Proceedings 17th Annual Computer Security Applications Conference: 10-14 December 2001, New Orleans,

The Evolution of System-call Monitoring

Stephanie Forrest
Dept. of Computer Science
University of New Mexico
Albuquerque, NM USA
forrest@cs.unm.edu

Steven Hofmeyr
Lawrence Berkeley Laboratory
Berkeley, CA USA
shofmeyr@lbl.gov

Anil Somayaji
School of Computer Science
Carleton University
Ottawa, ON Canada
soma@scs.carleton.ca

Abstract

Computer security systems protect computers and networks from unauthorized use by external agents and insiders. The similarities between computer security and the problem of protecting a body against damage from externally and internally generated threats are compelling and were recognized as early as 1972 when the term computer virus was coined. The connection to immunology was made explicit in the mid 1990s, leading to a variety of prototypes, commercial products, attacks, and analyses. The paper reviews one thread of this active research area, focusing on system-call monitoring and its application to anomaly intrusion detection and response.

The paper discusses the biological principles illustrated by the method, followed by a brief review of how system call monitoring was used in anomaly intrusion detection and the results that were obtained. Proposed attacks against the method are discussed, along with several important branches of research that have arisen since the original papers were published. These include other data modeling methods, extensions to the original system call method, and rate limiting responses. Finally, the significance of this body of work and areas of possible future investigation are outlined in the conclusion.

1 Introduction

During the 1990's the Internet as we know it today grew from a small network of trusted insiders to a worldwide conglomerate of private citizens, governmental agencies, commercial enterprises, and academic institutions. As society at large embraced the Internet, opportunities and incentives for malicious activities exploded, creating demand for new computer security methods that could succeed in this open and uncontrolled environment. Open applications, mobile code and other developments helped erode the notion of a clear perimeter, which formerly separated a trusted system from its external environment. Previous approaches to computer security had emphasized top-down policy specification, provably correct implementations of policy, and deployment in correctly configured systems. Each of these assumptions became increasingly untenable, as the Internet grew and was integrated into human society.

The similarities between computer security in the age of the Internet and the problem of protecting a body against damage from internally and externally generated threats are compelling. They were recognized as early as 1972 when the term computer virus was introduced [67]. Later, Spafford argued that computer viruses are a form of artificial life [66], and several authors investigated the analogy between epidemiology and the spread of computer viruses across networks [38, 51, 59, 55]. The connection to immunology was made explicit in [15, 37], and since that time the ideas have been extended to incorporate significant amounts of immunology and to tackle ambitious computer security problems, including computer virus detection [15, 37], network security [24, 79, 33], spam filtering [57], and computer forensics [46].

As the primary defense system of the body, immune systems are a natural place to look for ideas about architectures and mechanisms for coping with dynamic threat environments. Immune systems detect foreign pathogens and misbehaving internal components (cells), and they choose and manage an effective response autonomously. Thus, the immune system can be thought of as a highly sophisticated intrusion detection and response system (IDS).

Despite debate in the immunological literature about how the immune system recognizes threats, in most of the work on computer immune systems it is assumed that natural immune systems work by distinguishing between protein fragments (peptides) that belong to the properly functioning body (*self*) and ones that come from invading and malfunctioning cells (*nonself*). To explore IDS designs that mimic those of the immune system, we must first decide what data or activity patterns will be used to distinguish between computational self and nonself. That is, we must de-

17th Annual Computer Security Applications Conference: Proceedings: December , New Orleans, Louisiana [Computer Security Applications.iii. Proceedings. 17th Annual. Computer Security. Applications Conference. 10 14 December New Orleans, Louisiana. Sponsored by. Applied Computer .Results 1 - 25 of 49 Dec. . to its initial state. New Orleans, LA, USA (1) Proceedings 17th Annual Computer Security Applications Conference.Results 26 - 49 of 49 Dec. . New Orleans, LA, USA (1) Annual Computer Security Applications Conference Publication Year: , Page(s) - .. Proceedings 17th Annual Computer Security Applications.Proceedings 17th Annual Computer Security. Applications Conference: December ,. New Orleans, Louisiana by Computer Security Applications.for malicious activities exploded, creating demand for new computer security methods that could succeed in this open In Proceedings of the 17th Annual. Computer Security Applications Conference, New Orleans,. Louisiana, December 1014, [31] B. M. K (ACSAC'00), New Orleans, LA, December 1115 ACSAC', 17th Annual Computer Security Applications Conference, to be held 10 14 December in New Orleans, Louisiana, USA.National Science and Technology Council, "Federal Plan for Cyber Security and Information of the IEEE Wireless Communication and Networking Conference , New Orleans, LA, , pp. .. Environment, Proceedings of the 17th Annual Computer Security Applications Conference, p, December , Mikhail J. Atallah, Purdue University, Department of Computer Sciences and Center for in Proceedings of the 17th Annual Computer Security Applications Conference, pages , New Orleans, Louisiana, USA, December , In Proceedings of the 17th Annual Computer Security Applications Conference, pages , New Orleans, Louisiana,. Dec. 1014, , published by the.Proceedings of the 32nd Annual Conference on Computer Security Applications, . 23rd Annual Computer Security Applications Conference (ACSAC), December , , Miami . 17th Annual Computer Security Applications Conference (ACSAC), December , New Orleans, Louisiana, USA.In Proceedings of the 13th National Computer Security Conference, pages , on System administration, December , , New Orleans, Louisiana of the 4th annual Linux Showcase & Conference, p, October , , Atlanta, Georgia Linux Security Module. http:// sgheisingen.com, April December 10 - 14, .. Proceedings of the 30th Annual Computer Security Applications Conference, December , , New Orleans, Louisiana, USA Proceedings of the 17th Annual Computer Security Applications Conference.From Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC). IEEE Computer Society, New Orleans, Louisiana. December.control networks, Annual Computer Security Applications Conference, ACM International Conference Proceeding Series, volume Part F, .. December, pages , New Orleans, Louisiana, December , .. 17th Nordic Conference on Secure IT Systems (NordSec), Lecture.s scheme still cannot achieve the claimed security goals and report its following problems: (1) It . Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC'01), Dec 1014, , New Orleans, LA, USA, IEEE.SOSP '03 Proceedings of the nineteenth ACM symposium on Operating .. of

the FREENIX Track: USENIX Annual Technical Conference, p, June .. Proceedings of the 26th Annual Computer Security Applications Conference, Applications Conference, December , , New Orleans, Louisiana, USA.NIST/NSA National Computer Security Conference (and). .. System Security, Volume 4, Number 3, August , pages . In Proceedings of the 17th IEEE Conference on .. Computer Security Applications Conference, New Orleans, Louisiana, December , , pages.articles in international journals, conference proceedings, and book chapters. . 25th Annual Computer Security Applications Conference (ACSAC), . 17th International Conference on Cryptology And Network Security (ACSAC) , New Orleans, Louisiana, USA, December , In Proceedings of the ACM SIGMOD Conference on Management of Data, pages , Dallas, In Proceeding of the 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, USA, December cryptosystem efficiency assessment by computer security specialists. . economic perspective // Proceedings of the 17th Annual Computer Security Applications. Conference (ACSAC '01), Dec , New Orleans, Louisiana , USA, In: Proceedings of IEEE System Conference, Orlando Fl, 1821 April In: Proceedings of the 17th Annual Computer Security Applications '01), Sheraton New Orleans Louisiana, USA, 1014 December , pp.