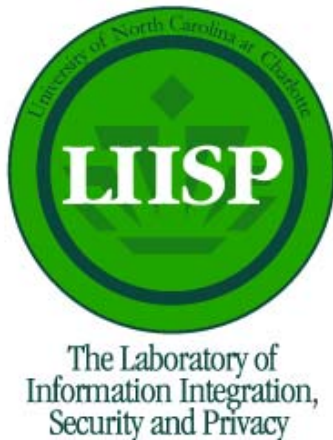


Secure Information Sharing within a Collaborative Environment



DoE ECPI Project

**Gail-Joon Ahn
UNC Charlotte**

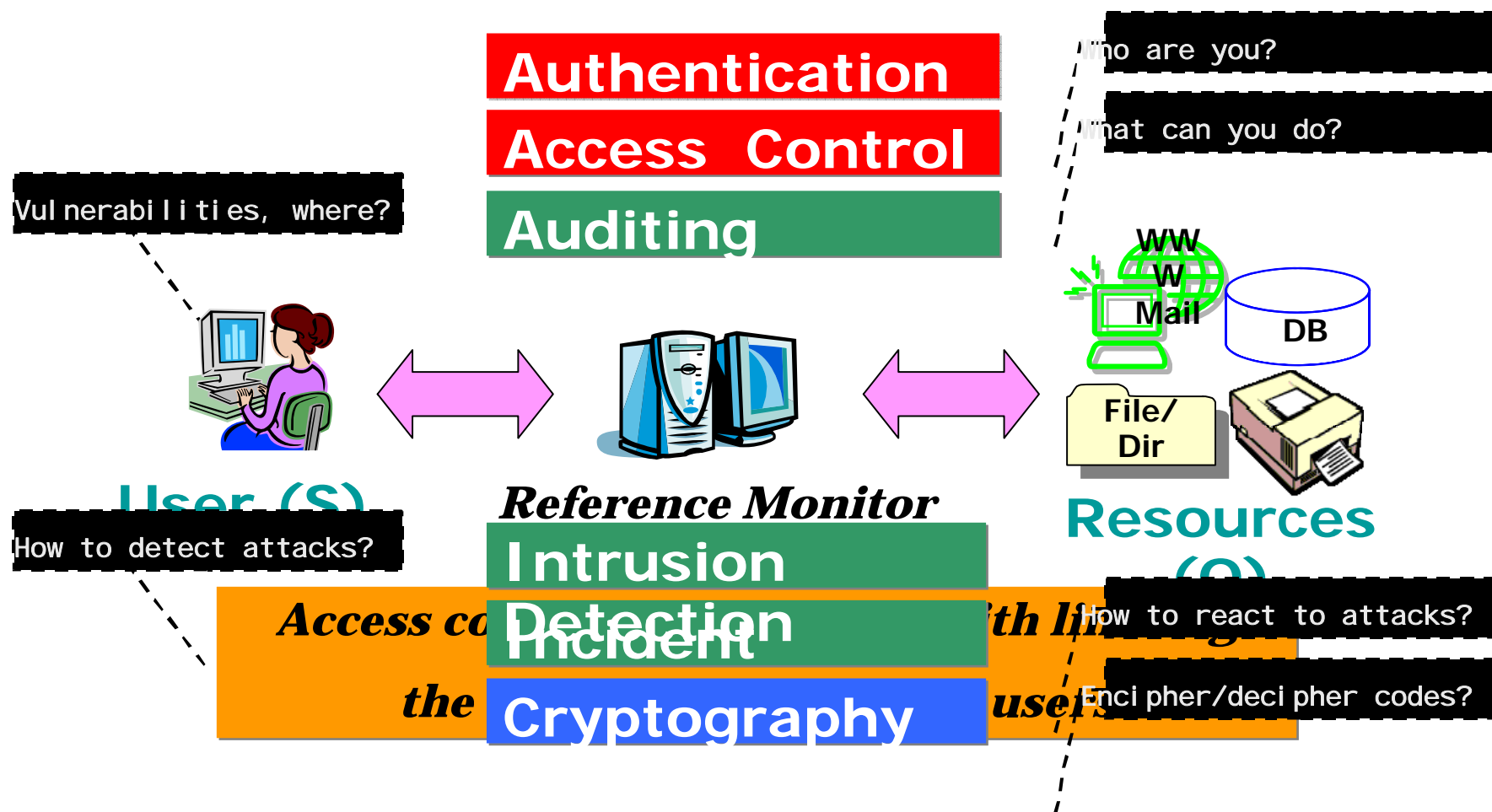


Contents

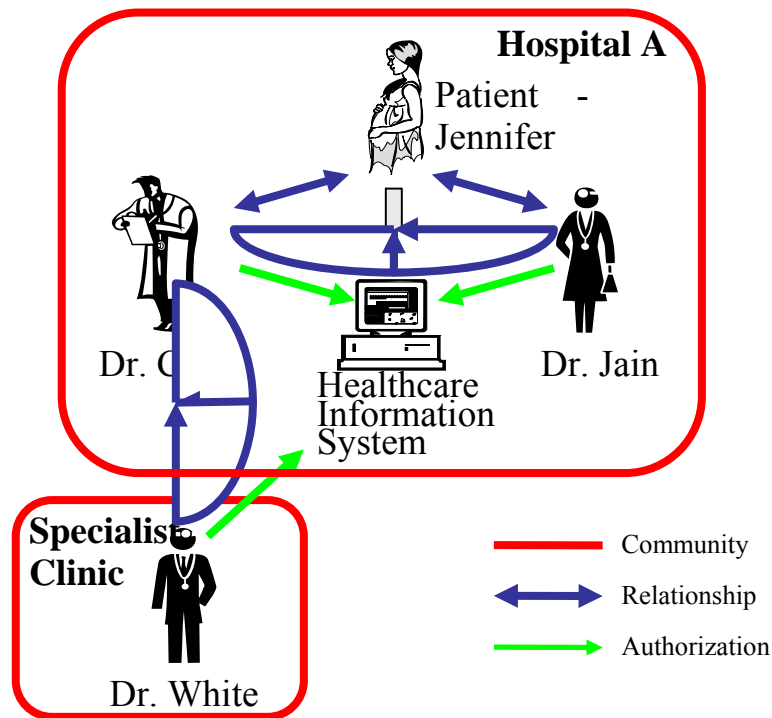
- Introduction
- Motivation and Related Work
- Our approach
 - Role-based Delegation : Concepts and Model
 - Other Supporting Mechanisms
- Ongoing and Future work
- Summary



Security techniques



Collaborative Environment



How can we share critical information in a secure manner?

- Selective information sharing is necessary

- Information may be shared across organizational boundaries
 - Scalable authentication
 - Token-based
- Access Control
 - It is impossible to fully predict what data should be shared, when and to whom
 - Role-based delegation
 - Interoperable access management
- Identity Management
 - A mechanism must be provided for revoking the sharing when it is no longer needed
 - Privacy Attribute Mgmt.
 - Identity Federation





Research Issues

- Can we share information in a secure manner?
- Do we need new security models for this environment?
- What kind of security requirements/constraints/policies should be identified?
- How can we specify them?
- How can we enforce security policies over distributed domains?
- What security architectures are needed?





Our Approaches

- Propose security model to address human-to-human delegation and revocation
- Use authorization language to express and enforce delegation and revocation policies in this model
- Identify security architectures and supporting components
- Evaluate the feasibility and applicability of our approach

