A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

LA-UR -89-635 CONF-891064--1

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

LA-UR--89-635

DE89 008013

TITLE LOS ALAMOS CCS FORMAL COMPUTER SECURITY MODEL

AUTHOR(S) J. S. Dreicer and W. J. Hunteman

SUBMITTED TO 12th National Computer Security Conference, Baltimore, MD, October 10-13, 1989

Los Alamos

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

LOS ALAMOS CCS FORMAL COMPUTER SECURITY MODEL

Jared S. Dreicer & William J. Hunteman
Center for Computer Security
Los Alamos National Laboratory

ABSTRACT

This paper provides a brief presentation of the formal computer security model currently being developed at the Los Alamos Department of Energy (DOE) Center for Computer Security (CCS). The initial motivation for this effort was the need to provide a method by which DOE computer security policy implementation could be tested and verified. The actual analytical model was a result of the integration of current research in computer security and previous modeling and research experiences. The model is being developed to define a generic view of the computer and network security domains, to provide a theoretical basis for the design of a security model, and to address the limitations of present models. Formal mathematical models for computer security have been designed and developed in conjunction with attempts to build secure computer systems since the early 70's. The foundation of the Los Alamos DOE CCS model is a series of functionally dependent probability equations, relations, and expressions. The mathematical basis appears to be justified and is undergoing continued discrimination and evolution. We expect to apply the model to the discipline of the Bell-Lapadula abstract sets of objects and subjects.

INTRODUCTION

There are a number of goals for this paper: (1) to introduce the Los Alamos CCS (LACCS) model, (2) to present a brief introduction and discussion of computer security, and (3) to discuss the future direction and application of this work.

Other formal models have been developed; two of the most prominent are the Bell & LaPadula and the SRI models. Although both of these models have undergone scrutiny and analysis for years, it is generally agreed that they are not useful in developing a secure system.[1,2] However, both the Bell & LaPadula and the SRI models have provided insight into the development of multi-level secure systems. The LACCS model attempts to alleviate the limitations of these other models.

Application of the formal models to securing a computer system requires consideration of all aspects of computer security. These aspects include the traditional hardware and software, as well as, the operating environment of the computer system.

COMPUTER SECURITY

The fundamental objective of securing a computer system is to prevent or deter unauthorized or unaccountable access to the system and the information being processed or stored. This objective requires a holistic approach to security that goes beyond the traditional hardware and software views of computer security. The vulnerabilities in the computer system hardware and software have received the most attention in previous research work. This work has focused on evaluating the likelihood that a given threat would be successful in exploiting hardware or software vulnerabilities.

However, the operating environment for the system provides a larger, and possibly easier to exploit, range of vulnerabilities. The threat agent's goal is to achieve unauthorized disclosure, modification, or destruction of information or hardware regardless of where the vulnerability exists. The LACCS model provides an integrated view of the system. The model supports a global view of the system while addressing the threat agent's perspective.

The total environment of a secure computing system often receives relatively little attention when considering threats against the information. Vulnerabilities in the operating environment (procedural issues) can contribute to vulnerabilities in some of the system security mechanisms. Extreme situations have been observed where a breakdown in the procedures has negated many of the information protection mechanisms.

Another avenue of system attack for the threat agent is the denial of authorized use of the computing system. The denial of use can be achieved through a variety of techniques. The introduction of faulty circuit boards or microcode can deny use and possibly cause physical damage to a system. Software actions, including the introduction of a virus, can cause a system to be unresponsive to its users or frustrate the users with the resultant effect that the system is not used in an effective manner.

Use of the system can also be denied through a variety of techniques that do not require access to the system hardware or software. The introduction of commonly available chemicals into the heating or ventilation system for the computer facility can result in the shutdown and evacuation of the entire facility. Frequent false alarms, e.g., bomb threats and fire alarms, can also have the effect of denying use of the system.

Threats resulting in the disclosure, modification, or destruction of information can be achieved through a wide variety of operations specific to the information sensitivity and the computing system being attacked. However, the standard manner in which most of these actions are accomplished is primarily due to problems or difficulties in information management and the authorization, enforcement, and verification methodologies employed in the system. Some specific DOE areas affected by the methodologies are

- user authentication and authorization, e.g., personnel clearances, physical access controls, and software mechanisms for authentication and authorization;
- information management, e.g., configuration management of hardware and software, discretionary and mandatory access controls, backup of sensitive information, accountability, marking of objects, and assurance testing;
- communications, e.g., use of TEMPEST equipment and construction of communications facilities; and
- operating procedures, e.g., clearing and sanitization of storage objects and reliable marking of human readable output.

Previous work in computer security models, e.g., Bell & LaPadula,[3] and other research have concentrated on authorization and classification levels of information and information management. These models have not incorporated the issues involved in defining the necessary secure environment for the system. The LACCS model provides a comprehensive framework for considering all computer security issues.

LACCS MODEL

In an analytical manner the LACCS model incorporates the computer security concerns and issues briefly discussed in the introduction and the previous section. Further, the LACCS model goes beyond simply characterizing the DOE computer security policy; it addresses generic problems of computer security.

