ELSEVIER

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Computer Communications 28 (2005) 1317–1336

computer communications

www.elsevier.com/locate/comcom

A modeling and simulation methodology for analyzing ATM network vulnerabilities

Aparna Adhav[a], Tony S. Lee[b], Sumit Ghosh[c,*]

[a]*Cisco Systems, 225 East Tasman Drive, San Jose, CA 95134, USA*
[b]*Yahoo! Inc., 701 First Avenue, Sunnyvale, CA 94089, USA*
[c]*SENDLAB, Department of ECE, Stevens Institute of Technology, Hoboken, NJ 07030, USA*

Received 25 August 2004; revised 29 January 2005; accepted 31 January 2005
Available online 3 March 2005

Abstract

The design of complex asynchronous distributed systems including ATM networks is in itself quite challenging and designers rarely expend either the time or energy to consider how unexpected changes in the operating environment may affect the reliability of the system, let alone take into consideration imaginative ways in which a clever perpetrator may maliciously cause the system to fail, often catastrophically. While the occurrence and impact of attacks launched against telephone networks, store-and-forward networks such as the Internet, and the power grid, are widely reported in the news media, a systematic analysis of these attacks in the scientific literature is lacking. This paper is the first to propose the use of modeling and asynchronous distributed simulation as a systematic methodology to uncover vulnerabilities in complex ATM networks. The approach is demonstrated in two steps. In step 1, a few complex attacks are identified, which while based on the principles of ATM networking, are representative of those that would be construed by intelligent enemy agents. An attack is viewed as a perturbation of an operationally correct ATM network and may be classified under two broad categories. The first attack type focuses on failing specific, standard functions in ATM networks while the second category of attacks refers to the prescription of a malicious intent or objective. Under step 2, the attacks are modeled utilizing a representative ATM network and analyzed through a simulation utilizing an asynchronous, distributed, and accurate ATM simulator, that executes on a network of Pentium workstations under Linux, configured as a loosely-coupled parallel processor. Thus, the environment underlying the evaluation of the vulnerabilities reflect reality, implying, in turn, realistic results. In addition to revealing the weaknesses, the findings of this methodology may serve as a guide to either redesigning the ATM network and eliminating the vulnerabilities or synthesizing a sentinel that conceptually surrounds and protects from network from attacks. While the methodology is generalizable to ATM-like MPLS network and future network designs, it is beyond the scope of this paper.

Keywords: ATM network; Vulnerabilities; Security breaches; Threat scenarios; Catastrophic failures

1. Introduction

While fault simulation and test generation tools [1] have been in practice for over two decades in the field of computer-aided design of VLSI and digital systems to identify design and manufacturing errors in hardware systems, they were primarily confined to synchronous system designs subject to a centralized clock. In contrast, the approach proposed in this paper applies to complex asynchronous distributed systems where individual entities are driven by their own independent clocks and interact asynchronously with one another.

As complex systems, networks consist of a number of constituent elements that are geographically dispersed, are semi-autonomous in nature, and interact with one another and with users, asynchronously. Given that the network design task is already intrinsically complex, it is natural for the traditional network designer to focus, in order to save time and effort, only on those principles and interactions, say D, that help accomplish the key design objectives of the network. The remainder of the interactions, say U, are viewed as “don’t cares” or passive, bearing no adverse impact under normal operating conditions. In reality, however, both internal and external stress may introduce

* Corresponding author. Tel.: +1 201 216 5658; fax: +1 201 216 8246.
E-mail addresses: tlee@yahoo-inc.com (T.S. Lee), sghosh2@stevens.edu (S. Ghosh).

