M.I.T. Laboratory for Computer Science

Request for Comments No. 269
December 31, 1984

Non-Discretionary Controls for Inter-Organization Networks

by Deborah L. Estrin

A version of this paper was ~~submitted~~ accepted to the 1985 IEEE Symposium on Security and Privacy.

NON-DISCRETIONARY CONTROLS FOR INTER-ORGANIZATION NETWORKS

Deborah Estrin.
30 December 1984

This paper describes a conceptual model for implementing usage controls in Inter-Organization Networks (IONs). After describing security requirements in networks that cross organization boundaries, I suggest how traditional, non-discretionary controls can be adapted to support usage control in IONs.

1. Introduction to IONs

When two or more distinct organizations interconnect their internal computer networks to facilitate inter-organization interchange, they form an Inter-Organization Network. The interchange may be person-to-person communication via electronic mail; exchange of cad/cam data, software modules, or documents via file transfer; input to an order/entry or accounting system via a database query and update protocol; or use of shared computational resources via an asynchronous message protocol or remote login. In most inter-organization arrangements, the set of resources that an organization wants to make accessible to outsiders is significantly smaller than the set of resources that it wants to remain strictly-internal (i.e., accessible to employees of the organization only). In addition, because the potential user is a person (or machine) outside the boundaries of the organization, the damage associated with undesired use can be high. Because of these characteristics, IONs have unique usage-control requirements.

Unlike traditional security requirements, the goal is not to prohibit access by outsiders; some outside access is explicitly desired. The goal is to support access to certain machines, services, and processes, while preventing access to all other internal facilities; hereafter referred to as ION facilities and strictly-internal facilities, respectively. In addition, because the function of the internal network predates and dominates that of the ION, interconnection must not interfere with internal operations. Therefore, it is not acceptable that ION facilities be physically isolated from all strictly-internal resources for this would interfere with use of facilities and communications internally. We want to

