Foundations of Computer Security

Lecture 25: The Chinese Wall Policy

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

The Problem

The policies so far have been general. Let's consider a policy for a very specific commercial concern: *the potential for conflicts of interest and inadvertant disclosure of information by a consultant or contractor.*

Example: A lawyer specializes in product liability and consults for American Airlines. It could be a breach of confidentiality for her to consult also for United Airlines. *Why?* A simultaneous contract with McDonalds would not be a conflict.

Chinese Wall Policy

Brewer and Nash (1989) proposed a policy called the **Chinese Wall Policy** that addresses such conflicts of interest.

Strictly speaking, this is not an integrity policy, but an access control confidentiality policy.

Levels of Abstraction

The security policy builds on three levels of abstraction.

Objects such as files. Objects contain information about only one company.

Company groups collect all objects concerning a particular company.

Conflict classes cluster the groups of objects for competing companies.

For example, consider the following conflict classes:

- { Ford, Chrysler, GM }
- { Bank of America, Wells Fargo, Citicorp }
- { Microsoft }

Chinese Wall Policy

We have a simple access control policy: A subject may access information from any company as long as that subject has never accessed information from a different company in the same conflict class.

For example, if you access a file from GM, you subsequently will be blocked from accessing any files from Ford or Chrysler. You are free to access files from companies in any other conflict class.

Notice that permissions change dynamically. The access rights that any subject enjoys *depends on the history of past accesses*.

Chinese Wall

Formally, the policy restricts access according to the following two properties:

(Chinese Wall) Simple Security Rule: A subject s can be granted access to an object o only if the object:

- is in the same company datasets as the objects already accessed by s, that is, "within the Wall," or
- belongs to an entirely different conflict of interest class.

(Chinese Wall) *-property: Write access is only permitted if:

- access is permitted by the simple security rule, and
- no object can be read which is:
  - in a different company dataset than the one for which write access is requested, and
  - contains unsanitized information.

Lessons

- Unlike previous policies, Brewer and Nash's Chinese Wall Policy is designed to address a very specific concern: conflicts of interest by a consultant or contractor.
- This illustrates that security policies can be crafted to solve very specialized problems.
- The Chinese Wall is an access control policy in which accesses are sensitive to the history of past accesses.

Next lecture: Role-Based Access Control