Report on DIMACS Working Group Meeting on Policy Driven Decision Making and Dynamic Interoperability

December 8, 2000

Workshop Organizers:

Tom Buckman, MITRE Corporation
Joan Feigenbaum, Yale University
Fred Roberts, Rutgers University

ReportAuthors:

Sri Divakaran, Rutgers University
Fred Roberts, Rutgers University

February 25, 2001

1 Workshop Focus

Modern military operations emphasize a need to be able to rapidly assemble multiservice, multination, coalitions. The modern, high-speed, high-tech information-based economy has put a premium on the ability of companies to partner rapidly in joint ventures. This has led to a requirement for services and nations or corporations to quickly interface operational processes and federate supporting communication and information systems, in order to meet mission objectives. This calls for a new approach to achieving interoperability, one that emphasizes the ability of operational units and their supporting information systems to adapt to unanticipated changes in operational requirements that occur during the execution of a mission or that occur in the context of new joint ventures.

In order to respond to unanticipated changes in requirements, it will be necessary to rapidly translate policy decisions generated by mission commanders, senior executives, system operators, security authorities and others into coherent sets of commands or protocols that can be used directly by supporting information systems to reconfigure themselves to satisfy these policy requirements.

The objective of this initial working group meeting was to explore previous work done by theoretical computer scientists in the area of policy driven decision-making and its potential application to solving problems associated with enabling dynamic interoperability. It was anticipated that previous work done in this area related to scenarios, in which mutually distrustful (or partially distrustful) parties wish to perform a security-critical joint action, may apply.

The working group meeting concluded with a roundtable discussion on ideas presented during the course of the day. The discussion focused on identifying areas for further research which could serve as a focal point for a follow-on workshop and working group meeting.

2 Summary of the Presentations

Network Configuration Management and Interoperability, C.S. Rajagopalan, Telecordia Technologies

Dr. Rajagopalan talked about some of the interoperability policy issues that arise in the context of management of large networks. He addressed the problem of managing a large network among a group of system administrators.

Dr. Rajagopalan motivated his talk by describing the following scenario:

The Open Telecom Act mandates access to the Telecordia network to all new telecom start-ups. In order to enable access to the new telecom start-ups and at the same prevent unauthorized access to Telcordia networks, the system administrators manage the fire walls manually and the global policy for network security is determined and enforced manually. This results in lack of flexibility in the validation and enforcement of policies for network security. Also, in practice the network availability issues dominate the security issues and this often results in network security being compromised.

Dr. Rajagopalan mentioned that the goal in network security management is to provide a network that is dynamic, responsive and controlled by high level policy. In addition, we also need to address the issues like what specific changes are permissible in the network, what services can we provide and how do we define the characteristics that constitute a good global policy.

However, to provide such a network using existing tools, we encounter the following problems:

- These tasks are human intensive
- Network ownership is distributed
- Networks are increasingly complex and configuration space is dynamic
- Desirable services can cause security compromises
- There is an increasing application dependence on remote resources

In the second half of the talk, Dr. Rajagopalan mentioned that his goal is to build a network infrastructure where security properties are upheld automatically. In this context he discussed the following problem:

Given the policy for each subnet and the network description, find initial configurations so that all policies are upheld.

While discussing the above problem, Dr. Rajagopalan discussed:

- the languages for expressing security policies
- how to validate security policies
- the assumptions and limitations of netork control
- how to monitor a changing network
- the policies to constrain network behavior
- active management of constraints
- the compiling of policies into constraints between configuration of network elements

- the scalability issues in building large self-securing networks

Dr. Rajagopalan concluded his talk by raising the following questions:

- How much power is enough in a policy language to express security policies?
- What kinds of guarantees should be built into policies?
- Should interoperability be domain specific?
- How should our network models approximate reality?
- What is the right notion of consistency in distributed networks?
- Is there a theory of control for heterogeneous networks?

Dynamic Policies through Context Sensitive Situations, Opher Etzion, IBM Haifa

Dr. Etzion motivated his talk by describing a dynamic e-business of delivering flowers. In this context, he described a virtual flower store that needs to acquire the following services based on policies that are dynamic:

- billing
- shopping cart
- payment to supplier
- bid of flower shops
- bid of delivery companies

Dr. Etzion mentioned that the problems that arise in dynamic e-business can be explained in terms of the following key concepts:

- **Context**: the context can be expressed either in terms of a temporal element, or as an element bounded by two events or in terms of spatial properties
- **Situation**: the situation can be described in terms of a predicate over the history of events or a trigger similar to databases.
- **Action**: the program that reacts to a situation
- **Policy**: in a given context if a situation occurs, the policy decides which action should be executed

Dr. Etzion concluded his talk by mentioning that the work on dynamic policies is applicable to many domains like CRM, system management and business process management. He also mentioned that in IBM Research they have already worked on contexts and situations that arise in dynamic e-businesses and their current work focuses on designing actions and policies for dynamic e-businesses.