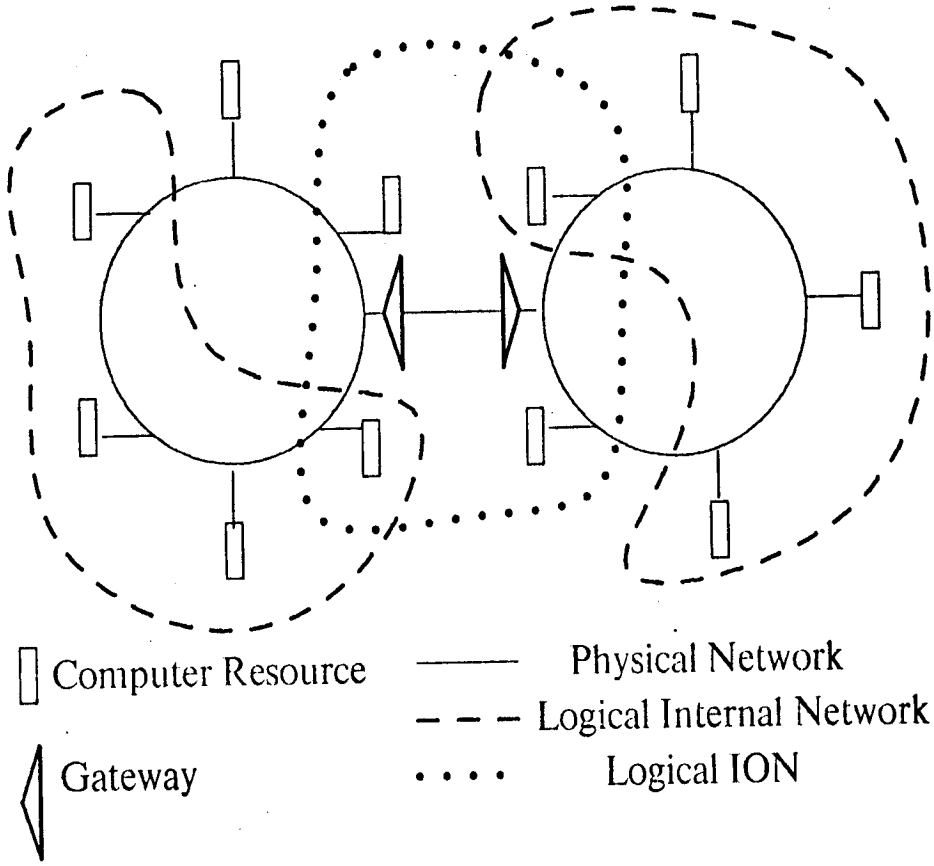

Figure 1-1: Overlapping Logical Networks: The ION shares physical resources with the two organizations' internal networks. However, at the logical level, the ION is isolated from the internal networks.

implement *logical networks* that can be isolated from one another yet share physical resources (see figure 1-1).[1] Similarly, when two organizations interconnect, it may be inappropriate to impose a connection between the other organizations to which each was interconnected previously. In other words, the new ION may overlap physically with the existing IONs, but it must not form a transit path between those organizations that desire to remain isolated from one another (such as *B* and *C* in figure 1-2).

[1]The term *logical network* refers to a collection of computational resources and applications that communicate with one another. Logical networks operate on top of physical networks which are composed of communication links and switches.

