

# Enclaves and Collaborative Domains

James A. Rome<sup>1</sup>

Computer Science and Mathematics Division  
Oak Ridge National Laboratory, Oak Ridge, TN 37831

E-mail: jar@ornl.gov

## Abstract

A well-defined policy forms the basis for implementing security and for determining if the policy is being enforced. Policies become more difficult to define when multiple sites are involved, or when resources are controlled by different people. By splitting the problem into local enclaves and collaborative domains, which define policy across enclave boundaries, it becomes easier to express policies and to resolve differing site policies.

## Introduction

Enclaves are defined as a set of information and processing capabilities that are protected as a group. The information processing capabilities may include networks, hosts, or applications. What determines when an enclave should be used?

### *Need for an enclave*

An enclave is required when the confidentiality, integrity, or availability of a set of resources differs from those of the general computational environment. An enclave is local to a site, and thus does not cross organizational boundaries. In addition, there needs to be a good reason for treating these resources as a separate, defined entity (association). Some examples that illustrate the need for an enclave are:

- ❖ A set of resources requires uninterrupted 24/7 availability.
- ❖ Proprietary information must be shared among several computers.
- ❖ A mission-critical database must be protected from any possibility of being changed.
- ❖ A remotely-operated facility has special quality of service (QOS) needs.
- ❖ Members of a wireless LAN might be required to take action to prevent weak wireless encryption from exposing their data.

---

<sup>1</sup> The submitted manuscript has been authored by a contractor of the U.S. Government under Contract No. DE-AC05-00OR22725. Accordingly, the U.S. Government retains a non-exclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