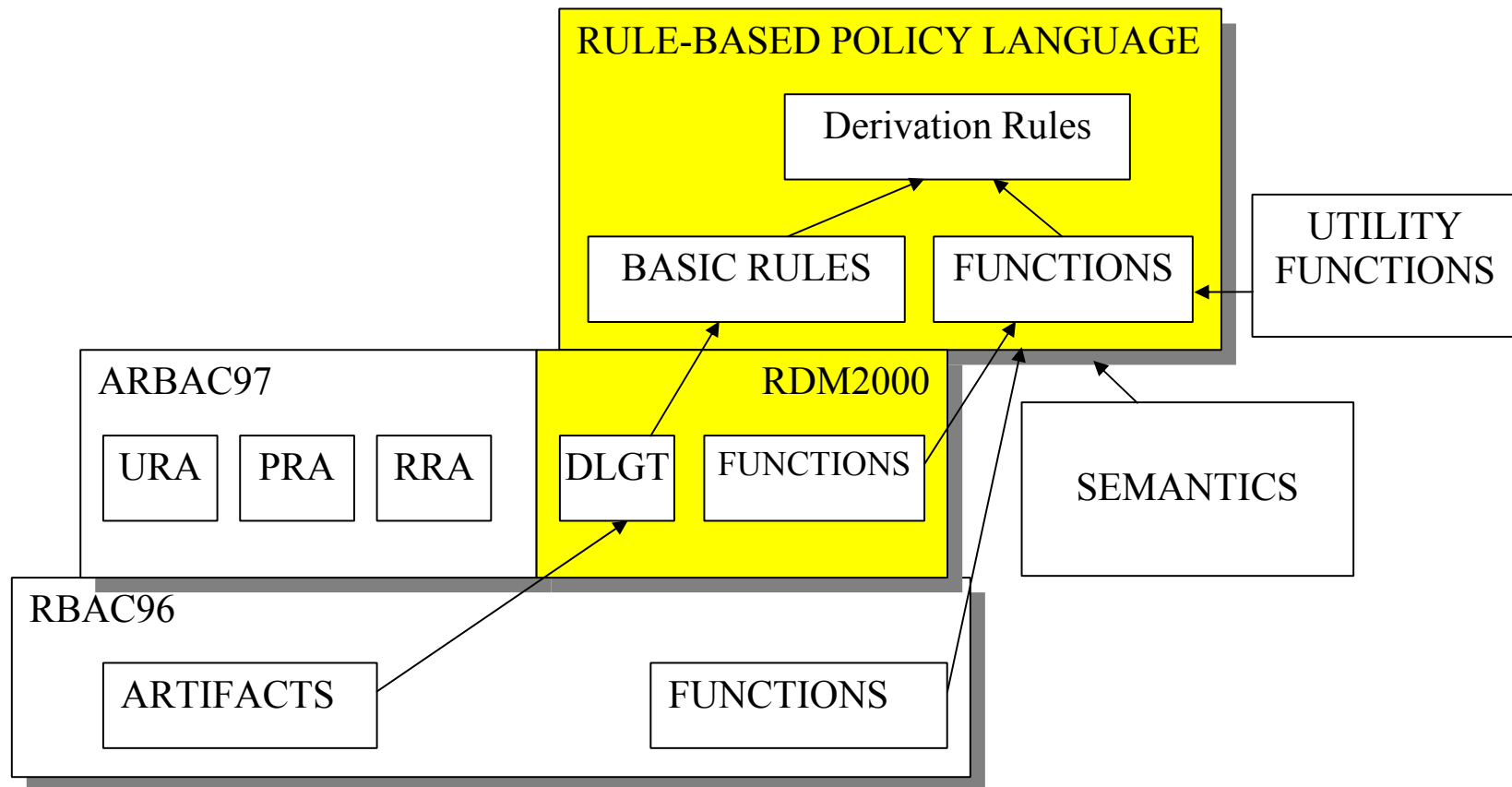


Delegation Issues

- **Permanence**
 - Type of delegation in terms of their time duration
- **Monotonicity**
 - The state of the power that the delegating role member possesses after he or she delegates the role
 - Monotonic and non-monotonic
- **Totality**
 - How completely the permissions assigned to a role are delegated
- **Administration**
 - Who will be the actual administrator of the delegation?
- **Levels of delegation**
 - Defines whether or not each delegation can be further delegated and for how many times
- **Multiple delegation**
 - The number of users to whom a delegating role member can delegate at any given time
 - More effective if the delegation is temporary
- **Delegation Forms**
 - **Human-to-Human**
 - A user delegates his/her privileges to another users
 - **Human-to-Machine**
 - A user delegates his/her privileges to a system so that the system can access the resources on behalf of the user
 - **Machine-to-Machine**



