Specifications for Multi-Level Security and a Hook-Up Property
Paper By: Daryl McCullough

Reviewer: Vicky Weissman

March 22, 2001

This paper introduces the Hook-Up Theorem to determine if connecting secure components will result in a secure system. Although the proof of his theorem is given in a technical report, the paper does have a clear, succinct overview of the security models presented by Bell and LaPadula, Goguen and Meseguer, and Sutherland. Following the review, McCullough shows that none of these models are adequate for deciding if a non-deterministic system built from secure parts is secure. Finally, the hook-up theorem is stated with a reference to the technical report for details.

Review of Related Work:

Bell and LaPadula give a method for achieving an intuitive notion of security. The 2 other approaches attempt to define the meaning of security. More specifically,

- The Bell and LaPadula strategy requires that users only read objects at their level or lower and only write (or modify) objects at their level or higher.
- Goguen and Meseguer define security by the non-interference requirement that a user's actions can only affect users of an equal or higher level.
- Sutherland states that a user should not be able to deduce anything about the actions of higher level users.

Weaknesses of Related Work:

- The Bell and LaPadula approach does not handle information that is not in objects, does not handle operations other than read and write, and requires 'trusted subjects' such as the memory management which must access all objects.
- The Goguen and Meseguer definition does not have the property that 2 secure components necessarily form a secure system. The example concerns 2 connected components. The high-level output from the first must go to the second and the high-level output from the second must got to the first. Only the first component receives outside input. If both components state if they've seen an odd or even number of high-level events, then the 2 components can only have different answers if some high-level input has occurred. Therefore, the composed system is not secure by the noninterference definition, even though the 2 components are individually secure.
- The Sutherland definition does not match our intuitions about security for non-deterministic systems. To see this, consider a program that takes an integer from a low-level user and returns the corresponding bit of a high-level document. If the requested bit corresponds to

a portion of the file that has been erased or not yet written to, then the program returns a random bit. The program does not violate the deductibility requirement, but it clearly allows a low-level user to infer the contents of a high-level object with very high probability.

The Hook-Up Theorem:

Definition: Hook-Up Security

We will say that a system is hook-up secure if for all traces τ_1, and for all sequences τ_2 formed from τ_1 by adding or deleting high-level inputs, there is a trace τ_3 such that τ_3 is the same as τ_2 in the constant portion, and differs from τ_2 in the changed portion only in high-level outputs, and such that the first changed output of τ_3 occurs no sooner than the first output in the changed portion of τ_2.

Roughly speaking, a system is hook-up secure if it is possible to construct a valid trace by inserting or deleting high-level outputs from a sequence that was created by inserting or deleting high-level inputs from a valid trace.

If a system is hook-up secure, then it is secure by the non-interference and deductibility definitions. Furthermore, if a system consists entirely of components that are hook-up secure, then the system is hook-up secure.