Autonomous Agents

A solution for Large Scale Intrusion Detection?

Mark Crosbie
Hewlett-Packard/COAST
Critical Problems

• Distribution of configuration information.
• Allowing local configuration changes.
• Putting “local wisdom” in reports.
• Data acquisition for trend analysis and risk management.
• Tool evaluation in an enterprise-wide setting.
Distributing Configurations

- How do we distribute configurations across administrative domains?
- Push or Pull model?
- Automated or human driven?
- Diverse user groups - not everyone is an expert!
- Need a background propagation mechanism.
Autonomous Agents

- Lightweight, mobile code modules.
- Migrate and replicate across network - implicit “push” model.
- Background task - no need for human intervention.
- Can interact with local “wisdom stores” when generating reports.
Reporting Problems

• Reporting - how do we get the right information to the right people?
• Will they know what to do with the report?
• Each group has a local “wisdom store”.
• Agents interact with wisdom store to provide reports tailored for the group.
• Relieves burden on central security “expert”
Evaluating a large IDS

- A System that attempts to break into itself.
- Automate attack capture.
- Replay attacks across the enterprise.
- Evaluate detection relative to enterprise-wide security policy.
- Feedback of test results into configuration.
Problems that remain

• Do we want automated intrusion responses? *Active Intrusion Detection.*
• How does the IDS integrate with enterprise reporting and issue tracking tools?
• Allowing local configuration changes, but remaining within enterprise policy.
Conclusions

- Problems are often to do with humans, not technology.
- Can’t change the world - must integrate with existing technologies.
- Automate tasks - humans are not always “experts”.
- Use “push” models for distributing configurations.