УДК 004.457

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ФУНКЦИОНИРОВАНИИ ПРОЦЕССОВ НА ОСНОВЕ ТРАССИРОВКИ СИСТЕМНЫХ ВЫЗОВОВ В ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX

Ксенофонтов В.С. (Университет ИТМО)
Научный руководитель – доцент, кандидат технических наук, Гирик А.В.
(Университет ИТМО)

Введение. В операционных системах семейства Linux выполнение процессов осуществляется в двух режимах: в режиме ядра, обеспечивающем доступ к аппаратным ресурсам и управление памятью, и в режиме пользователя, обеспечивающем выполнение прикладных программ верхнего уровня. Переключение и обмен информацией между режимами реализуется посредством механизма системных вызовов.

Известен подход к обеспечению информационной безопасности вычислительных систем, состоящий в обнаружении аномалий в функционировании запускаемых процессов во время их работы. Одной из задач, возникающих при реализации данного подхода, является минимизация ущерба производительности процессов.

В связи с тем, что каждое действие процесса, модифицирующее объекты вычислительной системы, обеспечивается последовательностью системных вызовов, накопление и анализ совокупности этих последовательностей позволяет осуществить детектирование аномалий в поведении процесса.

На текущий момент разработчиками осуществляется поддержка утилиты Strace, предназначенной для накопления информации о системных вызовах запущенного процесса. Недостатком данной утилиты в контексте детектирования аномалий является принцип ее работы, основанный на возможностях библиотечной функции ptrace, связанной с одноименным системным вызовом. Использование данной функции приводит к частым переключениям между режимами, что существенно снижает производительность подконтрольного процесса. Утилита также не имеет собственных механизмов выявления аномалий, а производительное использование отчета о ее работе для анализа невозможно, так как для этого необходима обработка объемной текстовой информации. Актуальными для задачи инструментами являются модули ядра (loadable kernel modules), а также механизмы, предоставляемые модулем Berkeley Packet Filter.

Основная часть. Суть предлагаемого решения заключается в минимизации аналитической активности по детектированию аномалий в режиме пользователя с перемещением ее в режим ядра в целях предотвращения вычислительно дорогостоящих переключений режимов и копирования данных в пространство пользователя. Формирование реализованного подхода основано на изучении возможностей загружаемых модулей ядра, оптимизированных механизмов работы стандартных трассировщиков и функционала модуля Berkeley Packet Filter, в том числе механизма Seccomp.

Выводы. В результате проведенного исследования был разработан прототип программного средства детектирования аномалий в поведении процессов. Целевым семейством операционных систем, в которых предполагается применение средства, является семейство Linux. Полноте раскрытия потенциала разработки поспособствует ее внедрение в вычислительные средства организаций, где допустимые действия в рамках учетных записей четко регламентируются в соответствии с полномочиями пользователей.

Список использованных источников:

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. — СПб.: Питер,

2015. — 1120 с.: ил.

2. Эриксон Дж. Хакинг: искусство эксплойта. 2-е издание. – Пер. с англ. – СПб.: Символ-Плюс, 2010. – 512 с., ил.

3. Strace в Linux: история, устройство и использование: [Электронный ресурс]. 2006 - 2023. https://habr.com/ru/company/badoo/blog/493856/.

4. Пособие по программированию модулей ядра Linux: [Электронный ресурс]. 2006 – 2023. https://habr.com/ru/company/ruvds/blog/681880/.

5. BPF and XDP Reference Guide: [Электронный ресурс]. https://docs.cilium.io/en/latest/bpf/.

Ксенофонтов В.С. (автор) Подпись

Гирик А.В. (научный руководитель) Подпись