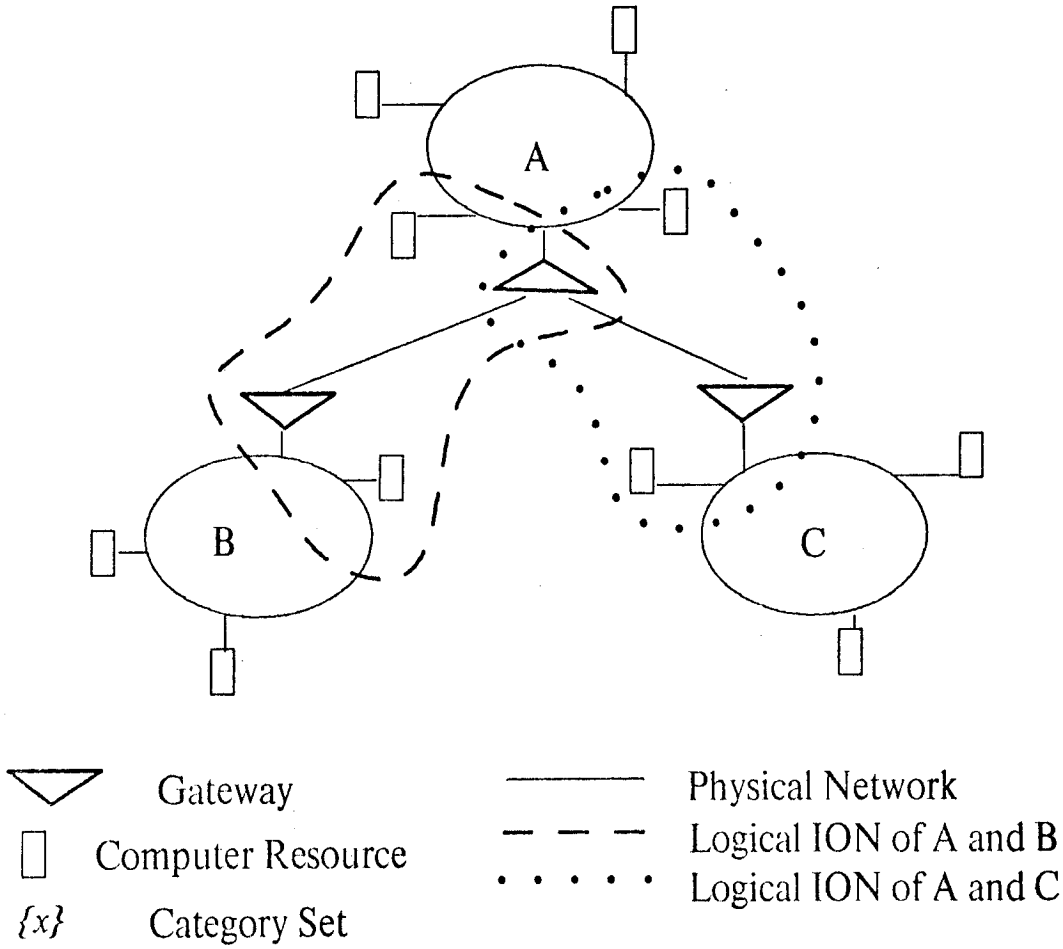

Figure 1-2: Overlapping IONs: The ION between A and B shares physical resources with the ION between B and C. However, at a logical level the two IONs are not connected to one another, i.e., B cannot communicate with C via A.

2. Non-Discretionary Controls

Because most of an organization's internal resources are to remain strictly-internal, the default condition for outsiders should be no access. Furthermore, these strictly-internal resources should not be required to take any action, such as beefing up their security, in order to be protected from external access. A requirement to take explicit security action, even a small one, when external links are added is infeasible or undesirable in most large organizations for several reasons:

1. Typically, the purpose of an internal network is to facilitate communication and resource sharing. Increased internal usage controls that are tailored to restrict outsiders may interfere with this objective.

2. The administration of most networks is intentionally decentralized. Consequently, it is very difficult to assure conformance with new policies such as accessibility of internal resources to outsiders.

3. Internal networks grow incrementally by adding connections to other internal networks as well as single machines. It is hard to check if such additions introduce resources into the internal network that do not conform to network-wide policy.

4. In order for users to enforce a security policy they must be educated as to its purpose and operation. Educating all users of a decentralized network is hard to accomplish once, let alone every time an external link is established.

Therefore, only the administrators of the external link (i.e., the ION gateway) and the internal resources that are explicitly being made accessible should be required to take security action. Owners of all other internal resources should be assured that their facilities are not accessible to outsiders. In other words, the management of a strictly-internal resource should not have to rely on its own discretionary action for restriction of external access to its facilities. This requirement suggests the use of *non-discretionary* access controls to isolate strictly-internal resources and networks from the ION without relying on the discretion or explicit action of strictly-internal resource owners.

There are two essential differences between the non-discretionary access controls called for here, and those traditionally employed in military security systems [3, 4]. First, in the case of military systems the most common use of non-discretionary controls is to restrict the flow of information from higher classification levels to lower ones (no read up and no write down) [1]. In IONs, of equal or greater concern is preventing outsiders from *invoking* proprietary, expensive, or scarce resources that are supposed to be strictly internal. In traditional terms, control of invocation concerns unauthorized disclosure, modification, and denial of *resources*; whereas, information flow control concerns only unauthorized disclosure of *information*. Although many commercial and government institutions are extremely concerned about the outgoing flow of information, in this paper we focus on

invocation control because it has received far less attention in the past.[2]

Second, the non-discretionary invocation controls that have been developed are designed to protect the integrity of the *invoker*, not the *invoked* [2, 5]. For example, the integrity rating of a program indicates the level of assurance that a user can have that the program does not contain any trojan horses. Based on these ratings, the simple integrity policy allows a user to invoke programs of *equal-or-greater* integrity only.[3] In contrast, we are trying to protect each ION participant in its role as service *provider*, not *user*. To do so, we must protect the provider from unauthorized disclosure, modification, and denial of resources. Therefore, we want a policy that prevents a program from being invoked by a user that does not have an adequate integrity rating. The invocation policy should allow a user to invoke services of *equal-or-less* integrity only. Rotenberg [6] was also concerned with protecting information providers but did so only in the form of controlling information flow, i.e., unauthorized disclosure of information. He assumed that any service provided necessarily returned information, and that information flow controls would prevent the returning of information to unauthorized users. In current day network environments there exist facilities that do not necessarily return information or that do so only after the resources have been expended or an irreversible action has been taken (e.g., gateway, print servers, robotic devices, order/entry system). In this environment, control of invocation is needed in order to protect the owners of such services.