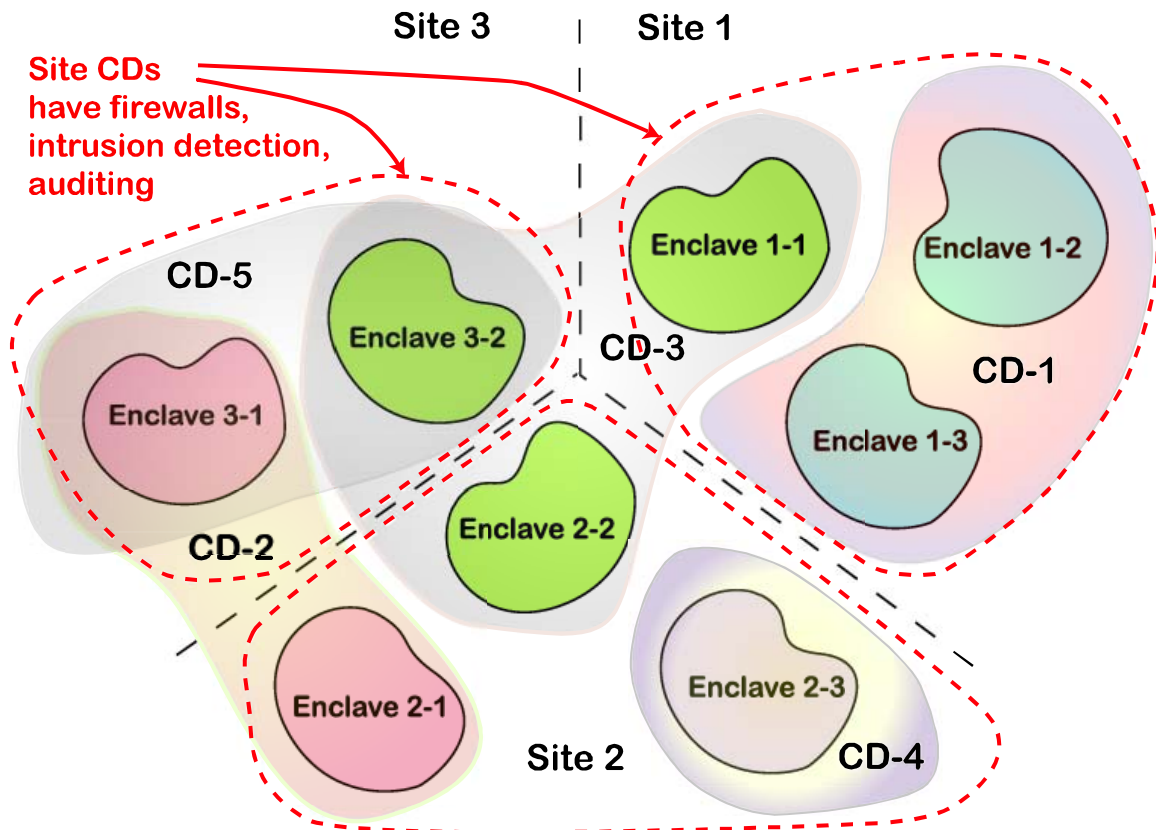
## ***Collaborative domains***

As defined, an enclave cannot cross organizational boundaries. A Collaborative Domain (CD) connects or contains enclaves at one or more sites, and is the natural mechanism for instantiating inter-organizational collaborations. The CD provides the association aspect of the enclave. Like an enclave, a CD provides a framework whereby a set of information and processing capabilities are defined and protected as a group. While a CD may be associated with one or more enclaves, an enclave is always associated with at least one CD. In other words, the CD associated with an enclave provides the reason for treating the enclave resources as a group. The enclave implementation policies are site-specific, but if the enclave is associated with a cross-site CD, the CD's requirements must not conflict with those of the enclave. This also implies that every CD policy and implementation needs at least two different approvals, one from the hosting site enclave, and one from the associated CD(s).

Every enclave is in an "external" CD that defines the Enclave's relationship to the rest of the world. All other CDs must give the CD members some special privileges or extra security that is the essence of the CD policy.

Some examples of CDs are:

- ❖ The automatic "external" CD that defines the Enclave's relationship to the rest of the world.
- ❖ A proposal writing effort with participants from several different sites that might need to access resources on one or more of the sites. The special privilege might be to access the proposal files on computers spread across the CD.
- ❖ A Multi-site remote microscopy collaboratory. Microscopes at each site are operated by remote users. Special CD requirements might be proof of training and protection of proprietary information. Site access might be via PKI certificates valid for only the session time.
- ❖ A Diesel Collaboratory CD might have special rules that pool proprietary data from different manufacturers, but assuring that each manufacturer can only "see" his own data except in statistical analyses. When the CD dissolves, each manufacturer removes his own data.
- ❖ The rules governing how home users (in a Home Enclave) remotely connect to their place of work.



**Figure 1. Collaborative domains and enclaves at three sites.**

Shown in Fig. 1 are three sites with enclaves, and five collaborative domains. All the different possibilities are illustrated:

- ❖ CD-1 connects two enclaves at a single site.
- ❖ CD-2 connects two enclaves at different sites.
- ❖ CD-3 connects three enclaves at three sites.
- ❖ CD-4 is associated with a single enclave. There can be no “bare” enclaves,
- ❖ CD-5 illustrates the point that a single enclave can be a member of more than one CD. In that case, both CD policies must be cognizant of this situation and accept it.
- ❖ A CD cannot be in *part* of an enclave. Enclaves are indivisible.
- ❖ The Site CDs provide site-wide services for all enclaves to provide a base level of security. The Site CD provides firewalls, intrusion protection, auditing, and a site-wide security plan.

In general, a CD has its own security policies which in general differ from those of the hosting institutions. How can the CD be assured that its security requirements will be enforced and respected by the host institutions? If the individual enclaves do not provide the necessary mechanisms, the CD must supply them. For example, if a remote microscopy CD requires training in order to use a microscope, the CD can require that a digitally-signed proof of training be presented to gain access to the enclave containing the microscope. Conversely, by its approval of the enclave policy, the site assures itself that the site’s infrastructure will be protected and appropriately used by the CD.

A problem with the definition and delineation of protection levels by means of enclaves is that many site resources may be unique and expensive. The large supercomputers and online electron microscopes probably should be located within enclaves that provide increased security, availability, or integrity; yet it is these resources that are most in demand for cross-realm collaboration. In Fig. 1, Enclave 3-2 might represent an enclave containing such a resource that is shared by several CDs. Either the resource in question must be able to keep the data from each enclave separated, or the different CDs connecting to the Enclaves must accept the lack of data security.

