PRS)
  - Event driven
  - Automated manual
  - Short horizon
- Look-ahead Planner (SIPE)
  - resource usage
  - info retrieval conflicts
- Common Representation Formalism
- Each Domain Requires its own Extensions and Customizations
- Intelligent, Adaptive Scheduler of Tasks (threads)

SRI International
AI Center

PRS-CL
A Procedural Reasoning Reactive Execution System

TECHNOLOGY

- Reasoning based upon predefined procedural knowledge
- Reactive and goal driven
- Real-time response
- Meta-level reasoning
- Multiple cooperating agents
- Interactive, menu-driven, graphical interface

APPLICATIONS

- Space shuttle fault diagnosis
- Aircraft maintenance
- Air battle management
- Mobile robot control
- Communications network management
- Joint military operations
- Sonobuoy deployment

Design Issues

- Phased Response
  - Are there dependable cues
  - Limit: avoid becoming denial-of-service (computer or human)
- Building up Catalogue of Attack Scenarios
  - Reuse of attack components
  - Ease of specifying
- Ability to Identify
  - Variants
  - New attacks using some known components
- Distributed Attack in small Cluster of Computers
- Single Platform Type

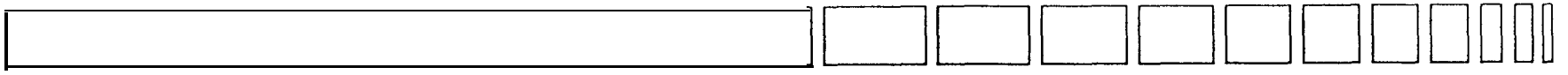
Scaling-Up

- Filtering and Routing Info
  - Little relevant structure in network
  - Trust vs. need-to-know
- Incomplete Info
  - Too little for meaningful report
    - request info from “authorities”
    - reanalyze
  - Enough to report
    - clearing house
    - involved hosts
    - siblings

Thresholds for above??

- Automatic Processing of Reports
- Determine what can reasonably be shared with whom

User in Loop vs. Uses at end of a pipe



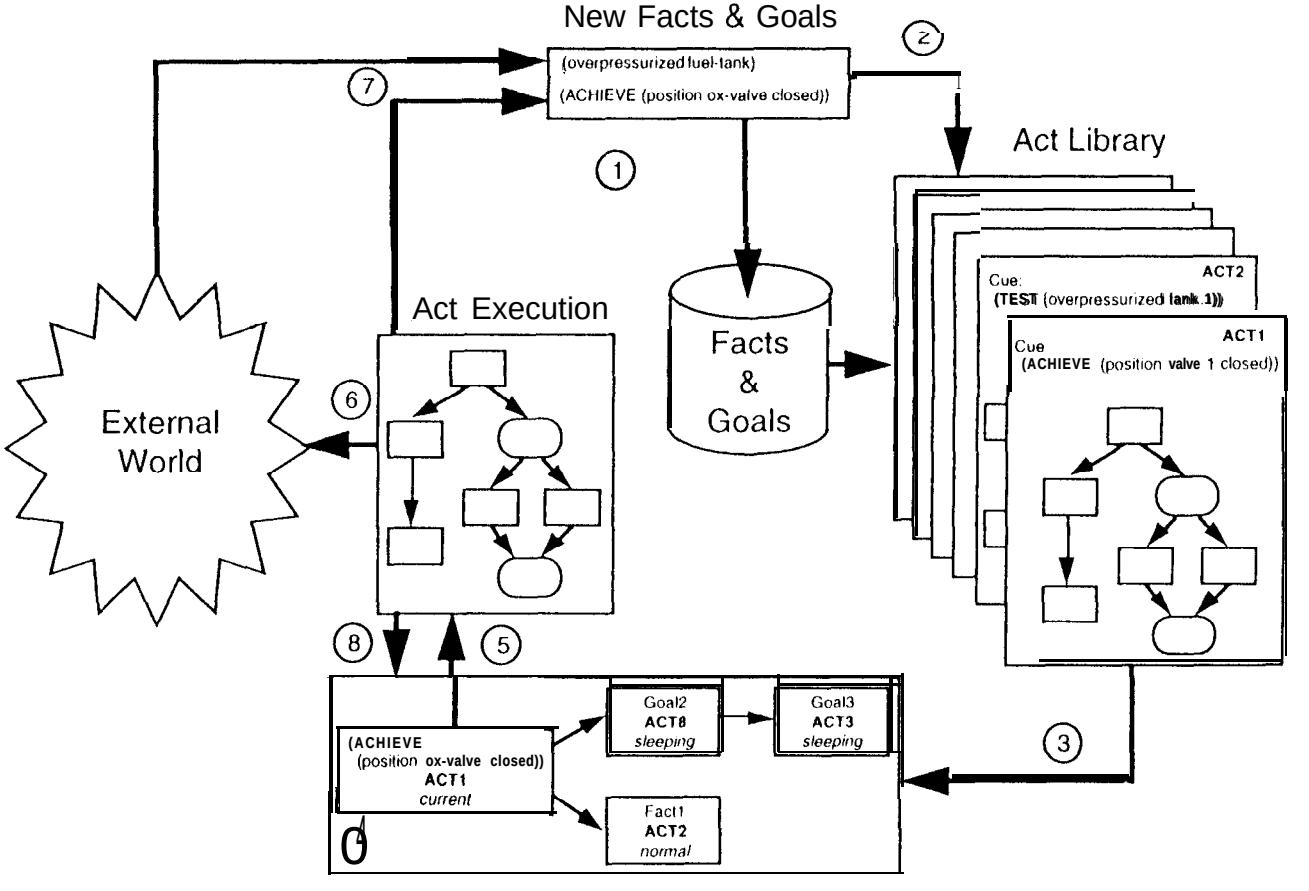
- User of security system is major knowledge source
  - Often unavailable
  - Mobile
  - Different user interfaces
- Backup with automated reasoning system
- Collaboration of Humans and Automated Systems
- Agent-based Architecture