Based on these characteristics and requirements, we suggest that special network entry points, *ION gateways*, implement non-discretionary invocation controls. ION gateways are logical gateways that

---

[2]One form of information control that we do address explicitly is information flow that is not mediated by an employee of the organization (i.e., extraction). Such flows require invocation of a file transfer or database or other computer-based service by an external entity and therefore are covered by invocation controls. IONs also raise concerns about the outgoing flow of information that IS mediated by employees. For example, automatic distribution lists remove direct employee discretion from the process of generating outgoing mail. In addition, organizations often are concerned about excessive dependency on resources that are not controlled by the organization itself. However, these concerns are more traditional in nature and can build on more traditional mechanisms. Future research will discuss the extension of these traditional information flow controls to these ION requirements.

[3]The simple integrity policy is described as the mathematical dual of the basic security policy by Biba in [2].

mediate and control the forwarding of messages from outsiders into the internal network.[4] In addition, ION facilities that are invocable by outsiders must implement discretionary or non-discretionary controls to protect other non-ION resources. Finally, because organizations communicate with multiple external organizations, and these inter-organization relationships are not hierarchically related to one another, the access rights should be based on category sets (compartments) and not sensitivity levels.

The participating organizations can tailor the strength of the gateway's implementation to suit their security requirements. These requirements will vary with the value of online information and resources, as well as the nature of the inter-organization relationships. *The general requirement is to raise the level of monitorability and accountability to that of telephone and paper communication.*

In the following sections we describe two example IONs and discuss how non-discretionary controls can be implemented in the ION gateways and ION facilities without modification to strictly-internal facilities.

3. Examples

The following two examples illustrate how non-discretionary invocation controls could be used to protect the resources of interconnected organizations. In the first example the default condition is no access, and the major concern is to isolate strictly-internal resources from ION resources. In the second example, the default is more open access and a primary concern is to prevent transit from one outside organization to another via a third, mutually-accessible organization.

A manufacturer of subassemblies and specialized components for automobiles, *CarParts Inc.*, has connected some of its internal computer facilities to those of two of its major customers, *General Auto* and *Average Motors*, who happen to be major competitors of one another (see figure 3-1). The connections are intended to support exchange of cad/cam data between the manufacturing and

---

[4] ION gateways may be composed of multiple, physically distributed components, e.g., a packet forwarder, policy filter, authentication server.