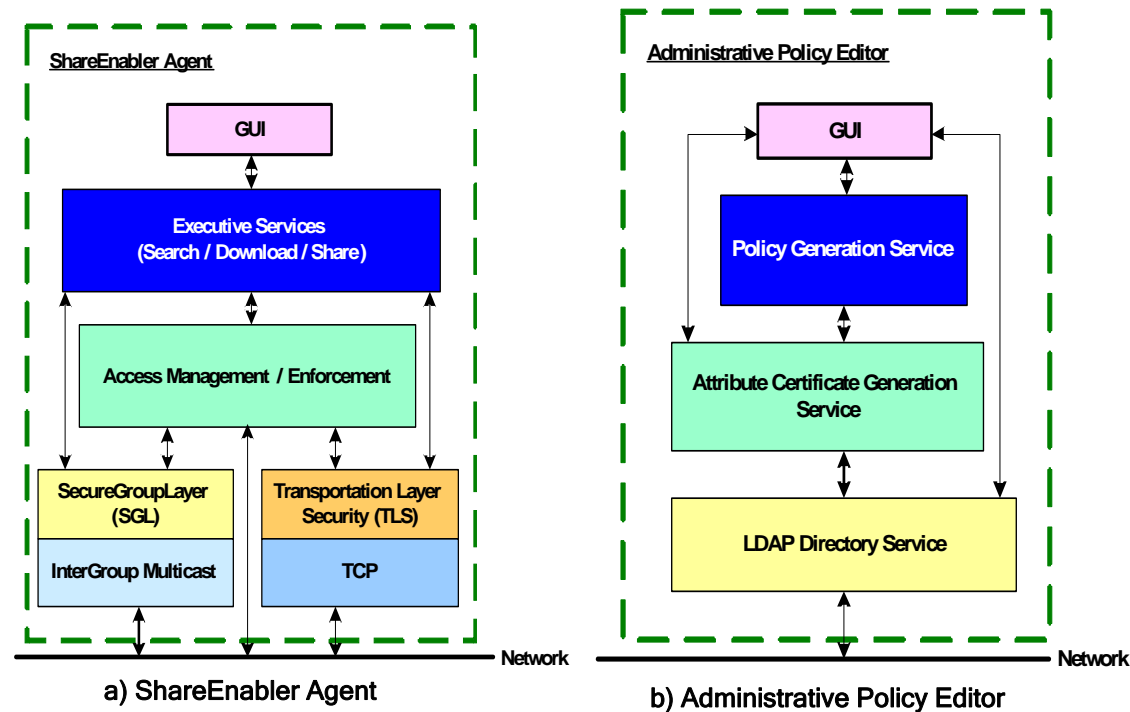
Role-based Delegation



Available in **ACM Transactions on Information and System Security**, Vol.6, No.3



ShareEnabler



- Currently testing it on Grid and Scishare (P2P)