In order to support the capability to consider "what-if" questions in the computer security and network domain, a generic model is required. This requirement is necessary due to the speed and frequency of technological change in computer science research and the computer industry (hardware and software).[4] New computer system configurations and topologies, communication and design protocols, threats, vulnerabilities, and operating methodologies are continuously developed and utilized. The ability to employ these technological developments or counter them depends on the capability to determine their operational effectiveness.

The desire to apply the LACCS model to subjects and objects in terms of the Bell-LaPadula model definition essentially requires mapping these abstract sets to the equivalent abstraction in the LACCS model. However, the perspective of the Bell-LaPadula model is fundamentally different, in that it results in an indication of whether or not the system state is secure. The comprehensive system state is determined by the combination of all the transition states. If each transition state is secure then the resulting system state is secure, this is known as the Basic Security Theorem.[5] Security is defined in terms of the relationship between the clearances of subjects and classifications of system objects. As long as the rules and dominance relation with respect to access control and management is observed, then security is maintained.

For the LACCS model, there are two perspectives associated with security: the attacker's (insider, agent, and hacker) and the defender's (computer system security officer). In terms of subjects and objects, the attacker and defender, as well as the functioning computer system, are all subjects (active entities) and the information resident on the computer system is an object (passive entity).

The following probability equations and relations abstractly describe the essential subsystem and interface components from the standpoint of the two security perspectives and from a physical computer and network systems outlook. Equation (1) results in a measure of the security expectancy for the modeled system, the defender's ultimate consideration.

$$S_e = 1.0 - D_e \tag{1}$$

Equation (1) is defined in terms of subjects and objects, since D_e is composed of both active and passive entities. The security expectancy measure is the comprehensive result of the model. The security expectancy (S_e) and the damage expectancy (D_e) for a system are inversely related.

Designers of a system are concerned with the security expectancy for an actual or proposed system. Both system security developers and attackers are interested in the damage expectancy for the system but for distinctly different reasons. Damage expectancy is determined by threat arrival, which is a concern for security developers and attackers, and threat damage, which is a concern for system designers. Damage expectancy is principally related to subjects, but the subjects have objects as components, indicated in the following discussion. Equation (2) demonstrates the relation.

$$D_e = F(T_{ad}, T_d, T_{aa}) \tag{2}$$

Threat arrival for defender (T_{ad}) is related to the penetrability, resistivity, and discrimination reliability of the system to the entrance of a threat element. Equation (3) depicts the factors that affect the threat arrival.

$$T_{ad} = F(T_{sps}, S_{pts}, S_r) \tag{3}$$

T_{sps} is the survivability of the penetrating threat, an active subject, before entering the system. S_{pts}, a subject, is the pre-threat survivability of the system. S_r is the system reliability, a subject. These factors are dependent upon the threat access mechanism, system implementation, and the system integrity.

Threat damage (T_d) is dependent on the system's vulnerabilities, information sensitivity, mission criticality, and resilience to disclosure and deterioration. These components are represented in Equation (4).

$$T_d = F(V_n, I_c, M_c, S_{rdi}, S_{rdt}) \quad (4)$$

V_n is the vulnerability or hardness of the system; this is an object. I_c is the highest classification of information resident on the system; this is an object. M is a measure of the national importance of the system; this is an object. S_{rdi} and S_{rdt} are indicators of the capacity of the system to limit information exposure and recover from deterioration. These factors result from the integration of subjects and objects.

Threat arrival for attacker (T_{aa}) is determined by the penetration initiation, success, and potential. Equation (5) presents the relation.

$$T_{aa} = F(T_{atp}, T_{p/a}, T_{h/a}) \quad (5)$$

T_{atp} is a threat attempt, a subject. $T_{p/a}$ is a threat penetration given an attempt, a subject. $T_{h/a}$, a subject, is the harm that results from a successful penetration attempt. These components are dependent on the threat prevention and access mechanisms and the type and implementation methodology. The interpretation of T_{aa} can range from representing a system that has been destroyed ($T_{aa} = 1.0$) to one that has been harmed ($0.0 < T_{aa} < 1.0$).

CONCLUSION

The LACCS model was recently formulated and is in the process of examination and refinement. The model has undergone several modifications to better conform to the computer and network domain. It is the intention of the authors to demonstrate the model as a top-level definition of a secure system. Further work will identify the similarities and differences between the Bell-LaPadula objects and subjects and the LACCS model terminology. Additional work is planned to apply the LACCS model to the development and review of secure systems and networks.

REFERENCES

1. C. Landwehr, "Formal Models for Computer Security," ACM Computing Surveys, Vol. 13, No. 3, 247-278 (September 1981).

2. T. Taylor, "Comparison Paper Between The Bell and LaPadula Model and The SRI Model," Proceedings of the 1984 Symposium on Security and Privacy, 1984, pp. 195-202.

3. D. E. Bell and L.J. LaPadula, "Secure Computer System: Mathematical Foundations and Model," M74-244, Mitre Corp (1973).

4. C. Landwehr, "The Best Available Technologies for Computer Security," IEEE Computer, 86-100 (July 1983).

5. DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria (December 1985).