



Engineered Collectives: Agent-Enabled Assurance of Distributed Information Systems

*RAND Workshop
On Complexity and Public Policy
September 27-28, 2000*

Laura R. Gilliom
Distributed Systems Assurance
Department

Sandia's Engineered Collectives Program....

..... is about designing teams of autonomous participants that work collaboratively to do complex jobs.



The Problem

Today's information security approaches are failing against the modern cyber-threat.

Information security features are implemented hierarchically (eg., system administration functions, intrusion detection systems, PKI cryptography, "need-to-know" products)

Significant vulnerability to insider threat

Single points of failure

Clear targets of opportunity

Consequently, today in systems where ultra-high security is required, today the only recourse is to "Keep it Simple."

The Problem (con't)

- ◆ **The trend in information systems usage is toward greater functionality, ease-of-use, autonomous operation, and seamless interoperability.**
- ◆ **Even within extremely sensitive applications, demands for functionality are “winning out” over requirements for security.**
- ◆ **We need a solution that concurrently provides high levels of functionality and high levels of security.**

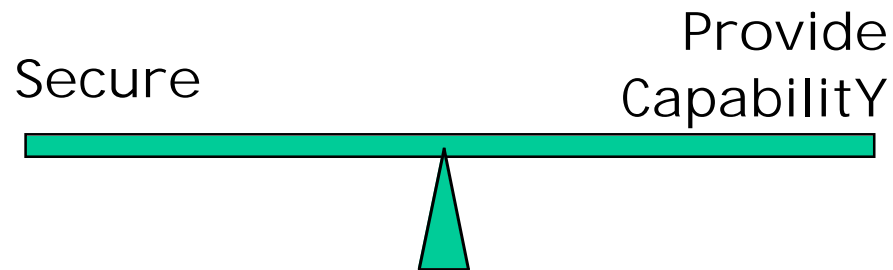
A Revolutionary Approach to Cyber-Security is a Critical National Need

Provide the ability to have concurrently:

High levels of information security, including addressing the insider threat

and

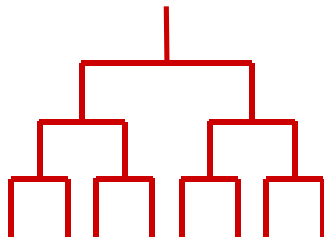
State-of-the-art capability and functionality in a distributed information enterprise



**We Have Conceived an
Innovative Technical Solution
And Are On Track to
Demonstrate a Research
Prototype in Washington DC
in 1QFY01**

Our Solution....

Implements secure system architectures built on a non-hierarchical or decentralized paradigm.



