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.

СПИСОК ЛИТЕРАТУРЫ:

1. Program to recover/crack SHA1, MD5 & MD4 hashes. URL: http://www.golubev.com/files/ighashgpu/readme.htm.
2. World Fastest MD5 cracker BarsWF. URL: http://3.14.by/ru/md5.
3. *Трахтенгерц Э. А.* Программное обеспечение параллельных процессоров. М.: Наука, 1987.
4. Документация по работе с SIMD-архитектурой AMD. URL: http://developer.amd.com/sdks/AMDAPPSDK/assets/AMD_Accelerated_Parallel_Processing_OpenCL_Programming_Guide.pdf.
5. Документация к GPU Nvidia. URL: http://developer.nvidia.com/nvidia-gpu-computing-documentation.

А. А. Панов

ПЕРЕДАЧА ДАННЫХ ЧЕРЕЗ РЕЧЕВЫЕ КАНАЛЫ СИСТЕМЫ GSM

Изначально система GSM позиционировалась как «исключительно речевая» коммуникационная сеть. Одним из известных ее усовершенствований стало добавление возможности передачи данных. Самым распространенным каналом передачи данных, добавленным в сеть GSM, является General Packet Radio Service (GPRS). При этом GPRS-трафик и речевой GSM-трафик разделяют один и тот же радиоканал. Чтобы избежать ухудшения качества обслуживания речевого трафика GSM, речь обладает приоритетом, а остаточная пропускная способность сети отведена под GPRS. Эта пропускная способность напрямую зависит от загрузки сети речевым трафиком, с увеличением которого, соответственно, растет время стояния в очереди на обслуживание пользователей GPRS. К существенным недостаткам GPRS также относятся прерывистая зона покрытия и проблемы совместимости. Кроме того, многие существующие сети GSM имеют ограничение пропускной способности GPRS. Одним из решений данной проблемы может стать использование непосредственно самих речевых каналов GSM для передачи данных.

Другим важным поводом для разработки системы передачи данных по речевым каналам GSM послужила неполная защищенность речи в процессе передачи ее от одного пользователя к другому. Передаваемая речь защищена от несанкционированного доступа лишь на этапе прохождения от абонентского терминала до базовой станции (т. е. в канале радиодоступа). По магистральным каналам GSM и каналам телефонной коммутируемой сети общего пользования (ТфОП) речь передается в открытом виде (PCM — импульсно-кодовая модуляция или ADPCM — адаптивная дискретная импульсно-кодовая модуляция), доступ к ней могут получить как операторы сети, так и неавторизованные пользователи. Решением этой проблемы, в частности, занимались сотрудники английского центра исследований коммуникационных систем, которые свели эту задачу к передаче данных через речевые каналы системы GSM [1].

Входящий речевой сигнал преобразуется в битовый поток речевым кодером, который, в свою очередь, шифруется и направляется в модулятор. На выходе модулятора получаются речеподобные волновые формы, которые и передаются в системе GSM с одного абонентского терминала на другой. Т. е. речь передается как зашифрованные данные.

Таким образом, идея передачи данных по речевым каналам системы GSM сводится к разработке и реализации модема, который на передающей стороне переводит входящий поток данных в набор волновых форм из диапазона тональной частоты (300—3400 Гц) — процесс модуляции, а на приемной стороне осуществляет преобразование полученных волновых форм в битовый поток — процесс демодуляции. По существу, такой модем представляется парой кодер/декодер, кодирующей передаваемые данные в сигнал, который трактуется системой GSM как речь,