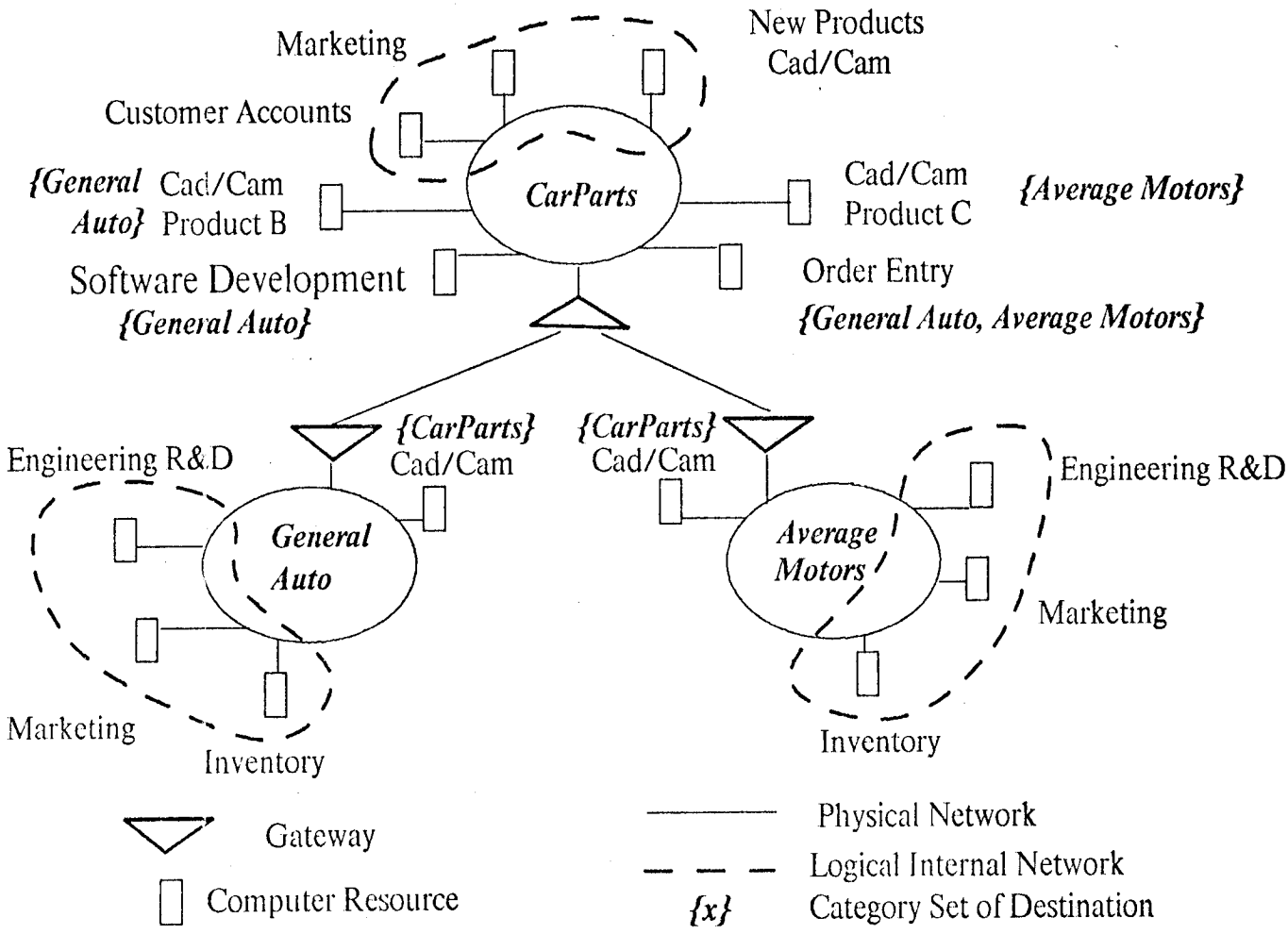

Figure 3-1: Example of an Inter-Organization Network: One ION exists between *CarParts* and *General Auto* and another ION exists between *Car Parts* and *Average Motors*. Both IONs overlap physically yet are isolated logically from the strictly-internal networks of the three organizations.

engineering departments of *CarParts Inc.* and each of its customers. *General Auto* is able to invoke one of *CarParts Inc.*'s servers that contains cad/cam data for the product line that *General Auto* purchases. *Average Motors* can do the same for the different product line that it purchases. Both servers are invoked by sending appropriate messages through the gateway, and both servers return the requested data via the same gateway to the requesting organization. In addition, both customers have replaced paper invoices with online access to *CarParts Inc.*'s order/entry system, which also

uses a message-based protocol. Finally, *CarParts Inc.* and *General Auto* are jointly developing special cad/cam software for automotive applications, for which *CarParts Inc.* allows *General Auto* to access the server that contains the most recent software module updates. Aside from these ION resources, *CarParts Inc.* has many strictly-internal computer-based facilities: customer accounts, market forecasting models, cad/cam facility for new product development, inventory system, gateway to vendors of sub-sub-assemblies, and internal electronic mail.

In order to isolate ION from strictly-internal facilities, and the *General Auto* ION facilities from the *Average Motors* ION facilities, *CarParts Inc.* can implement the following controls:

1. Implement a single ION gateway and prohibit direct connection of all internal machines to outside organizations. Equip the gateway with an authentication mechanism to certify the source of each message.

2. Assign appropriate category sets to each of the ION facilities, and no category sets to strictly-internal ones. *CarParts Inc.* assigns the category set {General Auto} to its *General Auto* Product Cad/Cam system and its Software Development Server, the set {Average Motors} to its Product C Cad/Cam system, {General Auto, Average Motors} to its order/entry system, and null set to all other internal systems. See figure 3-1.

