Building Secure and Dependable Information Systems

Wenbing Zhao
Cleveland State University, USA

INTRODUCTION

Information systems are essential building blocks in any business or institution. They can be used to automate most business processes and operations. In the Internet age, virtually all such systems are accessible online, and many of them are interconnected. This mandates that such systems be made highly secure and dependable.

A secure and dependable system has many desirable attributes, including confidentiality, integrity, availability, reliability, safety, and maintainability (Avizienis, Laprie, Randell, & Landwehr, 2004). Confidentiality means that only legitimate users can access its services and that the communication, both within the system and between the system and its users, is kept confidential. Integrity means that the services provided by the system are what the users expect and no one can corrupt the information without being detected. Availability means that the services provided by the system are available whenever legitimate users want to use them. Reliability is a metric of the continuity of a service. The safety means the system will not have catastrophic effect on its users and environment. The maintainability indicates the ability to use, upgrade, and repair the system.

Historically, the confidentiality and integrity-related issues have been the focus in the secure computing field, while the availability and reliability issues are central concerns in dependable (or fault-tolerant) computing (Avizienis et al., 2004). We have seen a trend for the two communities to work together to advance the state of the art in building information systems that are both highly secure and highly dependable. In the last decade, many exploratory secure and dependable systems have been designed and implemented. The demand for secure and dependable systems has also prompted many companies to take initiatives to increase the trustworthiness of their products (Charney, 2006).

BACKGROUND

Security refers to the state of being protected against the loss of valuable asset (Pfleeger & Pfleeger, 2002). A secure information system is one that guarantees confidentiality, integrity, and availability of information. The information can be transmitted over the network, processed in a computer system, and persisted in stable storage. The threats to an information system can be categorized into the following four types:

1. **Interception:** An adversary gains unauthorized access to the information, for example, by breaking into a system or by eavesdropping messages sent over the network.
2. **Interruption:** An adversary prevents authorized users from accessing the information. This can be done by destroying information or by disrupting the availability of the system that provides the information. Examples of the latter include crashing the system, or overloading the system and the networks. Attacks of this sort are often referred to as *denial-of-service* attacks.
3. **Modification:** An adversary not only gains access to the information, but modifies it as well.
4. **Fabrication:** An adversary introduces fake information into the system. This can take the form of inserting counterfeit records into the databases or sending fabricated messages to a system.

There are many countermeasures to defend against the above threats. The most fundamental method is *encryption.* Encryption is the process of scrambling a *plaintext* into unrecognizable *ciphertext,* often parameterized with a *key.* The same or a different key is needed to *decrypt* (i.e., unscramble) the ciphertext back into the original plaintext. The messages sent over the network should be encrypted so that an eavesdropper cannot interpret the content of the ciphertext. The information stored on disk can be encrypted as well.

Other countermeasures include better software design and implementation (including good *access control*), and better security-related policies and procedures to minimize the vulnerabilities in software systems and their operations.

In dependable computing, the vulnerability and threats to a system are often modeled as a variety of *faults*. A fault can leads to an *error* in the system, and eventually can cause a system *failure*. Consequently, the means to achieve dependability include fault avoidance, fault tolerance, fault removal, and fault forecast. Fault avoidance is achieved through good design in software and hardware. Virtually all security measures can be regarded as a form of fault avoidance. Fault tolerance is essential to achieve high availability and reliability. Fault tolerance involves hardware and software redundancy so that if one component fails, other replicated components can continue providing services. Fault removal consists of removing software bugs and faulty hardware components during the testing phase, and isolating, removing, or repairing faulty components during run time. Fault forecasting involves the evaluation of the system operations with respect to the possibility of failure occurrences.

SECURE AND DEPENDABLE SYSTEM DESIGN

To build secure and dependable systems, the traditional software engineering practice must be enhanced to explicitly address the security and dependability issues from the beginning of the project lifecycle. The first step is to model all the potential threats to the system. Once a threat model is developed, appropriate security and dependability techniques must be used to mitigate the threats. A set of test cases must also be developed according to the threat model and used to verify the implemented system.

In this section, we first enumerate some common threats to information systems. We subsequently discuss how to counter such threats, using state-of-the-art security and dependability techniques. Finally, we discuss the challenges in building secure and dependable systems.

Threat Model

An information system can be modeled as a system that stores, processes, and exchanges information with other systems. Normally, the system can be accessed only through a few well-defined entry points. It also has a few exit points where information can flow out of the system. Below are some common threats to an information system:

- Illegal access or modification of information: This can happen in a number of different ways:
  - An adversary eavesdrops the messages transmitted over the network to gain access to the information.
  - An adversary may gain access through undocumented backdoor entry points, or through *buffer-overflow attacks*.
  - An adversary accesses or modifies information via compromised communication channels with a system.
- Unauthorized access to confidential information by authenticated users: This can happen if an adversary successfully launches a privilege elevation attack, for example, a regular user gains root or administrator privilege.
- Confidential information leak through exit points, either explicitly or through covert channels.
- Corruption or deletion of information, application code, or even the operation system services and logs.
- Repudiation: A user might deny that he/she has requested some information from the system or has supplied some information to the system.
- Reduced service availability caused by denial-of-service (DoS) attacks: An adversary might overload or crash the system, by sending ill-formed requests to the system.
- Hardware failures, power outages, or other environmental disasters.
- Incorrect software execution may render the service unavailable, delete or corrupt information, or leak confidential information: This may be caused by bad design, implementation bugs, or intrusions from adversaries.
- Threats may also come from internal, e.g., from disgruntled employees, or corrupted system administrators: They may be able to bypass normal interface and security check to steal confidential