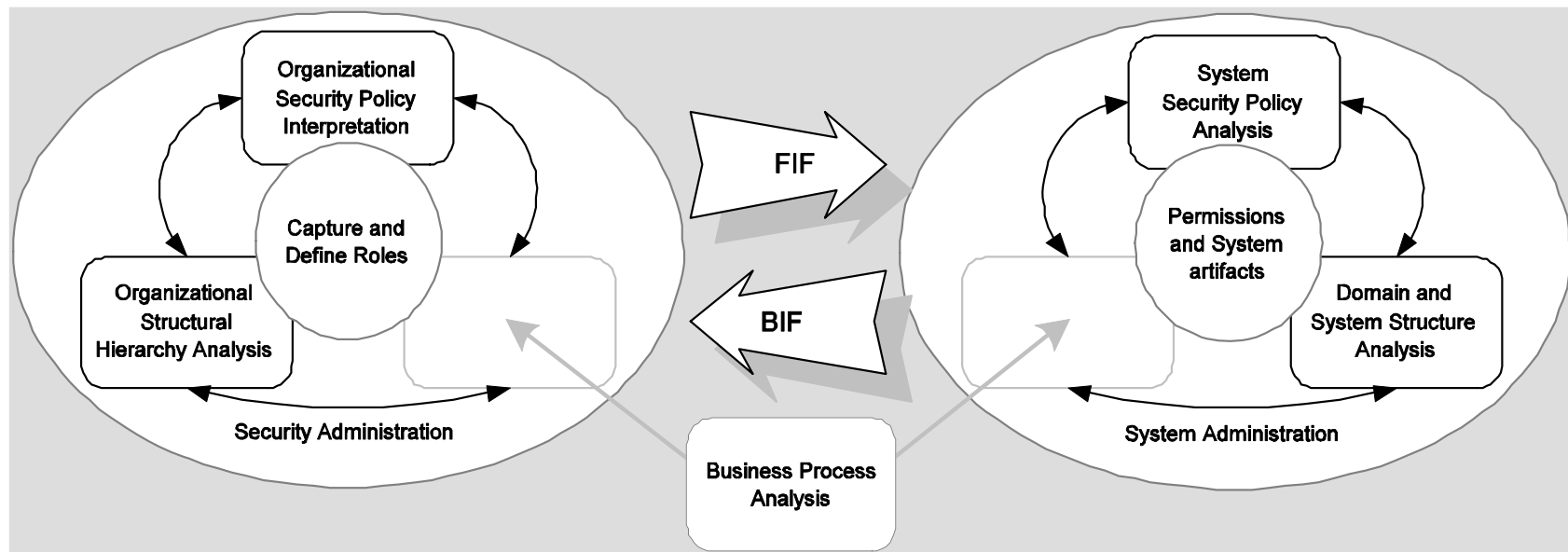
Other Supporting Components

- Role Engineering
 - Role identification
 - Meta-modeling
 - System, permission, and domain
- Role Administration
 - Structural analysis
 - Behavioral analysis



Information flow types in RE

- Forward Information Flow (FIF)
- Backward Information Flow (BIF)



“On Modeling System-centric Information for Role Engineering,” Proc. of 8th ACM Symposium on Access Control Model and Technology, June 2-3, 2003, Como, Italy.



RolePartner

The screenshot displays the RolePartner web application interface. The top navigation bar includes menus for File, Edit, View, Operations, Tools, and Help. Below the navigation bar is a toolbar with various icons for file operations and role management.

The main content area is divided into several sections:

- Role Hierarchy:** A tree view on the left shows the role structure. The selected role is 'ETRI02-Mgr', which is a sub-role of 'Proj-Mgr'. Other roles visible include 'rpSuperMgr', 'BoA-Mgr', and 'BoA-Mbr'.
- Assigned users:** A list showing the user 'rpuserid=doshin,ou=rbacUsers,dc=pmi,dc=uncc,dc=edu' assigned to the role.
- Inherited users:** A list showing the user 'rpuserid=gahn,ou=rbacUsers,dc=pmi,dc=uncc,dc=edu' inherited by the role.
- Assigned permissions:** A list showing the permission 'ID: RP-Perm-4 Name: ETRI02-Docs-ACI' assigned to the role.
- Inherited permissions:** A list showing two inherited permissions: 'ID: RP-Perm-0 Name: ETRI02-Proj-Web' and 'ID: RP-Perm-1 Name: ETRI02-Src-Web'.