hierarchical



autonomous

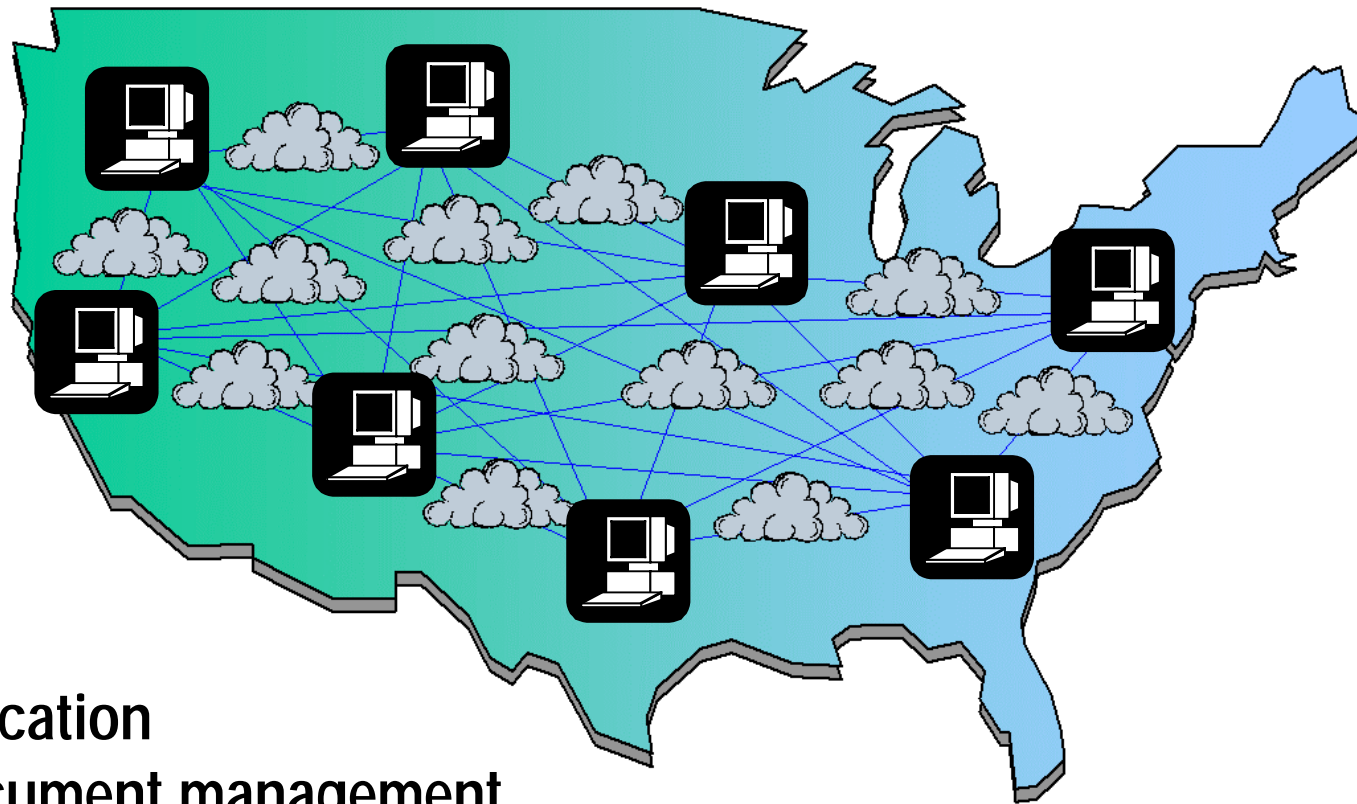


*A team, or collective
of autonomous actors*

The Secure Agent Collective

Secure software agents organized into a security architecture that significantly improves the security of the distributed information system of which they are part, even against malicious insiders.

We Will Demonstrate a Secure, Working “Need-to-Know” Computational Enclave in an Internet-like Environment



- user certification
- secure document management
- remote software upgrades

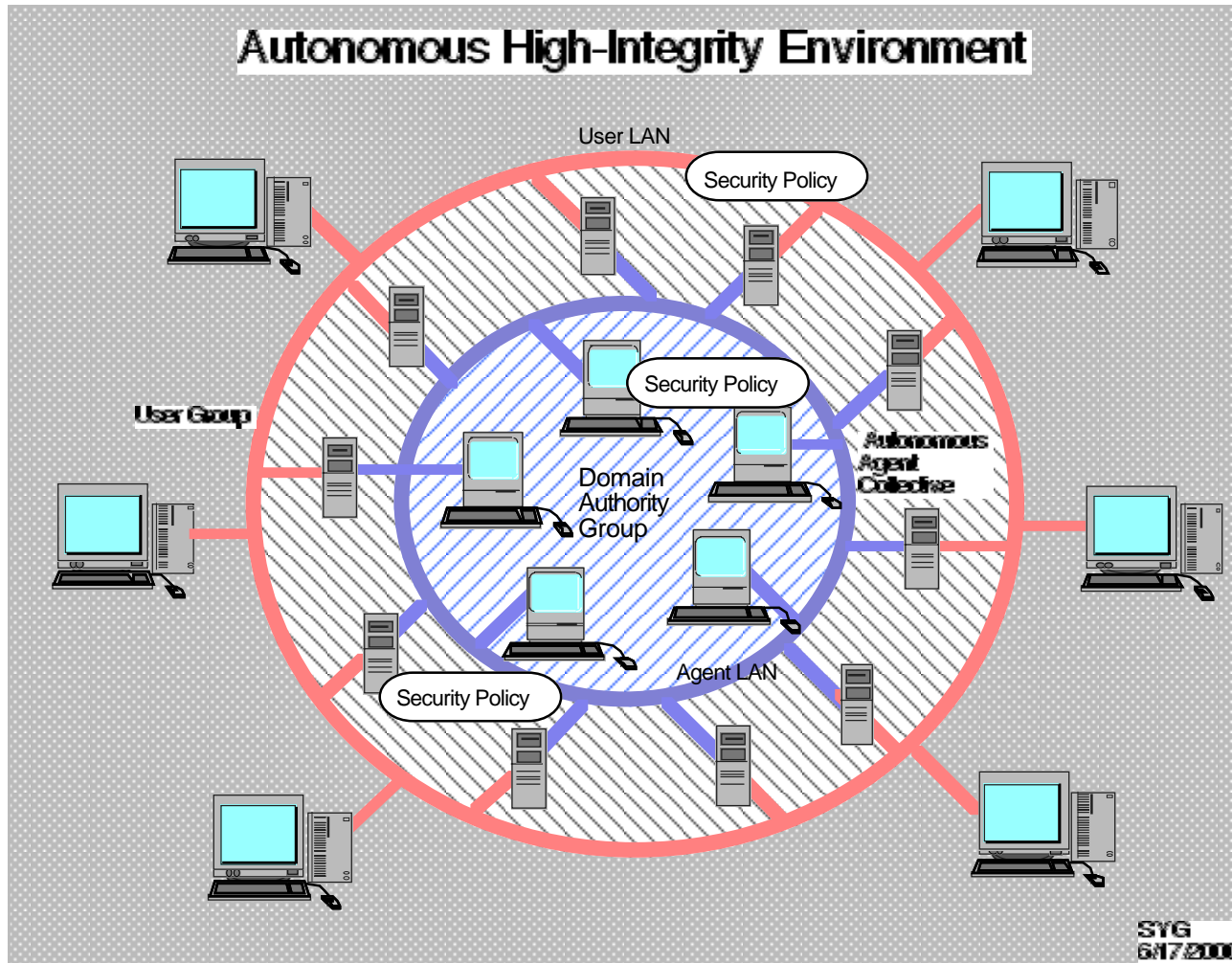
Measure of Success:

