Review of: A Lattice Model of Secure Information Flow
Paper By: Dorothy E. Denning

Reviewer: Vicky Weissman

March 22, 2001

The paper has 2 distinct parts. The first presents a model for information flow and proves that, under reasonable assumptions, the model can be used to construct a universally bounded lattice. The second part is a discussion of security mechanism that are used to enforce flow restrictions.

Definitions:

- A flow model (FM) is a 5-element tuple, $\langle$N, P, SC, $\oplus$, $\rightarrow\rangle$, in which N is the set of objects or 'information receptacles', P is the set of active agents or processes, SC is the set of security classes for both objects and agents, $\oplus$ is a binary operator that combines security classes, and $\rightarrow$ contains the legal 'flows' (for example A $\rightarrow$ B means that information from class A is allowed to flow to class B.) The security classes are closed under $\oplus$.
- Information flows from A to B if the information associated with A affects the value of the information associated with B.
- A flow model is secure iff there does not exist a sequence of operations which results in a flow that violates the $\rightarrow$ relation.
- A flow model is consistent iff all flows implied by a permissable flow is permitted by the $\rightarrow$ relation.
- A universally bounded lattice is a structure consisting of a finite partially ordered set, a least upper bound on the set, and a greatest lower bound on the set.

If we assume that the flow model is consistent, the set of security classes (SC) in the model is finite, and $\langle$SC, $\rightarrow\rangle$ is a partially ordered set, then $\langle$SC, $\rightarrow$, $\oplus\rangle$ form a universally bounded lattice. $\oplus$ is the least upper bound operator, also known as the join. The greatest lower bound must exist since it can be empty.

The lattice is suitable for hierarchically ordered sets such as the government's security levels (unclassified, confidential, secret, or top secret) and it also applies to property-based sets in which information can only flow to a set that has all of the sender's properties. Hybrid systems which combine these 2 types are also supported.

The discussion of mechanisms deals with both implicit and explicit flow. Implicit flow can only result from a conditional statement. For example, if a=0 then b:=c results in an implicit flow from a to b, regardless of a's value. The mechanisms themselves are not very interesting, particularly for our work, but the section includes 2 useful examples of security leaks. First, security violation reports can be used to convey information. For example, a high security agent could tell a low

security agent that the key is 27 by causing 27 security violations. Second, information can be leaked when an object's classification changes. For example, a low security agent will know that an object is high security when he/she notices that the object is no longer accessible (assuming that the object was not deleted.)