Conflict Resolution in Policy Management, Jan Chomicki, University of Bufalo

The simple event-condition-action (ECA) rule paradigm of active databases has proved very useful in many AI and database applications. However, its applicability goes beyond data management. ECA rules can be used in network management, and other application areas to express policies - collections of general principles specifying the desired behavior of a system. In this talk, Dr. Chomicki used a declarative policy definition language PDL in which policies are formulated as sets of ECA rules.

Dr. Chomicki defined a framework for detecting action conflicts and finding resolution to these conflicts. Conflicts are captured as violations of action constraints. The semantics of rules and conflict detection are defined axiomatically using logic programs. Given a policy and a set of action constraints the framework defined by Dr. Chomicki specifies a range of monitors that filter the output of the policy to satisfy the constraints. These monitors guarantee that constraint violations are fully resolved at run time either by cancellation or delay. The monitors may also differ with respect to a novel property called "unobtrusiveness" which requires that conflict resolution produce a result corresponding to some conflict-free execution of the policy.

In the later part of the talk, Dr. Chomicki presented algorithms to compute the monitors and analyze their computational complexity. He also presented the architecture of a PDL-based policy server used for providing centralized administration of a soft switch in communication network.

Dr. Chomicki concluded his talk by mentioning the need for providing a general framework for defining policy monitors for a broad class of policies. He also mentioned that a lot of work needs to be done for resolving conflicts for a more general class of policies.

XML based Interoperabilty Components, Tom Buckman, MITRE Corporation

XML has emerged as an essential construct in a number of recent initiatives aimed at improving interoperability at the business component level. These initiatives hold the promise of greatly improving the ability of organizations to quickly join themselves together to achieve mutually agreed goals and objectives. However, absent from the current work is the consideration of how to rapidly conduct policy negotiations between these organizations and translate the results into a coordinated set of actions that can be used to help automate the process of the organizations joining themselves together.

In this talk, Dr. Buckman described the role of XML within the architecture frameworks of three initiatives aimed at improving the interoperability at the business component level: RosettaNet, ebXML and Open Buying on the Internet.

In the initial part of the talk, Dr. Buckman described ebXML as a tool that provides the framework for creating interoperable business components for constructing a run-time infrastructure for businesses to network. Dr. Buckman then presented a new approach to Enterprise Application Integration using ebXML. The components of the ebXML solution consist of

- Business processes
- Core Business Components
- Registry and Repository

In the later part of the talk, Dr. Buckman mentioned that we need to take a closer look at policy considerations and the existing products do not consider complex policies. He also mentioned that

XML standards and agreements are key to providing an environment where business components can be combined and composed at run time.

Dr. Buckman concluded his talk by mentioning the following challenges that needs to be addressed for dynamic interoperability:

- Development of core components and business process decriptions for specific domains
- The need for a common extensible language for expressing policies
- The need for automated generation and execution of policy-based trading partner agreements

A Taxonomy for Computer Systems Interoperability, Bruce Barnes, Erols

Interoperability between heterogeneous computer systems is vital to many types of enterprises, but the need for interoperability is particularly conspicuous in naval and other military applications where pressing new requirements may arise quickly and change rapidly.

In this talk, Dr. Barnes described the problem of interoperability, information security in the context of Operation Maneuver from the sea and provided a visual taxonomy to help understand the scope and research needs of this enormous problem. Dr. Barnes explored several dimensions of computer system interoperability including the diversity of equipment and personnel over which systems interoperability is needed. Another dimension explored by Dr. Barnes included some of the attributes of the computer systems such as scalability, functionality and binding time.

Communal Access Control Policies, and Interoperability between Them, Naftaly Minsky, Rutgers University

Dr. Minsky observed that for a group of autonomous agents to interoperate effectively, they must be able to trust each other to comply with some common rules-of-engagement, or a policy. Moreover, it stands to reason that if the members of the group in question are heterogeneous, with little or no trust in each other, then their interaction-policy needs to be enforced; and that this enforcement needs to be de-centralized, if the group can be large.

