Applied Cryptology, Cryptographic Protocols, and Computer Security Models

Volume 29

PROCEEDINGS OF SYMPOSIA IN APPLIED MATHEMATICS

AMERICAN MATHEMATICAL SOCIETY

1. Introduction

We use the term computer system to describe collections of computational resources. These resources may communicate with each other or may comprise independent computers that interact only with human programmers and operators. With increasing frequency, computer systems are relied upon in applications where the successful completion of tasks and activities is especially critical. In many cases, a computer system is required to function without error or within certain efficiency bounds. The extent to which the systems fulfills such requirements is used to define the reliability or performance of the system. In highly reliable or efficient systems, system behavior is measured against its response to external input which lies within a certain range that has been specified as acceptable. Input lying outside the specified range may cause the system to fail or to become inefficient, but, since the system meets its requirements on the input for which it was designed, its reliability or level of performance are not affected by such input.

There are applications, however, for which such notions as reliability are unsuitable. In these applications, the range of specified input is determined by an adversary or enemy whose goals is to subvert the successful functioning of the system. Thus,

although input from the enemy may be outside the normal operating range, the system must continue to provide essential services, *in spite of* the input. For example, military or diplomatic communication systems must continue to deliver messages in a highly regular and predictable way, even though enemies may attempt to intercept secret communications, corrupt messages, or insert false messages into the system. Another example of a system whose successful operation requires withstanding subversion is an electronic funds transfer system. Such a system must protect financial transactions against intentional or unintentional disruption and diversion. By the same token, large scale databases of electronically stored information may contain data that is sensitive. Such data may be composed of financial records, personal data, or proprietary information. Such databases must deliver access and services without compromising the sensitive data.

The *security* of a computer system is defined by its ability to meet specific operating requirements, despite the actions of a knowledgeable and determined enemy. Security requirements may include maintaining the secrecy or integrity of information, providing highly reliable or available services, or preventing unauthorized use of system resources.

In this survey of, we will concentrate on three important aspects of system security: cryptography, software approaches, and cryptographic protocols.

Cryptography is the art of concealing the content of messages from an enemy who may be monitoring system activity. The rapid

spread of communication-based technology and the recent appearance of cryptographic techniques that provide highly secure message concealment, have led to a renewed interest in the field of cryptography. However, many of the security problems which arise from the use of modern computing technology cannot be directly solved by cryptographic techniques.

An alternative approach to solving security problems is to program the computer to monitor or protect against the most probable threats. Two important areas are the protection mechanisms which guard against unauthorized access or dangerous program execution and the protection of information stored in statistical databases. There are situations, however, in which software-oriented approaches to security must be augmented by still more secure system components. It is possible that by executing a cryptographic protocol, that is, an exchange of secret messages, more complex security mechanisms can be implemented.

The format of this survey is as follows. Chapter 2 will discuss data security, paying particular attention to modern techniques of encryption and cryptanalysis. In Chapter 3, we present the technical basis of access control modelling and multilevel system requirements and highlight the most useful models for multilevel security. The emphasis in Chapter 4 is on an alternative view of how security requirements can be met: through the use of protocols built on highly secure cryptographic techniques.

It will be clear as we proceed that this is not an unbiased survey, and the reader should beware that for every opinion offered herein, there is ample contrary argument available in

other technical circles. In the United States, for example, support has been consistent and sizable for other approaches to the multilevel problem. These approaches have, however, not met with great practical success. We hope that these views are accepted as alternatives to competing positions. We certainly do not offer them as replacements. Quite the contrary: we have not seen the alternative views discussed with any depth.

It is an interesting footnote to the technical developments discussed in the sequel that the noticeable increase in academic research activity in the area of computer security has lead to confrontations with agencies of the U.S. Government. On one hand, agencies such as the National Security Agency (NSA) have issued claims that their missions may be imperiled by the publication of certain results in cryptography. Some researchers have countered, on the other hand, that any restriction on the flow of research results constitutes an uneccessary and serious infringement of academic and intellectual freedom. They argue further that the stuff of basic research in cryptography is pure mathematics and computer science; it is not clear how to distinguish a pure number theoretic or complexity theoretic result from one which poses a genuine threat to national security. The alternative of restricting all basic research which which impinges on sensitive applications is probably not workable.

In 1980, the American Council on Education (ACE) formed a panel to study the issues raised by the differing viewpoints noted above. The ACE group ultimately recommended a system of voluntary reviews by NSA. The ACE recommendations contain the assumption that without compulsory pressures, most authors and professional

societies will cooperate with such a system of voluntary review. One of us (Davida) was a member of the ACE study group, and did not concur with their recommendations. In a minority statement, it was argued that any system of restraint -- even one which is voluntary -- will only hinder the development of cryptography in public and private sectors, to the ultimate detriment of the public and NSA itself. Two of us (DeMillo and Lipton) served on a panel of representatives from the professional societies to outline a response to proposed regulation of cryptographic research. As yet, there is no definitive resolution to the underlying problems.*

---

*The complete text of the ACE study group report has been published under the tile 'Report of the Public Cryptography Study Group' in the Communications of the ACM, 24(7): 434-449.