The enclave is a site-specific entity that must satisfy the site's security guidelines. But if the enclave is to connect to other enclaves and thereby give special privileges to that connection, it is the responsibility of the CD to adjudicate this inter-enclave trust. For example, the CD sends a resource request to a member enclave that is then free to approve or to deny it.

The proper split between enclave policy and CD policy allows us to look at the enclave in a less-complicated way.

### ***Enclave general principles***

The discussion can be clarified by looking at the problem from a higher level to determine what properties a generic enclave must have. To embed an enclave into a computer network requires that a set of five principles be satisfied:

#### ***1. Every computing resource must be in one and only one enclave unless it can prevent commingling of data from separate enclaves***

By computer resource, we mean a computer, printer, file server ... that can contain information or processing capability that must be protected.

- ❖ The network is generally outside of the enclave unless, for example, it connects two spatially-separated parts of a single enclave. Otherwise, the CD connecting the enclaves would specify the level of protection required (e.g., encryption) on the network link.

If a resource is in two enclaves, a way must be devised to assure prevention of commingling of the data from the two enclaves. For secure systems mandatory access control<sup>2</sup> (MAC) enforces a "need to know," and assures that data are kept separate. For more open systems, proper discretionary access controls (DAC), such as placing the enclave members in a single group and properly setting file access permissions might suffice.

- ❖ Every resource *must* be in an enclave in order that its protection level can be initially defined.

#### ***2. A user (or a process initiated by a user) enters an enclave when a resource in the enclave is used***

In general, the user will be accessing an enclave resource from a computer in a different enclave. Thus, a user can be in multiple enclaves at the same time.

- ❖ The enclave owner determines the list of authorized enclave users and must keep this list up to date.

---

<sup>2</sup> Mandatory access control prevents a user from sharing a file with another user unless both have the same security level and "need to know."

- ❖ Resource access can be controlled in three ways:
  - Physical access
  - Policy
  - Process — implements a policy

3. *“Entering” a different enclave from a CD or another enclave must entail some sort of access control*

Resources and information in an enclave have an owner that is determined by the CD and enclave policies. Only the owner of the resource can determine how access can be controlled, but this must be in accord with the policies of the enclave and the CD. If the entered enclave is different, it has different protection requirements, and they must be enforced with the proper assurance level.

- ❖ Processes acting on behalf of a user (or other processes) need to be traceable to a real person because it is the person whose access ultimately must be controlled.
- ❖ Unless an enclave has *no* user-based access controls, it does matter *where* a process runs, because its owner must be able to achieve authorization. For example, GRID computing assumes that it is acceptable for a task to run on any suitable resource on the GRID. However, “suitable” must be extended to include “is allowed access.”

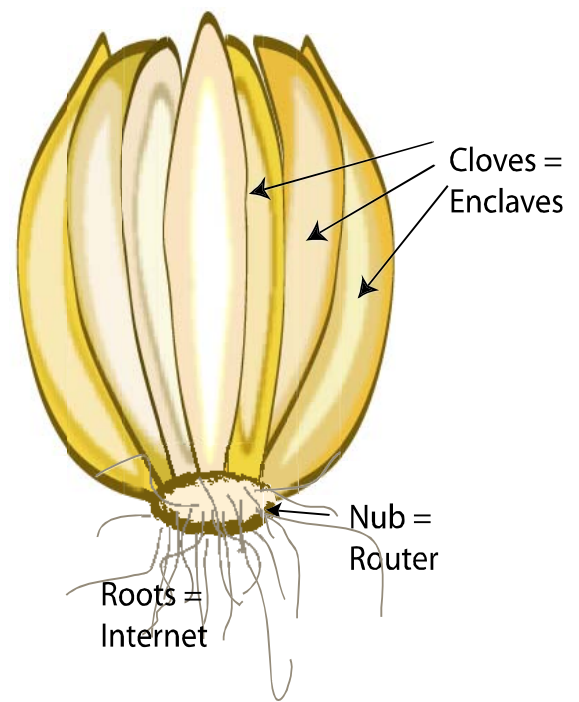
4. *Data can only be moved between enclaves by a user (or a user process) who is a member of both enclaves*

This implies trust of the user by both enclaves. After information is moved from the enclave to the CD, it is the CD policy that controls further distribution. Mandatory access control (MAC) could enforce permissions on such data transfers. This principle allows a user in *Enclave A* to use shared resources in *Enclave B* provided that *Enclave A* is satisfied as to the protection of its information in *Enclave B*. This implies that the protection level in *Enclave B* is at least as high as in *Enclave A*.