Guided by this premise, Dr. Minsky presented a coordination mechanism called Law-Governed Interaction (LGI) that enables a community C of distributed agents to interact under an explicit and strictly enforced policy, called the "law" of this community. This mechanism, which is currently prototyped by the Moses toolkit, has the following characteristics:

- The membership of C can change dynamically, and can be very large.
- LGI makes no assumptions about the structure and behavior of members of C, which can, therefore, be quite heterogeneous.
- The deployment of a community under a specified law is easy, incremental, and can be done dynamically.
- The enforcement of laws under LGI is strictly decentralized—for scalability.

Dr. Minsky described the law-governed interaction as a message exchange mechanism which enables a large and heterogeneous community of distributed agents to interact under explicit and strictly enforced laws. The laws in LGI are formulated strictly locally but enforced in a uniform manner over the community. Dr. Minsky then mentioned that LGI can be applicable in areas like B2B commerce, workflows, regulating mobile agents and enforcing security.

Generalized Certificate Revocation, Carl A. Gunter, University of Pennsylvania

Dr. Gunter introduced a language for creating and manipulating CERTIFICATES, that is, digitally signed data based on public key cryptography, and a system for REVOKING certificates. The approach described by Dr. Gunter provides a uniform mechanism for secure distribution of public key bindings, authorizations, and revocation information. An external language for the description of these and other forms of data is compiled into an intermediate language with a well-defined denotational and operational semantics. The internal language is used to carry out consistency checks for security and optimizations for efficiency.

Dr. Gunter described a technique for treating revocation data DUALLY to other sorts of information using a polarity discipline in the intermediate language.

Dr. Gunter described the main problem in certificate revocation as the fact that the retrieval of data is not integrated with data verification. He then described how to extend his work on Query Certificate Managers (QCM) for certificate revocation. In this context, he described the implementation and deployment of QCM for various retrieval options and he also mentioned the limitations of QCM.

Dr. Gunter concluded his talk by mentioning the following concepts in certificate revocation:

- policy directed certificate retrieval
- dynamic channel discovery
- chaining (transparent delegation)

3 Round Table Discussion

The following were some of the concerns / questions that were raised during the round table discussion:

Concerns

- This meeting only discussed the issues of interoperability in an abstract sense. In order to get a feel for the difficulties involved in interoperability across various domains we need to define interoperability in a more formal (mathematical) framework and then tackle the technical issues that arise in interoperability.
- Dealing with interoperability involves both compliance checking and policy enforcement. Both issues are very important and neither is completely understood as yet.
- Formal logic has an important role in the development of languages for expressing policy. This meeting did not explore the role and limitations of formal logic in the development of languages for expressing policy.
- There was no discussion of the efficient decidability of policy.

Questions for Further Work

- How do we best achieve interoperability? Can it be achieved best by compliance checking, language, enforcement?
- What is a good language for expressing policy?
- How can we translate a high-level policy statement in natural language into a system that will help us interoperate?
- What are the criteria for deciding on policy and its enforcement?
- What types of guarantees should be built into policy? (Average-Case?, Worst-Case?)
- How do you deal with issues of inconsistency, scalability and deployability in interoperability?
- How does one automatically generate and execute trading partner agreements?
- Different users have different levels of skill. How can we define plans for people with different skill levels?
- How can one translate policy events identified by the customers "on the fly"?
- How can we enable security policy end-to-end (from secure for customer profile down to local wire instances with policy for sub-network access and information access and availability)?
- Is there a possibility of "standardization" in this field? Are problems of interoperability really different in medical applications, automobile applications, B2B applications, etc.?
- Is there a good way to derive policies from models?
- More work is needed on the foundations of interoperability: credential retrieval, enforcement, interpreters. How can we arrange for this to happen?
- Large-scale experiments, making use of foundational work, are needed. How do we encourage them?
- How can you tell if you have implemented the policy that was intended? How can you tell if two policies are equivalent? If one is a subset of the other?

Suggestions for the Future

- The subject of interoperability needs to be addressed from three perspectives:
  - **Programming Languages**: The problem of what constitutes a good language for expressing policy.
  - **Software Engineering**: Establish standards and methodologies for interoperability.
  - **Theory**: Establish a mathematical framework and address problems of complexity and decidability of policy enforcement.

- We should consider getting together the people with interoperability problems from various domains to stimulate research in problems that are of real interest to the community. This could be done either through one meeting or some sort of a seminar series.
- We should consider holding a meeting that focuses on a specific application domain like B2B or medicine (patient records) and then get the user community and researchers together to address the problems of interoperability that arise in that domain.
- We should consider organizing a future meeting around a methodology or around a specific technical area (such as distributed security).