

Modern times

- Different assets need different types of protection against different threats
- Isolated computers are a rarity
- We have large holes in our defenses in order to provide services to the world
 - ⇒ Should I be at risk because someone I have no control over has not patched their system?
 - ⇒ I cannot even get friends to write Web services that protect against cross-scripting and SQL injection attacks by validating inputs.

Divide the domain and provide appropriate protection to each one

Collaboration

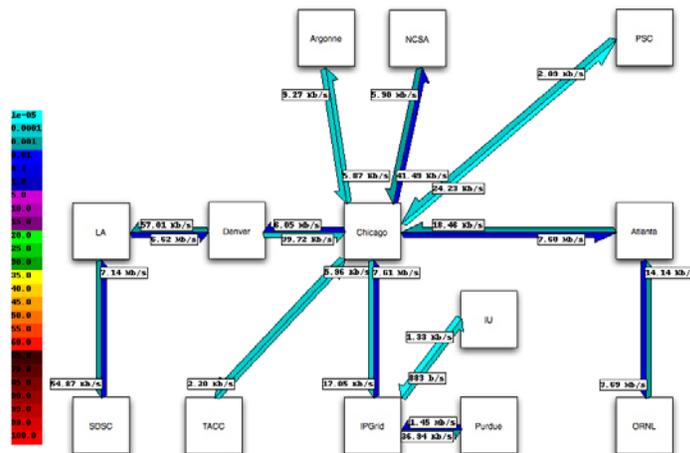
We also live in a world of virtual organizations

- DOE requires three Labs on a SciDAC proposal
- The NSF-funded TeraGrid is a good example of a cross-realm organization
 - ⇒ A common network infrastructure
 - ⇒ A common set of software (CTSS)
 - ⇒ Some common policies
 - ⇒ Separate computer centers under their own control, and each connected to the outside world

**Creating security policies and evaluating risk is a challenge in these collaborative domains
(I am leading the TeraGrid risk analysis effort)**

TeraGrid topology

Mon Apr 17 18:55:51 2006



OAK RIDGE NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY

UT-BATTELLE

5

What is an enclave?

A collection of computer resources that are to be protected at the same level and are also associated in some way.

- In my definition, an enclave is an entity run by one organization.
- Enclave policy and implementation are controlled by the organization.

OAK RIDGE NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY

UT-BATTELLE

6

When do you need an enclave?

If the confidentiality, integrity, or availability of a set of resources differs from those of the general computational environment.

These resources need to be treated as a separate, defined entity (association). For example:

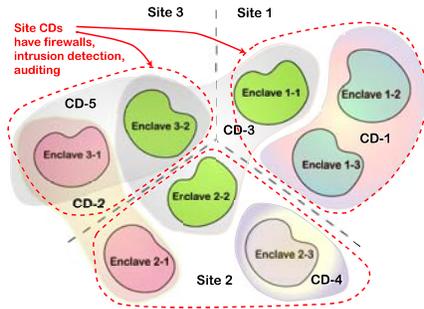
- **Resources that require 24/7 availability**
- **Proprietary or sensitive information shared among several computers**
- **Mission-critical databases**
- **Collaboratories**

Collaborative Domains

A Collaborative Domain (CD) connects or contains enclaves at one or more sites.

- **The natural mechanism for instantiating inter-organizational collaborations.**
- **Every enclave is associated with at least one CD.**
- **CD policies and implementation instantiate cross-realm trust.**

The big picture



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.

OAK RIDGE NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY

UT-BATTELLE

9

Example of a CD policy

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 on Enclave 2-1
- allow 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.

OAK RIDGE NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY

UT-BATTELLE

10

How to make sense of this all?

Step back and consider the general principles that an enclave must satisfy.

Every computer 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 data that must be protected.**
- **Every resource *must* be in an enclave in order that its protection level can be defined.**

A user (or a process controlled by the user) enters an enclave when a resource in the enclave is used

In general, the user will be physically on a computer in a different enclave. Thus, a user can be in multiple enclaves at the same time.

Issues:

- Who determines the list of authorized enclave users and how is this list kept up to date?
- Resource access can be controlled by
 - ⇒ Physical access controls
 - ⇒ Policies
 - ⇒ Processes

“Entering” a different enclave must entail some sort of access control

In general, the information and resources in an enclave are owned by the enclave.

- Ultimately, the enclave owner determines access.

But,

- Processes acting on behalf of a user (or other processes) need to be traceable to the root owner because it is the owner whose access 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.

Data can only be moved between enclaves by a user (or user process) that is a member of both enclaves

This implies trust of the user by both enclaves.

- **It is the CD policies that determine the inter-enclave trust policy and mechanisms.**
- **An enclave could extend a portion of itself outside of the enclave to interact with other enclaves, for example by a form on a secure Web page, or by a public information server.**

An enclave must satisfy the security requirements of all the entities of which it is a member

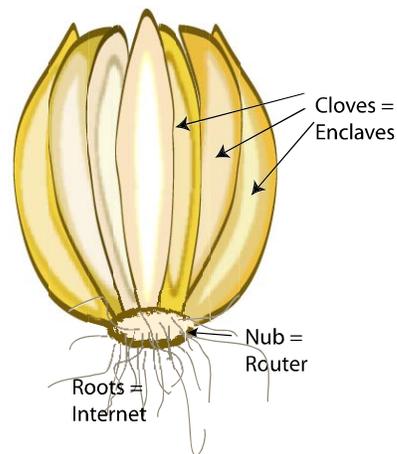
The site and the CD must both approve the enclave policy.