Below the main content area are two tabs: 'Properties' and 'Constraints'. The 'Properties' tab is active, showing the following details for the role 'ETRI02-Mgr':

- Role ID:** RP-Role-6
- Role name:** ETRI02-Mgr
- Role Type:** Local
- Number of Role Occupants:** 1
- Role Description:** ETRI02 project manager role
- Immediate Senior Roles:** Proj-Mgr
- Immediate Junior Roles:** ETRI02-Mbr
- Created At:** Thu May 15 04:05:15 EDT 2003
- Created By:** rpuserid=superadmin,cn=rbacusers,cn=rbacconfig,dc=pmi,dc=uncc,dc=edu
- Last Modified At:** Thu Jun 12 23:19:51 EDT 2003

On the right side of the 'Properties' tab, there are four buttons: 'Delete Role', 'Modify Role', 'Assign Perm', and 'Assign User'. At the bottom right, there is a 'Role Encoding' button.

The status bar at the bottom left indicates 'User DB is connected...'. The bottom right corner shows the user 'rpSuperMgr' and a green circular logo with the text 'LIISP'.

Ongoing and Future Works

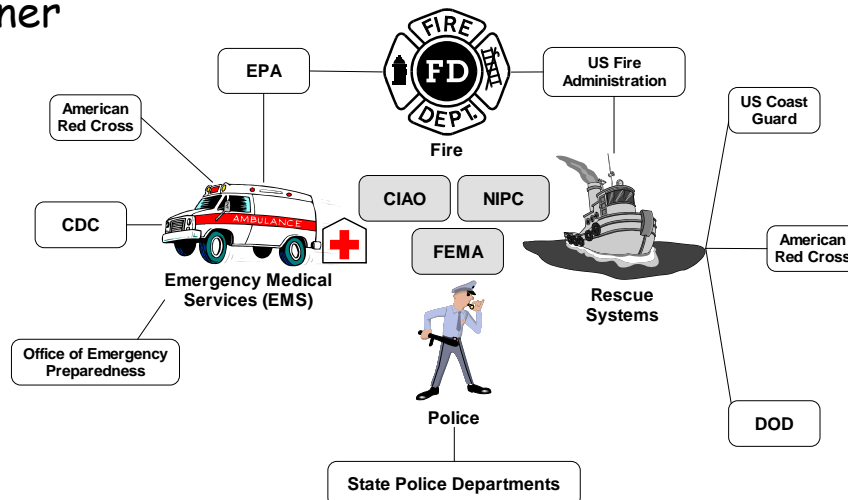
- **Ongoing related projects are**
 - Marriage with Wireless Communication and Collaborative Delegation
 - Supported by **NSF & DoE CAREER Award**
 - ACM TISSEC Vol.6 /No.3 2003, IEEE ITCC 2004
 - Private Attribute Management
 - Supported by **Bank of America**
 - IEEE IPCCC and DEXA 2004
 - Role Engineering Methodology
 - Collaboration with **NIST**
 - ACM SACMAT 2003, ACM SAC 2003
 - Vulnerabilities in Collaborative Systems
 - Supported by **SPAWAR**
- **Our future research includes**
 - Another type of delegation
 - Permission-centric delegation
 - Role-role delegation
 - Specification of constraints related to delegation
 - Correctness and convergence of rule derivations
 - Distribute and manage rules across organizational boundaries



Other Applicable Domains

Information sharing in Military domain ⇒

- Robotic warfare may be a reality by the year 2025.
- Battlefield robots need to communicate each other for their mission. They should be able to share information in a secure manner



Official DOD Photo

↑ Proactive protection for Critical Infrastructures

- Critical infrastructures need to share information each other because one incidents in a critical infrastructure may cause severe damages to other infrastructures due to interdependencies between critical infrastructures





Summary

- First attempt to propose a systematic role-based delegation model
- We have
 - articulated issues in delegation
 - specified this model with rule-based language
 - implemented a role-based delegation framework to manage information sharing in the healthcare information system
 - System components, System architecture, System implementation
 - Highlighted features: rule management and context constraints
- Acknowledgement
 - Supported by **Department of Energy CAREER award** (DE-FG02-03ER25565) and **National Science Foundation** (IIS-0242393)