- ❖ An enclave could extend a portion of itself outside of the enclave to interact with the world, for example by a form on a secure Web page, or by a public information server. This is governed by the rules of its External CD.
- ❖ It is the CD policies that determine the inter-enclave trust policy mechanisms.

5. *For all its enclaves, a CD must satisfy the enclave security requirements imposed on the CD by the enclave plus those unique to the CD*

This principle allows the CD to function within and across organizational boundaries. For example, the organization must determine and approve enclave access controls and user member requirements. It



may also determine the appropriate level of audit trails.

The advantage of an enclave model is that it changes the problem of protecting a large, mixed domain into the protection of multiple homogeneous domains. It represents a change in philosophy. Previously, site security was modeled after an onion with concentric layers of protection making the inner layers increasingly secure. In the onion model, a layer is responsible for protecting all the deeper layers, and it is in turn protected by the outer layers.

The enclave model is analogous to a head of garlic. Each enclave is analogous to a garlic clove, with its own hard protecting shell. Not shown in the figure is the wrapper protecting the whole head of garlic, which is analogous to the site firewall.

Enclaves can only interact with each other (i.e., transfer information) by going through a router at the nub, at which point access control and routing decisions can be made. The roots allow CDs that span sites to connect to its member enclaves.

### ***Policy definition issues***

Creating a good security policy is not simple, especially if one wants to avoid unnecessarily restrictive “one size fits all” approaches. In the past, security policies were essentially equated with file protection, which mainly covers the “C” of confidentiality, integrity and availability (CIA). For example, compartmented mode workstations (CMWs) use hierarchical security levels and need to know compartments, along with mandatory access control to enforce such access. However, in today’s cyber world, much more complicated security policies might be needed. Here are some examples:

- ❖ Access is only allowed for a reserved session time on a piece of remote-controlled equipment.
- ❖ Authorization is allowed after approval by 2 out of 5 Vice Presidents.
- ❖ You are only allowed access during business hours.
- ❖ You need to present proof of training (or payment) before you are allowed on.
- ❖ You can only give this information to a certain group of people.
- ❖ You must be a U.S. citizen.
- ❖ An executable program changes according to who is running the program. For example, some remote electron microscope controls are grayed out. The enclave must then provide the program with the strongly-authenticated user ID.
- ❖ A computing facility needs 24/7 availability.
- ❖ A large scientific database must notify users when data they obtained via queries has later been modified, for example because the data owner found his instrument was miscalibrated. (This is an important unsolved problem.)
- ❖ External sponsors require extra security measures.
- ❖ Stakeholders impose extra requirements of users before access is to be allowed, for example computer security training.

There are also important questions that must be answered:

- ❖ What happens to information if a user leaves a CD?
- ❖ How do you know that a resource is being used for its intended purpose, especially if the information flow is encrypted?

- ❖ What should be audited and by whom?
- ❖ Who maintains and updates the policies?
- ❖ What happens if the CD is dissolved?

Some of these policy examples are enclave-specific, but most really apply to the CD. But, because every enclave is associated with at least one CD, the policies of the enclave and its CD(s) become intertwined.

### **Enclave policy scope**

If several enclaves are members of the same CD, presumably, the other enclaves gain special privileges by virtue of this membership. These special privileges are under the purview of the CD. Otherwise, an enclave considers access from any other domain as being “external.” Thus enclave policy is more restricted in scope than the CD policy. The enclave policy only enforces the requirements of the host institution.

