Chapter 21
Intrusion Tolerance Techniques

Wenbing Zhao
Cleveland State University, USA

ABSTRACT

The authors believe that the research and development of intrusion tolerant systems will gain more momentum as more and more services are offered online. The expectation of such services is high, considering their essential roles in everyday operations of businesses and individuals as well. The impact of service unavailability and security breaches will only grow more serious. In this chapter, the authors survey the state-of-the-art techniques for building intrusion-tolerant systems. They also illustrate a few of the most urgent open issues for future research. Finally, they point out that to build secure and dependable systems we need a concerted effort in intrusion prevention, intrusion detection, and intrusion tolerance.

INTRODUCTION

Intrusion tolerance refers to the capability of maintaining the system availability and integrity despite malicious attacks. Intrusion tolerance has been a hot research area for more than a decade and various techniques have been introduced to achieve various degrees of intrusion tolerance (Castro & Liskov, 2002; Chai & Zhao, 2014 June; Chai & Zhao, 2014 August; Deswarte et al., 1991; Verissimo et al., 2003, Yin et al., 2003; Zhao, 2013; Zhao, 2014). Such techniques can tolerate intrusion attacks in two respects: (1) a system continues providing correct services (may be with reduced performance) and (2) no confidential information is revealed to an adversary. The former can be achieved by using the replication techniques, as long as the adversary can only compromise a small number of replicas. The later is often built on top of secrete sharing and threshold cryptography techniques. Plain replication is often perceived to reduce the confidentiality of a system, because there are more identical copies available for penetration. However, if replication is integrated properly with secrete sharing and threshold cryptography, both availability and confidentiality can be enhanced.

DOI: 10.4018/978-1-5225-7492-7.ch021

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

BACKGROUND

In this section, we introduce some basic security and dependability concepts and techniques related to intrusion tolerance. A secure information system is one that exhibits the following properties (Pfleeger & Pfleeger, 2002):

- **Confidentiality:** Only authorized users have access to the information.
- **Integrity:** The information can be modified only by authenticated users in authorized ways. Any unauthorized modification can be detected.
- **Availability:** The information is available whenever a legitimate user wants to access it.

Confidentiality is often achieved by using encryption, authentication, and access control. Encryption is a reversible process that scrambles a piece of plaintext into something uninterpretable. Encryption is often parameterized with a security key. To decrypt, the same or a different security key is needed. Authentication is the procedure to verify the identity of a user that wants to access confidential data. Access control is used to restrict what an authenticated user can access.

Integrity can be protected by using secure hash functions, message authentication code (MAC) and digital signatures. For data stored locally, including the application binary files, a checksum is often used as a way to verify data integrity. The checksum can be generated by applying an oneway secure hash transformation on the data. Before the data is accessed, one can verify its integrity by recomputing the checksum and comparing it with the original one. The integrity of a message transmitted over the network can be guarded by a MAC. A MAC is generated by hashing on both the original message and a shared secret key (and often with a sequence number as well). If it is tampered with, the message can be detected in a way similar to that for checksum. For stronger protection, a message can be signed by the sender. A digital signature is produced by first hashing the message using a secure hash function, and then encrypting the hash using the sender's private key.

High availability is achieved by using replication, checkpointing and recovery techniques. Replication is a technique that relying on running redundant copies of an application so that if one copy fails, the services can be provided by the remaining copies. Checkpointing means to take a snapshot of the state of a replica. The saved state can be used to bring a new or a restarted replica up to date. Checkpointing is also useful to avoid log buildup (when a checkpoint is taken, all previously logs can be garbage collected). Recovery techniques concern the tasks of removing faulty replicas, repairing them, and reintegrating them back to the system.

INTRUSION TOLERANCE TECHNIQUES

Intrusion tolerance is built on top of two fundamental techniques: replication and secret sharing/threshold cryptography (Deswarte et al., 1991). In the context of intrusion tolerance, a very general fault model must be used because a compromised replica might exhibit arbitrary faulty behaviors. Such a fault model is often termed as Byzantine fault (Lamport et al., 1982).

9 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/intrusion-tolerance-techniques/213656

Related Content

Network Intrusion Detection and Prevention Systems on Flooding and Worm Attacks
P. Vetrivelan, M. Jagannathand T. S. Pradeep Kumar (2016). *Combating Security Breaches and Criminal Activity in the Digital Sphere (pp. 183-207).*
www.irma-international.org/chapter/network-intrusion-detection-and-prevention-systems-on-flooding-and-worm-attacks/156460

CEO Bonus Pay and Firm Credit Risk
Hsin-Hui Chiuand Eva Wagner (2020). *International Journal of Risk and Contingency Management (pp. 1-19).*
www.irma-international.org/article/ceo-bonus-pay-and-firm-credit-risk/247140

Risk Planning and Mitigation in Oil Well Fields: Preventing Disasters
Nediljka Gaurina-Meimurec, Borivoje Pašiand Petar Miji (2015). *International Journal of Risk and Contingency Management (pp. 27-48).*
www.irma-international.org/article/risk-planning-and-mitigation-in-oil-well-fields/145364

Offline/Online Security in Mobile Ad Hoc Networks
Wen-Jung Hsinand Lein Harn (2013). *Theory and Practice of Cryptography Solutions for Secure Information Systems (pp. 199-222).*
www.irma-international.org/chapter/offline-online-security-mobile-hoc/76517

Distributed Monitoring: A Framework for Securing Data Acquisition
Matthew Brundage, Anastasia Mavridou, James Johnson, Peter J. Hawrylakand Mauricio Papa (2013). *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection (pp. 144-167).*
www.irma-international.org/chapter/distributed-monitoring-framework-securing-data/73123