AI Center

PRS-CL Architecture

Execution Cycle

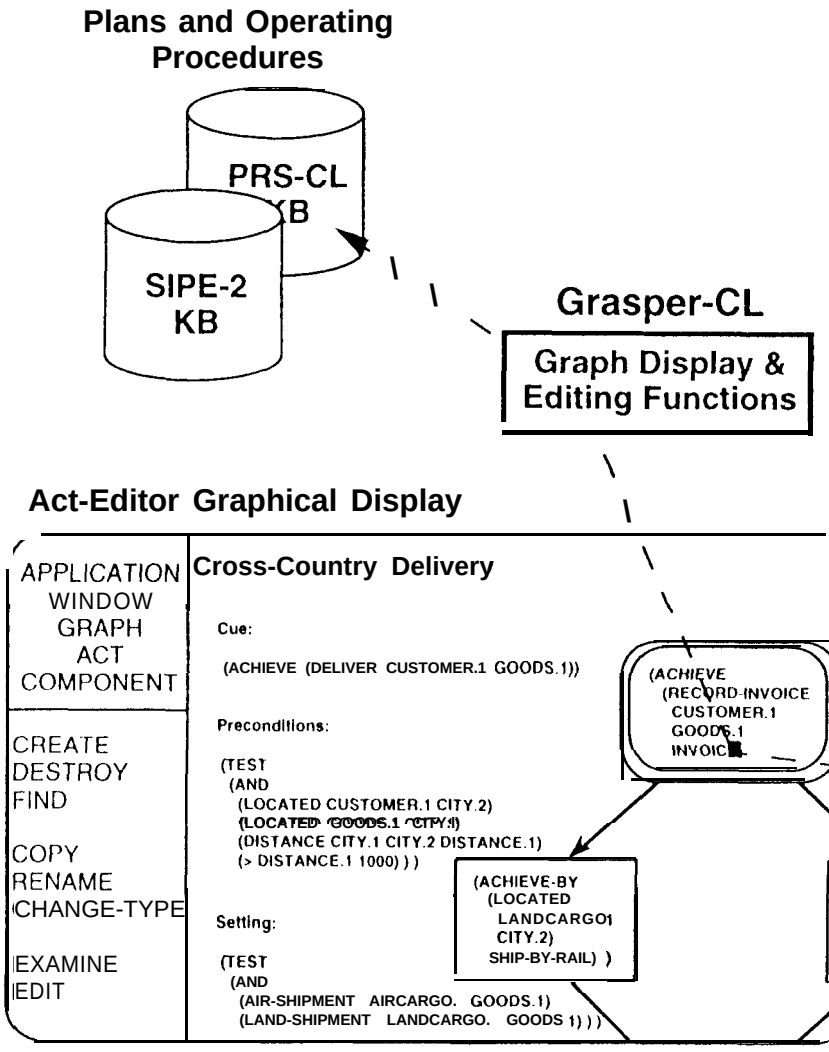
1. New information arrives that updates facts and goals
2. Acts are triggered by new facts or goals
3. A triggered Act is intended
4. An intended Act is selected
5. That intention is activated
6. An action is performed
7. New facts or goals are posted
8. Intentions are updated



AI Center

Act-Editor

Procedural Knowledge Browser/Editor



- Graphically browse procedures
- Edit procedures through direct pictorial manipulation
- Uniformly manage plans and operating procedures
- Verify against dictionaries of predicates and objects