- **Site determines**
 - ⇒ User access controls
 - ⇒ membership policies
 - ⇒ Required audit trail
- **CD determines**
 - ⇒ Cross-enclave policies
 - ⇒ What happens when members leave or the CD is dissolved

The garlic model of an enclave

The old model was an onion with nested spheres of increasing protection. Our new model is a head of garlic.

- Not shown in the figure is the garlic wrapper protecting the whole head, 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.
- A bad clove does not affect the rest of the head.



OAK RIDGE NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY

UT-BATTELLE

17

Enclave policies

The enclave is concerned with more localized issues:

- Data must be only available to authorized users.
- Users must have valid UCAMS accounts.
- There must be provision for scanning computers for vulnerabilities.
- An audit trail may be required.
- Enclave ACLs must be maintained.
- Proper disposition of resources when enclave is dissolved.

OAK RIDGE NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY

UT-BATTELLE

18

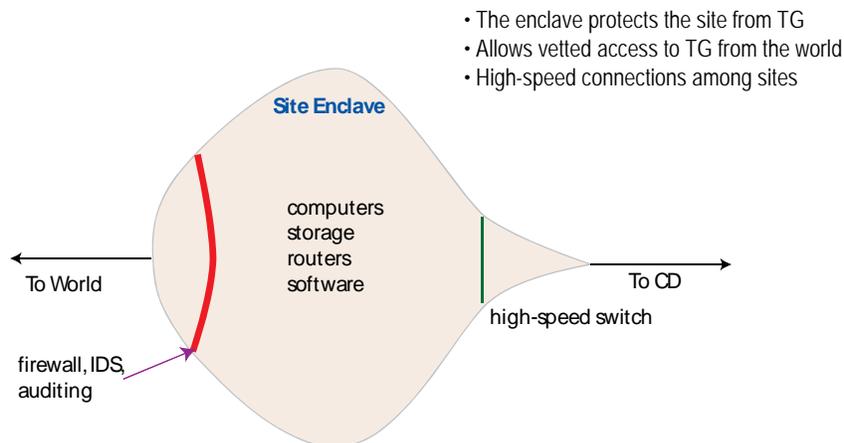
Policy resolution

The Enclave and CD policies may be different, but

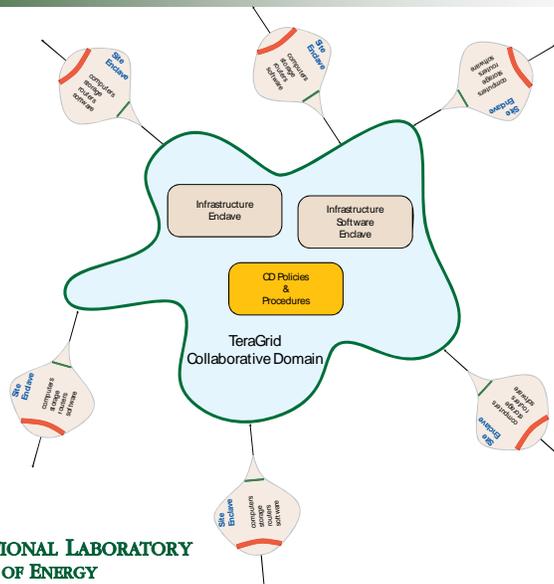
- They must be crafted so as to support each other.
- They must not interfere with each other.
- The enclave is NOT the entity to worry about cross-enclave trust if the enclaves are in the same CD. That is the responsibility of the CD.
- The enclave assumes that all entrants come from some other enclave and are “external.”
- It is only when the entrant is granted a special privilege by virtue of being from a certain enclave that the CD policy kicks in to enforce the special relationship.

It is often difficult to prove (or to ensure) that a policy is enforced.

TeraGrid — a site enclave



TeraGrid — Proposed decomposition



OAK RIDGE NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY

UT-BATTELLE

21

TeraGrid Risk Assessment

- I am leading the TeraGrid risk assessment.
- The concept of enclaves and collaborative domains helps split the large heterogeneous structure into well-defined chunks.
 - ⇒ The C,I,A = Low, Medium, High categorization can be different for each chunk
 - ⇒ The controls needed to mitigate the risks in each chunk can be different and more appropriate
- Creating policies for the CD is a challenge.
 - ⇒ Accepted CAs, incident response play book, acceptable use agreement

OAK RIDGE NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY

UT-BATTELLE

22

The harder issues . . .

- **TG connects the academic and DOE realms which have differing legal requirements:**
 - ⇒ Access by non-citizens to supercomputers
 - ⇒ Export control regulations
 - ⇒ Proprietary data
- **Some supercomputers are in both TG and the university enclaves. How do you separate these domains?**
- **How do you enforce agreed-upon policies?**
 - ⇒ Students leave and “give” accounts to other students
- **Light-authentication portals need restricted access to resources**