APPLYING THE WDL COMPOSITION THEORY TO ANALYZE SECURITY ARCHITECTURES

Lee A. Benzinger
Lockheed Martin Western Development Laboratories
San Jose, California

1 Introduction

The Western Development Laboratories (WDL) composition theory is a mathematical theory for modeling large, complex communications systems. The modeling approach we use for both a system and its components is that of "black box" information flow models. We discuss applications of the WDL composition theory to analyze, at an architectural level, the functionality and security of a large system. We are able to determine the functionality of the system from the functionality of its components and the system architecture. Similarly, we are able to determine the system security policy, provided we know the system architecture and the security policies of each of its components. Often it is very difficult to determine the impact on a system as a whole that are due to changes in its architecture and/or changes in its components. We can apply the WDL theory to determine the impact on system functionality or security policy due to such changes.

1.1 Applying the WDL Composition Theory

This paper discusses applying the WDL composition theory to a large, complex, distributed communications system. The WDL composition was applied to this system to do an analysis of the functionality and the security of the system at the segment level. The application resulted in the ability to do back-of-the-envelope calculations to assess changes in system functionality and system security policy due to changes in the system architecture. These back-of-the-envelope calculations depend upon applying theorems that are already part of the WDL composition theory. No additional mathematical proofs are necessary for this particular application.

In this section we discuss the system to which the analysis was applied. We also present some general ideas on composition and modeling. In Section 2 we provide a brief overview of the WDL theory, including some examples in Section 2.5. In Section 3 we discuss the application to the communications system.

1.2 The System

The system to which we applied the analysis is already accredited as a B1 system [2]. It is a system with multisensor capability that is designed to support tactical units throughout the world. It consists of a sensor platform and four sensors, and two deployable ground stations.

This system is large, consisting of eight segments. One segment alone, the control segment, has over 3 million lines of code. This system is also complex. It separates flows of information based upon labels. Currently, it can handle about 1 million labels. Each label consists of 25 terms. Shortly, the number of labels will triple in order to support global deployment.

This system is also dynamic. It is going through a series of maintenance upgrades and has changed over 50% in the last two years. It is moving from a proprietary operating system for the control segment to an open system architecture using Commercial-off-the-shelf products. The upgrade will be using Compartmented Mode Workstation (CMW) technology.

Any changes in this system have potential impact on its security, functionality, and, consequently, its accreditation. The WDL composition theory was applied to support the analysis of several potential changes to the architecture of this system at the segment level. The results of this analysis provided immediate feedback on the impact on security and functionality due to these changes.

1.3 Composition

Fundamental to building or analyzing a system is the composition problem: If you have two components, and you wire them together in some fashion ("compose the components") to obtain a system, what can you say about the system in terms of its components? For example, if the functionality of the components were known, it would be desirable to be able to express the functionality of the system in terms of the functionality of its components. In building and analyzing secure systems, the secure composition problem can be stated as follows: If you have two secure components, and you compose them to obtain a system, what can you say about the security of the resulting system in terms of the security of its components?

1.4 Modeling

We can build components and systems and then analyze them for functionality and security. However, it is quite useful to model the components and system, first, before implementation. Modeling helps to obtain insight into the system being built or analyzed. Modeling also helps to provide assurance that the resulting system will be correct. In fact, modeling is required for certain kinds of high assurance systems described by the DoD Trusted Computer System Evaluation Criteria [2].

2 WDL Composition Theory

The WDL composition theory is intended to model message passing systems, such as packet-based communications systems. In this section we provide a brief overview of the WDL composition theory.

2.1 Models

The WDL composition theory is a mathematics for "bubble diagrams." Models for components and the system are represented graphically by circles or "bubbles". In system and software engineering terms, these components and system models are "black box information flow" models. "Black box" refers to the fact that the model identifies the boundary of the component or system. It also indicates what is inside and what is outside the component or system, but does not necessarily indicate the functionality of what is inside the boundary.

Relationships between components are represented by lines which connect the bubbles. The interfaces for the components and system occur where the lines connecting components intersect the bubbles. Possible information flow to and from components and the system is represented graphically by lines entering and exiting the bubbles.