3. The ION gateway checks the category set of the source, $\{Ci\}_s$, and of the destination, $\{Ci\}_d$, of each message and forwards the message to the intended destination If and only If $\{Ci\}_s$ *Intersect* $\{Ci\}_d$ does not equal nullset, {} (referred to as the *Intersect* rule).

4. Equip the ION facilities (cad/cam-data servers, order/entry system, and software-module server) with discretionary or non-discretionary controls to isolate non-ION files and processes, and to prevent transit between the *General Auto* ION and the *Average Motor* ION.

Similarly, *General Auto* and *Average Motor* each label their own cad/cam and inventory systems with the category set {CarParts} only, and implement gateways with message authentication and the *Intersect* rule.[5]

The second example is of a computer manufacturer, *Creative Automation Inc. (CAI)*, that connects its internal network to a nation-wide network of computer R&D organizations. Informal, person-to-person research communication transpires with a large subset of all the organizations on the

---

[5]Note that each organization assigns category labels to incoming messages for interpretation by its own internal facilities. Therefore, although naming must be consistant within each organization, it need not be consistant throughout the ION as a whole.

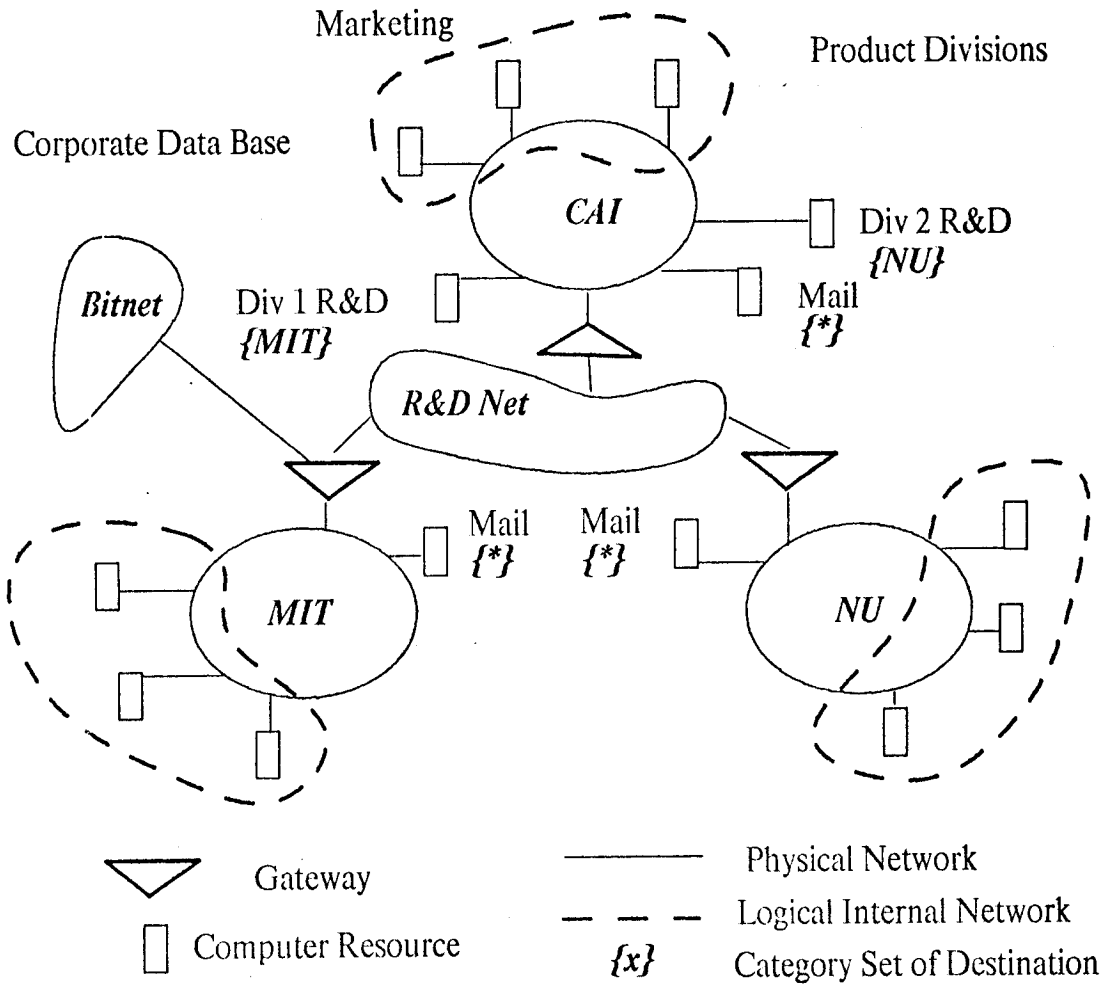

Figure 3-2: Example of an Inter-Organization Network: One ION exists between *CAI* and *MIT* and another ION exists between *CAI* and *NU*. Both IONs overlap physically yet are isolated logically from one another and from a third ION, Bitnet, to which MIT is connected.

network. In addition, there are two universities, *M.I.T.* and *Northeastern (NU)*, with which *CAI* is conducting two separate joint studies, one with each of its major research divisions. In conjunction with these studies, *CAI* supports some file transfer and remote job entry with these two organizations only. To support such tailored connections, *CAI* assigns the following category sets to its ION and strictly-internal resources: *CAI* assigns the category sets {M.I.T.} and {NU} to Division 1's and 2's respective R&D systems, and all three organizations assign the wild-card category set {*} to their

respective mail servers. See figure 3-2. The mail server is made accessible to all network members, whereas the joint-development facilities are made accessible to the select parties only. As described above, the gateway authenticates messages, implements the *Intersect* rule, and ION facilities are equipped with discretionary or non-discretionary controls to isolate non-ION processes and files. For the most part, the two universities, *M.I.T.* and *NU*, are not concerned about protecting internal resources. One exception is that *M.I.T.