- ◆ **Demonstrated strength against insiders during the reliable performance of the listed tasks.**
- ◆ **Red-teaming is being used iteratively.**

Current Status:

- **First Red Team exercise (2QFY00) successful:**
 - Red team did not halt any agent process nor damage or acquire any designated document
 - Agents detected port scans, floods, and unauthenticated messages and communicated this to one another
 - Agents selectively discarded unexpected inputs
- **Agent Collective is self-deploying**
- **Agent population is active on ten-node cluster**
- **Second Red Team exercise underway (4QFY00)**
 - Includes malicious insider challenges

Autonomous High-Integrity Intranet



The Secure Agent Collective Will Provide:

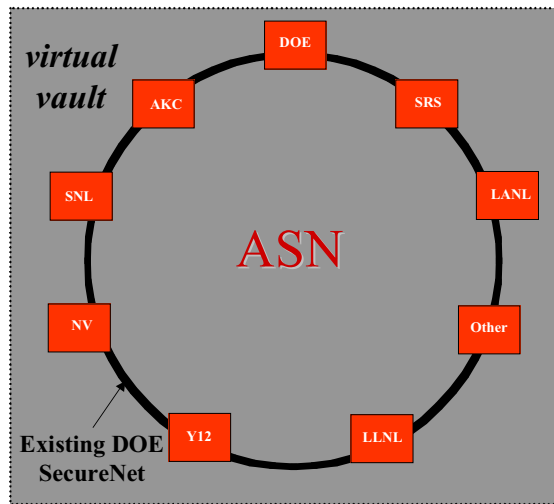
- ◆ **Strong security at the application layer**
- ◆ **Security that also reaches down into the OS**
- ◆ **Invisible management of security for the user**
- ◆ **Distribution of the trust in the system**
- ◆ **An explicit security policy, enforced by secure processes**

**Security is designed in, not added on!
Active not Reactive!**

To Enforce the Security Policy.....