### **CD policy scope**

It is only when the entrant to an enclave is given special privileges by virtue of being from a certain other enclave or being on a membership list that the CD policy comes into effect to enforce this special relationship. The CD policy also enforces any requirements that the CD might have that are over and above those of the host institution(s).

### **An example**

In Fig. 1, if Enclave 2-1 is *Top Secret*, and Enclave 3-1 is *Secret*, a valid CD-2 policy would enforce “write-up” and “read-down.” The enclaves could be connected by a properly-configured ftp server on Enclave 2-1 that would allow Enclave 3-1 members to upload files to a “write-only” directory, and Enclave 2-1 members to pull files from a directory in Enclave 3-1 that they were able to read. The Enclave 2-1 policy would determine the “proper” configuration of the ftp server, and the subset of CD-2 members allowed to access Enclave 3-1.

### **Policy framework**

There exist formal languages for expressing security policies, but they seem to be overkill for these purposes. What is needed is general agreement among the CDs and their enclaves on general protection requirements for different types of resources. A suggested method for implementing these policies should be provided, but other methods that satisfy the requirements should also be accepted. Methods and requirements for accessing a resource from inside and outside its enclave and CD must be defined.

To succeed this effort will require input, cooperation, and acceptance by the various Organization heads of security.

## **Enclave types**

For ease of administration, enclaves can be divided into several broad categories:

### ***Sensitive information***

These enclaves contain sensitive information that should not be accessed by the general population except through securely-designed interfaces. Examples of these enclaves include

- ❖ Business systems

- ❖ Human Resources, HIPPA
- ❖ Sensitive data such as trade secrets or labeled information (UNSR, Sensitive, UCNI)

### ***Public information servers***

- ❖ [www.ornl.gov](http://www.ornl.gov)

### ***Community resources***

Perhaps the trickiest enclaves to instantiate are those that constitute a resource that will be used from several other enclaves. They are thus in several CDs.

- ❖ Supercomputers
- ❖ GRID computing
- ❖ National facilities (e.g., the Spallation Neutron Source at Oak Ridge).

### ***User facilities***

User facilities are often accessed remotely by multiple classes of users, for perhaps a single session, and the data may be proprietary. Some user facilities at Oak Ridge National Laboratory (ORNL) are:

- ❖ High Temperature Materials Laboratory (HTML)
- ❖ High Flux Isotope Reactor (HFIR)

### ***Everything else***

By implication, anything that is not in a specific enclave is in the “general” enclave. The reason for this is that it serves to define the policies for the general population so that they can be reconciled with any enclave that is entered.

However, often these boilerplate enclave policies will be modified to meet specific requirements.

## **Security requirements**

A major purpose of establishing enclaves and collaborative domains is to be able to create valid, enforceable, and accountable security plans. Here we discuss some general requirements, vulnerabilities, and threats, and give an example showing how this enclave/CD infrastructure makes it more obvious how to create and implement a security plan.

When determining the network security requirements for an enclave and/or CD, one can use something similar to the DOE Cyber Security Architecture guidelines<sup>3</sup> to define

- ❖ the sensitivity of the resources — CIA;
- ❖ the external threat;
- ❖ the degree to which the enclave network structure, services, and resources should be exposed to external view and/or access;
- ❖ the type of network intrusion detection and response appropriate for the enclave;

---

<sup>3</sup> Cyber Security Architecture Guidelines, U.S. Department of Energy, DOE G 205.1-1 March 8, 2001.

- ❖ which network services are essential for business/mission operations (e.g., file transfer, email, DNS, World Wide Web, remote access, network management, collaboration, multi-media);
- ❖ best industry practices for securing essential network services and the risk tradeoffs associated with alternatives that may provide greater access, performance, or functionality;
- ❖ the ways that enclave network resources might be exploited to cause harm to external networks/enclaves; and
- ❖ alternative controls at the host and application view that complement network controls.

To create a security policy we must consider the vulnerabilities, threats, and mitigation techniques in the enclave/CD framework.

### ***Vulnerabilities***

Enclaves are inherently vulnerable if their policies and memberships are not maintained.