* has another gateway to a special network, *Bitnet*, which provides access to European institutions. In order for *M.I.T.* to remain on *Bitnet*, it must guarantee that no non-university parties send mail or other traffic over the subsidized network.[6] For this purpose, *M.I.T.* implements the *Intersect* rule in its gateway to the R&D net, assigning wild card category sets to entire regions of its internal network that it wants to be globally accessible, but assigning the *Bitnet* gateway a null category set.

4. Implementation Issues

In general, the following controls would be implemented by each ION participant:

1. Define categories and assign to each ION machine or process the set of categories for which it is to be used. For each ION in which the organization is a participant, define a category. If a process is intended for external access by members of a single ION (e.g., an order entry system for customers), then assign it only that category. If it is to be accessed by members of multiple IONs (e.g., a mail server), then assign it multiple categories. Strictly-internal services should be assigned *no label* since they are not intended for any ION categories. External entities are assigned the category associated with that particular ION.

2. Allow external invocations to enter the internal domain through specified gateways only, similar to the notion of entry points [6].

3. The gateway will forward (route) an invocation to the indicated destination If and only if the *Intersection* between the category set of the external invoker, $\{Ci\}_u$, and the category set of the destination ION process, $\{Ci\}_p$, is not nullset, {}. The mechanism can be implemented using a non-discretionary access control list for each ION process, where the list contains groups that are allowed to access the process. Strictly-internal processes have no category set, and are therefore not accessible to any external groups. Note that internal invocations originate within the organization's domain, do not enter through gateways, and therefore are not subject to these non-discretionary controls anyway. As do traditional gateways, the ION gateway must know where to route incoming and outgoing messages based on the destination address.

---

[6] This is necessary in order to conform with policy requirements of the European PTT's.

4. Implement discretionary or non-discretionary controls in ION machines to protect non-ION processes. In particular, isolate ION processes from non-ION processes running on the same machine or other internal machines. A range of traditional system security mechanisms can be applied.

The result is that no external invocations can be sent to processes that are not explicitly registered as accessible to outsiders and that an ION process can specify which categories of external users it is accessible to.