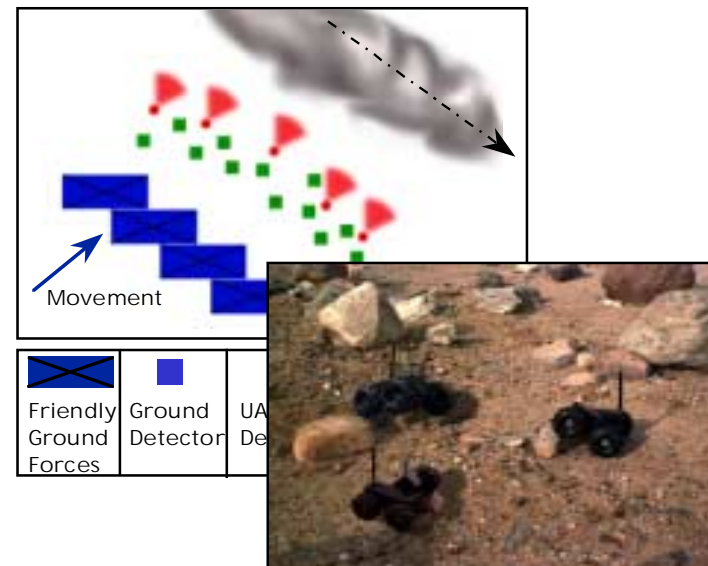
- ◆ **Agents situated in the network validate well-formed transactions and preserve the integrity of those transactions.**
- ◆ **Agents mediate information exchanges among humans and services**
- ◆ **Agents profile and regulate user actions (separation of duty)**

Currently Targeted Applications -



Provide an Architectural Option for Secure "Need-to-Know" Enclaves within the Nuclear Weapons Enterprise Information Infrastructure

Provide a Mechanism for the Secure Management Of Information Obtained from Distributed Mobile/Fixed Sensors as Conceived in the JV2010 Battlefield



Examples of Potential Future Applications of this Prototype

Nuclear Weapons

- ◆ “Need-to-Know” enclaves
- ◆ Multi-person authorization for key system administration functions
- ◆ Sandia/Supplier interactions over the Internet

Energy and Critical Infrastructure

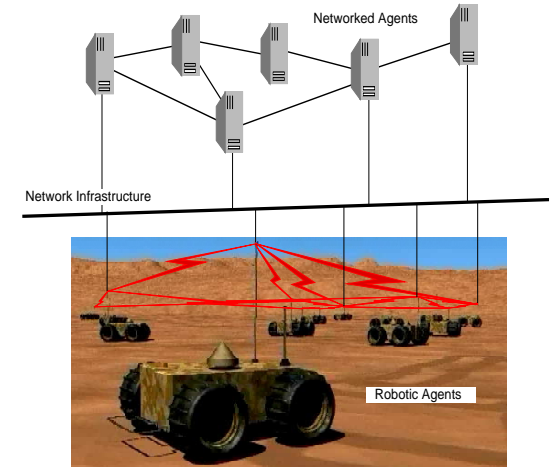
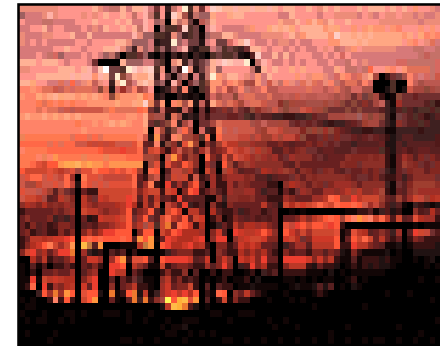
- ◆ Area Control for Electric Power Distribution
- ◆ Security architecture for Internet routers

Emerging Threats

- ◆ Robotic sensor teams for battlefield awareness
- ◆ Military command and control networks
- ◆ Coalition warfare

Synergistic Missions

- ◆ Intelligence community needs



Some Policy Implications:

- ◆ This technology provides a technical path toward real-time, secure policy analysis (to drive action).
- ◆ Existing Infosec policies may adversely affect our ability to implement this technology. Conversely, the technology could drive new Infosec policy.
- ◆ Existing “extremist COTS policy implementation” within the National Security community could adversely impact implementation of this or other real solutions.
- ◆ We are under-resourced, particularly with respect to technical professionals.

Acknowledgements:

Technical Team:

Steve Goldsmith, PI

Shannon Spires

Laurie Phillips

Rich Schroepel

Sandia's IDART Red-Team

Hamilton Link

Brian Murphy-Dye

Richard Billington

Gabi Istraël

Brad Nation

Sponsors:

Sandia LDRD Grand Challenge Program

Lab Senior Management

DOE, Office of Defense Programs

Dr. Ron Detry (SNL)

DARPA, Information Technology Office

Col. Mark Swinson

