ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 3
2012

В. М. Деундяк, А. А. Таран (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»). **О модификации системы обнаружения вторжений Форрест-Сомайаджи pH на основе учета значений аргументов.**

Применение систем обнаружения вторжений (СОВ) — один из наиболее эффективных способов получения своевременной информации об атаке или вторжении в компьютерную систему. Все СОВ разделяются на два типа: сигнатурные системы и системы обнаружения аномалий (АСОВ). Последний вид позволяет выявлять новые, еще не изученные атаки, поэтому разработка таких систем представляется наиболее актуальной.

В работах группы ученых во главе с С.Форрест предложена АСОВ для UNIX-подобных систем на основе анализа коротких последовательностей системных вызовов. Применение этого подхода вместе с описанием его программной реализации pH отражены в диссертации А. Сомайаджи [1]. Однако, тот факт, что в pH не исследуются аргументы вызовов, позволил Д. Вагнеру и П. Сото разработать в [2] метод мимикрирования атак для ее обхода.

В настоящей работе строится теоретическая модель СОВ, модифицирующая подход Форрест путем использования аргументов. Работа такой СОВ делится на два этапа. На этапе обучения прежде всего сохраняются все встречающиеся последовательности системных вызовов длины n и соответствующие им значения аргументов. Как только собрано достаточно информации об аргументах последовательностей, система строит правила, ограничивающие множество их возможных значений. Эти правила включают в себя интервалы и точеные значения для каждого отдельного аргумента, которые при необходимости дополняются соотношениями между выбранными совокупностями аргументов. На этапе анализа проверяется наличие встреченных наборов по n вызовов в собранном ранее словаре, а также соответствие их аргументов набору правил, сгенерированному на первом этапе. В случае любых отклонений передается сигнал о возможном вторжении. В силу применения аргументов в построенной модели возрастает сложность мимикрирования атак.

Отметим, что в литературе имеются модели СОВ, использующие информацию об аргументах системных вызовов. Но, как правило, в них учитываются данные для всей цепочки вызовов (см., например, [3]), поэтому такие методы, по-видимому, на практике применять затруднительно. По сравнению с ними метод анализа именно коротких последовательностей в построенной модели повышает скорость реагирования на аномалии.

СПИСОК ЛИТЕРАТУРЫ

1. *Somayaji A. B.* Operating System Stability and Security through Process Homeostasis. Ph.D. thesis. University of New Mexico, 2002.

© Редакция журнала «ОПиПМ», 2012 г.

2. *Wagner D.*, *Soto P.* Mimicry Attacks on Host-Based Intrusion Detection Systems. — In Proceedings of the 9th ACM Conference on Computer and Communications Security. IEEE Computer Society Washington, DC, USA, 2002, p. 252–264.
3. *Bhatkar S.*, *Chaturvedi A.*, *Sekar R.* Dataflow Anomaly Detection. — SP '06 Proceedings of the 2006 IEEE Symposium on Security and Privacy. IEEE Computer Society Washington, DC, USA, 2006, p. 48–62.