In many cases, information flow controls on outgoing traffic may be needed as well.[7] If an organization is unable to rely on existing policies to discourage employees from exporting confidential information via the ION, the organization may require additional information flow controls. For example, some features of computer-based communications remove direct employee discretion from the generation of ION messages, such as automatic distribution lists. A user who sends a message to a distribution list typically does not know the individuals on the list; the user knows only that they share a common interest. If one of the addressees on the list is located outside of the organization, an employee may export information without realizing it and therefore without considering relevant company policies.

Some information flow controls can be implemented using category sets and the *Intersect* rule: internal user A can send a message/file X to external user/resource B if and only if $\{C\}_a$ and $\{C\}_b$ have a non-empty intersection. However, more elaboration is needed and capabilities will vary with the type of control mechanisms available internally. For example, if internal systems implement non-discretionary controls that mark objects with security labels, the gateway can control outgoing information flow based on the security level of the message content as well as the category set of the message creator. Because each organization implements its own gateway, each can integrate existing, internal, labeling systems into its ION gateway.

In summary, the gateway authenticates, labels, and maintains information on category sets while

---

[7] For many inter-organization networks invocation control is needed for incoming traffic whereas information flow control is needed for outgoing traffic. Therefore, the two do not conflict with one another as they often do when both apply to traffic flowing in the same direction [5].

most of the rest of the world can go on unchanged. Because of the gateway's central role, there are a number of important design issues which require further elaboration but which I will only mention here. One is that the gateway and ION processes must be "trusted" programs by the organization that owns them. However, each ION participant can make its own decision as to the investment and trust that it will place in its ION gateway. The general requirement is to raise the level of monitorability to that of non-ION communication channels (e.g., telephone and paper). Therefore, organizations' security requirements vary according to the value of online information and resources, as well as the nature of the inter-organization relationships. The second issue is that the gateway must authenticate the source of a request/message in order to properly evaluate its category set. A range of tools, of varying strength, can be used, from third-party authentication servers to use of one-time encryption keys. However, whether they employ a self-authenticating encryption scheme, or a trusted third party, participants must agree on the authentication protocol used by their respective gateways.

5. Conclusion

In conclusion, initial analysis suggests that category sets and non-discretionary control mechanisms can be adapted to satisfy usage control requirements in inter-organization networks; namely, to isolate strictly-internal facilities from ION facilities. Further research is needed to understand the range of applications for which the proposed modifications might be suited, the implications for non-discretionary security models, and appropriate authentication schemes.

Acknowledgment

I would like to thank Jerry Saltzer for invaluable discussions, suggestions, and refinements of the ideas presented here. I also thank Bob Baldwin, Carl Landwehr, Steven Lipner, David Reed and Suzanne Sluizer for insightful comments and suggestions on a previous draft.

6. References

[1]
Bell, D., LaPadula, L.
Secure Computer Systems.
Technical Report ESD-TR-73-278, The Mitre Corp., June, 1974.

[2]
Biba, K.
Integrity Considerations for Secure Computer Systems.
Technical Report ESD-TR-76-372, The Mitre Corp., April, 1977.

[3]
Karger, P.
Non-Discretionary Acess Control for Decentralized Computing Systems.
S.M. Thesis, Dept. of Electrical Engineering TR-179, Massachusetts Institute Technology, Laboratory for Computer Science, May, 1977.

[4]
Landwehr, C., Heitmeyer, C., McCleen, J.
A Security Model for Military Message Systems.
ACM Transactions on Computer Systems 2(3):198-222, August, 1984.

[5]
Lipner, S.
Non-Discretionary Controls for Commercial Applications.
In *Proceedings of the 1982 Symposium on Security and Privacy*, pages 2-10. IEEE Computer Society, Oakland, California, April, 1982.

[6]
Rotenberg, L.
Making Computers Keep Secrets.
Ph.D. Thesis, Dept. of Electrical Engineering TR-115, Massachusetts Institute Technology, Laboratory for Computer Science, February, 1974.