Secure Distributed Heterogeneous Systems Management via Confederations and Oracles

William A. Arbaugh
Department of Computer Science

Virgil D. Gligor
Department of Electrical Engineering

University of Maryland
College Park, Maryland 20742

1 Introduction

The tremendous growth rate of the use of information technology has exacerbated the problem of effectively managing and securing the resultant information infrastructure. This coupled with the fact that the current state of the art in security is essentially "penetrate and patch" has created a situation where information technology is more vulnerable than ever[**?**]. The vulnerability of information technology is demonstrated by the large number of news stories relating to wide-spread computer intrusions as well as controlled network scanning[**?**][**?**]. For instance, the U.S. General Accounting Office released a report detailing scanning efforts by the U.S. Defense Information Systems Agency (DISA)[**?**]. During a three year period (1992-1995), DISA probed 38,000 different hosts for vulnerabilities finding 65% of all hosts vulnerable. While the GAO report did not specify what vulnerabilities DISA used to attack the military hosts, they likely used known vulnerabilities.

While previous studies and anecdotal evidence have demonstrated the increasing vulnerability of information technology, information security research is currently primarily focused on the underlying *security technology* rather than the secure management of the information technology. Yet, the tremendous growth in the use of information technology and it's rate of change creates a configuration and systems management nightmare that amplifies existing security problems, and also introduces new security problems as well. Current approaches for solving this complex problem are *ad hoc* and do not scale well. In this research, we will attack this situation by conducting a broad examination of distributed heterogeneous configuration and security management from both a theoretical and a systems approach. Ensuring that our approach scales and is based upon a formal representation.

In the remainder of this white paper, we first present our research objectives followed by our proposed technical approach. Next, the expected outcome and impact of the research is discussed. Finally, we conclude the paper.

2 Research Objectives

We have three primary research objectives:

1. XXXXX Virgil change this as needed XXXXX Develop a formal calculus for representing and reasoning about the configuration of distributed heterogeneous systems with respect to time.

2. Leveraging the calculus developed above- design and prototype a system for a scalable and secure distributed heterogeneous systems management that permits a range of manageability from fully automated to fully manual. Additionally, the system will permit readiness information to flow to parent organizations.

3. Investigate technology and methodologies for ensuring the state of an information system is as expected, i.e. a robust distributed independent audit capability.

3 Technical Approach

The first step in any research project is to understand the problem, and develop a formal model. The formal model provides the ability to reason about the domain, and serve as a sound basis for the systems engineering solution. Finally, once a solution is implemented an enforcement or auditing process is required to ensure that the system works as expected. Our technical approach will follow this methodology.

3.1 Formalization of Secure Distributed Hetergeneous Management

Year 1	$600,000
Year 2	$600,000
Year 3	$600,000
Year 4	$600,000
Year 5	$600,000

Table 1: Estimated costs by year

3.2 Methods for Secure Distributed Hetergeneous Management

XXXXX Discuss concept of confederations and information flows XXXXX

3.3 Enforcement of Configuration Management

XXXXX Komoku as an heterogeneous independent auditor XXXXXXXXX

4 Expected Outcome and Impact of Research

XXXX Must mention impact on University's Research in support of DOD
XXXX Must mention Impact on University's Teaching

5 Conclusions

A Cost break down by year

The estimated costs for this research are shown in Table **??**.