СПИСОК ЛИТЕРАТУРЫ:

1. *Hofman M.* Survival time: международные публикации института SANS. SANS Institute. 2009. URL: http://isc.sans.edu/survivaltime.html.
2. *Russinovich M., Solomon D.* Windows Internals: Covering Windows Server 2008 and Windows Vista. 5th edition. Microsoft Press. 2009. P. 420–491.

М. Р. Мухтаров

ПРИМЕНЕНИЕ ИММУННОГО ПОДХОДА В ЗАДАЧЕ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ

В работе предложен подход применения алгоритма негативной селекции для выявления аномалий в данных о сетевом трафике, полученных средствами протокола IPFIX. Для решения данной задачи предлагается способ формализации алгоритма генерации детекторов согласно формату экспорта данных о сетевом трафике протокола IPFIX.

Объектом исследования является типовая архитектура инфраструктуры «облачных вычислений» на базе средств с открытым исходным кодом: операционные системы на базе ядра операционной системы Linux, протокол доступа к хранилищам данных по сети Интернет, свободно распространяемые средства виртуализации. Основные угрозы информационной безопасности инфраструктуры «облачных вычислений» связаны с проблемой использования разделяемых аппаратных, программных и сетевых ресурсов [1]. Таким образом, существует необходимость поиска подхода к мониторингу событий информационной безопасности внутри инфраструктуры «облачных вычислений». В работе [1] был предложен подход размещения датчиков IPFIX в составе инфраструктуры «облачных вычислений», который подразумевает использование датчиков на «виртуальных сетевых интерфейсах».

Алгоритм профилирования сетевого трафика в рамках инфраструктуры «облачных вычислений» на основе данных, полученных средствами протокола IPFIX, предложен в работе [2]. В основе алгоритма лежит метод максимизации энтропии, описанный в работе [3]. В докладе предлагается решение задачи регистрации аномалии с использованием алгоритма негативной селекции, впервые описанной в работе [4]. Алгоритм негативной селекции является одним из подходов применения искусственных иммунных систем и основан на принципе уничтожения детекторов соответствующих нормальному профилю и сохранению детекторов, отличающихся от него [4]. Применение искусственных иммунных систем в задачах обнаружения вторжений и сетевых атак было предпринято в ряде работ [5–9]. В данной работе делается попытка комбинированного подхода, построения нормального профиля с использованием метода максимизации энтропии и алгоритма негативной селекции. В дополнение развивается подход размещения датчиков IPFIX на интерфейсах виртуальных машин, что актуально для решения задач регистрации аномалии в инфраструктуре «облачных вычислений».

СПИСОК ЛИТЕРАТУРЫ:

1. *Mukhtarov M., Miloslavskaya N., Tolstoy A.* Network security threats and Cloud Infrastructure Services Monitoring // IARA 2011. 22 May 2011. P. 141–145.

2. *Мухтаров М. Р.* Алгоритм построения профиля нормального поведения сетевого трафика на основе данных измерений протокола IPFIX // Материалы IX Курчатовской научной школы. Москва, 2011. 1 CD-ROM.
3. *Gu Y., McCallum A. and Towsley D.* Detecting anomalies in network traffic using maximum entropy // Tech. rep. Department of Computer Science. UMASS. Amherst, 2005. P. 1–6.
4. *Forrest S., Perelson A. S., Allen L. and Cherukuri R.* Self-nonself discrimination in a computer // Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy. IEEE Computer Society Press, 1994. P. 202–212.
5. *Idris I.* E-mail Spam Classification With Artificial Neural Network and Negative Selection Algorithm // International Journal of Computer Science & Communication Networks. 2011. Vol. 1 (3). P. 227–231.
6. *Wen-zhong G., Guo-long C., Qing-liang C.* Improved negative selection algorithm for network anomaly detection on high-dimensional data // Journal of Computer Applications. Volume 29. (2009). P. 805–807.
7. *Котов Д. В.* Подход к обнаружению вторжений на основе модели иммунной системы и иммунокомпьютинга // Материалы семинара «Информатика и компьютерные технологии». СПб.: СПИИРАН, 2010. – URL: http://www.spiiras.nw.ru/rus/conferences/ict/kotov_2010.pptx. Дата обращения: 10.01.2012.
8. *Seredinsky F., Bouvry P.* Anomaly detection in TCP/IP networks using immune systems paradigm // Computer Communications. Volume 30. (2007). P. 740–749.
9. *Gabrielli N. and Rigodanzo M.* An Artificial Immune System for Network Intrusion. Detection on a Web Server: First Results // Proceedings of the 2nd Italian Workshop on Evolutionary Computation (GSICE 2006). Italy, Siena 2006: 1 CD-ROM.

Л. А. Надеинский

О ПОСТРОЕНИИ АЛГОРИТМА ХЭШИРОВАНИЯ, СТОЙКОГО К НАХОЖДЕНИЮ КОЛЛИЗИИ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ГРАФИЧЕСКИХ ПРОЦЕССОРОВ

В научно-технической литературе рассматривается активно используемая уязвимость хранения паролей в хэшированном виде, основанная на одном из методов распараллеливания последовательных алгоритмов [1, 2].

В ходе работы по исследованию особенностей современной SIMD-архитектуры выявлены такие свойства, как латентность памяти, возможность чтения из памяти только последовательно блоками по 128 байт, осуществление только последовательного обращения к массивам процессорными нитями. Эти особенности применены для разработки и реализации класса стойких к распараллеливанию на SIMD-архитектуре криптографических хэш-функций. Перенос алгоритма на SIMD-архитектуру GPU может быть осуществлен различными способами [3]. Доказано, что для противодействия распараллеливанию на SIMD-архитектуре алгоритмов хэш-функций необходимо, чтобы мощность множества упорядоченных наборов раундов хэширования была не меньше, чем мощность множества всевозможных хэш-кодов, а количество различных реализаций вариантов раундов превышало количество мини-процессоров на GPU [4, 5]. В целях противодействия распараллеливанию необходимо и достаточно организовывать раунды хэширования таким образом, чтобы на каждые несколько тактов работы мини-процессора (не более 800 тактов) осуществлялся доступ к памяти в произвольном порядке. Показано, что алгоритм хэширования, обладающий этими свойствами, не поддается распараллеливанию на современной SIMD-архитектуре.

Предложена программная реализация такой криптографической хэш-функции, скорость работы которой сравнима с реализациями алгоритмами SHA-2.