- ❖ A terminated enclave member may still have access to some enclave devices.
- ❖ Improper disposition of enclave assets upon dissolution of the enclave may allow access to restricted enclave information.
- ❖ Trust in enclave members may be misplaced.

Enclaves may also be vulnerable if the infrastructure is improperly configured, because that could allow leakage of information across the enclave boundaries.

The other information leakage channel is via unauthorized access to the enclave through its interface to the world. Either the devices within the enclave must all have proper access controls, or the enclave itself must be protected by a network device that performs the authentication process. Vulnerabilities are related to the membership of the enclave and the use of the information in the enclave:

- ❖ Failure to update the authorization list when membership of the enclave changes.
- ❖ The enclave could have members not acceptable to the host organization (e.g., foreign nationals from other sites). For example, the owner of a UNIX machine could make user accounts without using a site's user control mechanisms that would be accessed via an encrypted protocol.
- ❖ Once information is removed from the enclave by an authorized user, the enclave no longer has control over its use.

### ***Threats***

An enclave is subject to most of the same threats as a general network, but it also has its own particular threats:

- ❖ Access to unauthorized accounts in the enclave. In particular, the originator of encrypted access to user accounts cannot be detected by network intrusion detection devices..
- ❖ Access to the enclave by exploiting vulnerabilities in services that are allowed to enter and exit the enclave.
- ❖ Direct access to an enclave device that does not have authentication (e.g., a PostScript printer that can execute commands).

## ***Risks and concerns***

These vulnerabilities and threats result in the following risk and concerns:

1. Information disclosure
2. Data theft or interception (sensitive and nonsensitive) by packet capture between the enclave entrance and the enclave remote user unless encryption is used.
3. Unauthorized access to enclave data via services on enclave computers (e.g., Web servers).
4. Unauthorized connections to/from the enclave
5. Access by “plugging into” a data port that is a member of the enclave.
6. Creation of unauthorized enclave accounts by enclave members, and their use.
7. Unauthorized access to devices in the enclave that lack authentication.
8. Secure authentication of users not being applied to all enclave resources.
9. The ability to associate enclave logs with users (for forensics).
10. Protect authentication credentials (encrypted and preferably one-time passwords).
11. Connection of enclaves by user processes. For example, making a device in an enclave a member of a GRID that is not contained in the enclave.
12. Dissolution of an enclave and proper disposition of its resources. Will the information in the enclave be destroyed, remain protected according to the enclave guidelines, or merged into another enclave?
13. There must be owners assigned the equipment and information in the enclave.

## **An extended example**

A group of PC users sometimes work with sensitive data that must be protected. However, when they are not working with the sensitive data, they would like to surf the Web, get e-mail, and in general behave as if they were normal computer users. By splitting the group into two enclaves and a collaborative domain, it makes it clearer where the particular security issues lie. Once the enclaves and CDs are defined, a solution to the problem suggests itself.

### **Vulnerabilities**

The Sensitive Enclave contains information that is sensitive and cannot be accessed without strong authorization. It can only be transferred to authorized parties using string encryption.

- Malicious code contained in the submitted Sensitive data.
- Access to unallowed information from within or without.
- Vulnerabilities due to unpatched software.
- Virus and worms not caught because of a lack of antivirus software or antivirus software that is not updated.
- The Sensitive data repository is in one location and needs off-site backup for disaster recovery.

## **Threats**

The list of potential threats specific to the Sensitive Enclave is provided below:

- The biggest threat is posed by a legitimate Sensitive User disobeying the rules and transferring data outside the Enclave to unauthorized entities.
- Attack on the Enclave at the network interface.

## **Unmitigated Risk and Concerns**

These vulnerabilities and threats result in the following risk and concerns:

1. Information disclosure by a malicious user, malicious software or hardware, or by remote hackers
  - a. Data theft or interception (sensitive and nonsensitive) by packet capture on the Enclave LAN.
  - b. Sensitive data remaining on a user's machine after the connection to the server is terminated.
2. Interception of encrypted data on the target computer when it has been transmitted to a sponsor.