0140-3664/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2005.01.018

abnormal operating conditions into the network under which the set U may begin to induce any number of unintended effects, even catastrophic failure. A secure network design must not only protect its internal components from obvious attacks from the external world, but, and this is equally important, resist internal attacks from two sources, foreign elements that successfully penetrate into the network and attack from within and one or more of the internal components that spin out of control and become potentially destructive. This section introduces the notion of network vulnerability analysis, conceptually organized into three phases. Phase I focuses on systematically examining every possible interaction from the perspective of its impact on the key design objectives of the network, and constitutes an indispensable element of secure network design. Given that the number of interactions in a typical real-world network is large, to render the effort tractable, phase I must be driven from a comprehensive and total understanding of the fundamental principles that define the network. Phase I is likely to yield a nonempty set of potential scenarios under which the network may become vulnerable. In phase II, each of these weaknesses is selected, one at a time, and where, possible, a corresponding attack model is synthesized. The purpose of the attack model is to manifest the vulnerability through an induced excitement and guide its effect at an observable output. The attack model assumes the form of a distinct executable code description, encapsulating the abnormal behavior of the network, and assumes an underlying executable code description that emulates the normal network behavior. In phase III, the attack models are simulated, one at a time, on an appropriate testbed, with two objectives. First, the simulation verifies the thinking underlying the attack model, i.e. whether the attack model succeeds in triggering the vulnerability and forcing its manifestation to be detected at an observable output. When the first objective is met, the simulation often reveals the impact of the attack model on network performance. Under the second objective, the extent of the impact is captured through an innovative metric design.

The remainder of the paper is organized as follows. Section 2 is a brief review of the current literature on attack models. Section 3 presents the fundamental ATM network principles that form the basis for launching the vulnerability analysis. Section 4 focuses on vulnerability analysis and synthesis of the attack models intended to expose the vulnerabilities. Section 5 presents details on the assessment of the attacks through modeling and asynchronous distributed simulation on ATMSIM 1.0 [2] and the lessons learned for hardening ATM networks in the future.

2. Brief review of the current literature on attack models

A careful examination of the literature on attack models for networking reveals that nearly all efforts focus on store-and-forward networks [3]. The literature also reveals the lack of a systematic analysis of the vulnerability of data networks from basic principles. As a result, both a set of basic attacks derived from the vulnerability analysis and an approach to validate such attacks are missing in the literature. Virtually all of the reported efforts, except for [4], are ad hoc, lack systematic modeling and analysis, and do not support efforts to use them to harden networks. Since, the Internet, the most well-known store-and-forward network has been around the longest, the literature contains a rich set of documented methods to launch attacks on the Internet as well as a collection of clever techniques to defeat them. These include:

- Denial of service attack via PING: a denial of service attack via PING occurs when oversized IP packets are transmitted inadvertently or intentionally via PING. Given that the maximum packet size in TCP/IP is set at 65,536 bytes, when confronted with oversized IP packets, networks may react in unpredictable ways including crashing, freezing, or rebooting of the system.
- Password breaking: though crucial to system security, system files such as/etc/passwd are normally readable by all users, tempting perpetrators to attempt to break the encrypted information stored in these files.
- TCP Wrapper: the proposed enhancement permits the system administrator to selectively reject requests for services such as ftp, rsh, and rlogin from suspicious sources.
- Data encryption: as a logical step, sensitive data may be encrypted to defeat unauthorized tapping and access by intruders.
- Firewalls: the philosophy underlying firewalls is to shield the network from the external world and concentrate attacks at a single point that can be effectively monitored by the network management.
- Trojan horse: the concept of Trojan horse attacks refers to the technique of secretly implanting hostile entities in a network. Thus, in theory, unless a system is designed and implemented completely by one trusted individual, the system does not and should not lend itself to 100% trust. Thompson [4] warns of the danger of compiling malicious code, deliberately or accidentally, into the operating system, labeling them Trojan horses. A careful analysis reveals that all networks are fundamentally vulnerable to the metastability problem [2,5] that affects every sequential digital design when a flip–flop encounters an asynchronous input signal from the external world.
- Classification of attacks on networks: potential security violations may be organized under three categories: (1) unauthorized release of information, (2) unauthorized modification of information, and (3) unauthorized denial of resources. All of these attacks may be further classified into two types, active and passive. While active attacks are capable of modifying information or causing denial of resources and services, under passive