2.2 Notation

In the WDL composition theory, we denote with uppercase letters, A, B, C, ..., both a component and its functionality. We denote by S a system and also its functionality, but conceptually, it is just like a component. We denote the security policy for a component A by P_A. Similarly, we denote the security policy for the system S by P_S.

2.3 System, Components, and Policies

Mathematically, components, the system, and their corresponding security policies are represented as sets in the WDL composition theory. A component, for example, is the set of all possible corresponding pairs of sets of its inputs and outputs. This is quite general, since it includes as a proper subset all systems that are (mathematically) functional in nature. For a mathematically precise definition of a component, a system, and a security policy, see [1]. Since components, the system and their corresponding security policies are sets, there is a convenient way to represent the statement that a component A satisfies its policy, P_A. It is simply $A \subseteq P_A$ or A is a subset of P_A.

2.4 Operations

For components and their policies there are two kinds of composition: serial and parallel. Serial composition of two components A and B is denoted by $A \circ B$. It represents the result of "wiring" the outputs from A to the inputs of B. Parallel composition of A and B is denoted by $A \cup B$. It represents the result of "wiring" A and B in parallel. It is also possible to intersect components and policies. For example, $P_A \cap P_B$ is the intersection of the security policies for A and B.

2.5 Examples

In this section we consider some examples of the composition problem for systems that have just two components, A and B. The "wiring" of the components A and B, whether it is serial or parallel, represents the architecture of S.

2.5.1 Example One: Composition

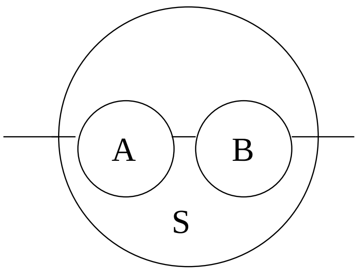

Figure 1: $S = A \circ B$

If S is the serial composition of components A and B, then $S = A \circ B$. See Figure 1. In terms of information flows for S, there is just one flow, namely from A to B.

If S is the parallel composition of components A and B, then $S = A \cup B$. See Figure 2. In terms of information flows for the system S, there are two flows, namely, through A or through B.

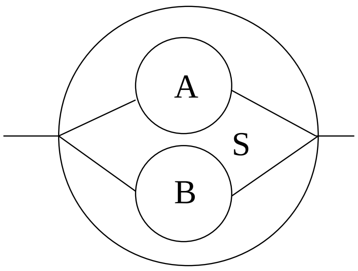

Figure 2: $S = A \cup B$

2.5.2 Example Two: Secure Composition

Suppose next that A and B are secure components, i.e., there are security policies P_A and P_B and $A \subseteq P_A$ and $B \subseteq P_B$. If S is the serial composition of components A and B, then $S = A \circ B \subseteq P_A \circ P_B$ from the subset theorems. What we have done is to show that the system S satisfies a policy that is expressed in terms of the security policies of its components. If S is the parallel composition of components A and B, then

$$S = A \cup B \subseteq P_A \cup P_B.$$

In Example 1, using the WDL composition theory, we have solved the composition problem of expressing the system functionality S in terms of its components, A and B. In Example 2, we have shown that the system S satisfies a policy that is expressed in terms of the security policies of its components. For serial composition,

$$P_S = P_A \circ P_B.$$

For parallel composition,

$$P_S = P_A \cup P_B.$$

3 Application of the WDL Theory

The application of the WDL theory to analyze a simplified version of the communications system uses the two operations of serial and parallel composition. These operations are applied to analyze flows for architectures consisting of three or four components. These architectures represent possible changes to the existing communications system. We were able to show that two candidate segment level architectures for this system resulted in different system functionality and different system security policies. The application of the theory involved applying some basic theorems to express the permissible flows through the system. The ease with which an analysis can be made allows experimentation with different architectures and different component functionality in the design or modification of a system. The impact of such change upon system functionality and system security policy can be, at least in the cases we have considered, easily determined.

References

[1] George W. Dinolt, Lee A. Benzinger, and Mark G. Yatabe. Combining components and policies. In Joshua Guttman, editor, *Proceedings of The Computer Security Foundations Workshop VII*. IEEE

Computer Society, IEEE Computer Society Press, June 1994.

[2] Trusted computer systems evaluation criteria. Technical Report CSC-STD-001-83, DoD Computer Security Center, Fort Meade, MD, August 1983.