## ***Security Policies***

Based upon the above discussion and a questionnaire filled out by the enclave owner, we can create security policies for the Sensitive Enclave and Collaborative Domain. We split the enclave into two parts: a Sensitive Server Enclave that contains the data, and a Sensitive User Enclave that contains the Users.

### **Sensitive Server Enclave security policy**

This enclave consists of Microsoft Windows computer servers and printers that contain or process Sensitive data, with no non-administrative user accounts. These devices shall all reside on a private VLAN (Sensitive Server VLAN).

- They shall reside a locked computer room.
- IPSEC will be enabled for TCP/IP (this requires Windows 2000 or higher). IPSEC encrypts information flow to and from network mapped drives.
- Security-related operating system and application bugs shall be patched promptly.
- Windows PCs shall have up-to-date antivirus protection.
- All administrative functions shall be performed from the console.
- Each Server shall have personal firewall and malware detection software installed.
- There shall be periodic backups stored in an appropriate sensitive data safe.
- Incoming access shall only be from the Sensitive User Enclave VPN addresses, plus the company ISS scanner and patch server.
- Printers for Sensitive data shall be in the Server Enclave.
- No outgoing connections will be allowed.

### **Sensitive User Enclave security policy**

The Sensitive User Enclave consists of Microsoft Windows personal computers used by members of the enclave for their work. They shall all be on the same private VLAN (Sensitive User VLAN).

- These computers shall all have
  - Up-to-date anti-virus software
  - Personal firewalls
  - Patches obtained from the Company patch server
  - Malware detection software that includes a keystroke sniffer detector.
  - IPSEC enabled for TCP/IP (this requires Windows 2000 or higher).
- Users shall all have up-to-date computer security training.
- Users shall have an additional userID that is enrolled in the VPN Sensitive Group.
- No incoming access will be enforced by the VLAN policy.

### **Sensitive Collaborative Domain security policy**

- User access to the Sensitive Server Enclave shall be accomplished via a captive tunnel from the Sensitive User Enclave.
- ISS scanning and patch server access will be allowed.
- During use of Sensitive data, all files shall remain on the Sensitive server(s).
- Any data transferred out of the Sensitive Enclave shall be strongly encrypted.

To accomplish data transfer between the two enclaves, the VPN shall be configured as follows:

- All users in the Sensitive Enclave placed into a separate VPN group.
- They will be identified by their alternate userID, and shall use one-time password tokens to authenticate to the VPN server (via RADIUS).
- When the VPN tunnel is connected, it shall be captive, i.e., *all* traffic from the Sensitive User Enclave users shall be directed through the tunnel.
- The Sensitive Users Enclave members shall only be allowed to connect to the Sensitive Server Enclave VLAN when the VPN tunnel is in place.

The users have to obey policies from the Collaborative Domain.

- When the users work with sensitive data, *all* files shall remain on the server.
- When users wish to transfer files out of the Server Enclave (in order to send them to their sponsors, for example), the file shall be encrypted with the recipient's public key on the server and then transferred to the user's PC. The VPN tunnel will then be dropped.

The Sensitive User Enclave is actually in a second CD (in addition to the general one all organization users reside in), namely the remote Sensitive User Enclave(s) in which their sponsors, customers, etc. reside. The following CD policies apply to such transfers:

- Any transfers of the encrypted sensitive files out of the Server Enclave shall be logged in writing with the date, userID, file name and recipient's name.
- The user shall attach the encrypted file in an e-mail message to the recipient. It shall be signed with the user's private key and if possible encrypted also.

## **Conclusions**

By splitting security into enclaves and collaborative domains, it is easier to specify the policies, and to determine exactly who has to approve the policies. This is especially important in cross-realm collaborations where the security chiefs at the separate sites and the collaboration owners all have to approve. The split allows each organization to enforce its own enclave policy, and if it conflicts with the policy of the collaborative domain, decide whether or not to make an exception.

## **Acknowledgments**

The author would like to thank Walter Dykas (Oak Ridge National Laboratory) for his insightful comments. J. D. Pfluckiger (Pacific Northwest National Laboratory) first introduced the concept of collaborative domains, but his enclaves could cross site boundaries, and were also divisible, so that a CD could be in only part of an enclave.