Распределенная система восстановления паролей*

Д. В. Закаблуков[1,2], С. В. Пикулин[1,3], А. А. Чиликов[1,2]

[1]Passware, Inc., Mountain View, CA 94040, USA
[2]МГТУ им. Баумана, 105005, Москва, 2-я Бауманская 5, Россия
[3]ВЦ РАН, 119333, Москва, Вавилова 40, Россия

dimaz@passware.com, spikulin@gmail.com, chilikov@passware.com

Аннотация.

В современных информационных системах широко используются механизмы защиты данных, в том числе с использованием шифрования. Задача получения доступа к защищенным данным часто возникает в компьютерной криминалистике. В ряде случаев единственным способом достичь этого является перебор паролей. Применение современных стойких алгоритмов делает указанную задачу крайне трудоемкой. Одним из путей ее решения является использование высокопроизводительных вычислительных кластеров. В рамках доклада мы расскажем о нашем опыте разработки и сопровождения коммерческих систем такого класса (Passware Kit Forensic). Речь пойдет об особенностях архитектуры распределенного гетерогенного кластера, возникающих проблемах и путях их решения.

Ключевые слова

Параллельные вычисления, компьютерная криминалистика, перебор паролей, аппаратное ускорение, CUDA, OpenCL, FPGA.

1 Введение

Задача эффективного восстановления доступа к защищённым данным при утрате пароля чрезвычайно актуальна. Компьютерные криминалисты заинтересованы в извлечении цифровых улик с носителей и портативных устройств, полученных в ходе следственных действий; подразделения безопасности коммерческих предприятий и правительственных организаций проводят аудит стойкости паролей, применяемых сотрудниками предприятия; широкий круг пользователей нередко сталкивается с ситуацией утраты пароля к важному документу или сервису.

В тех случаях, когда пароль не может быть восстановлен мгновенно, требуется переборная атака. Эффективность атакующей системы определяют следующие факторы:
– способность к использованию для вычислений разнородного оборудования, включая центральный процессор (CPU), графические карты (GPU) и др.;
– возможность построения вычислительного кластера (на базе ресурсов, объединенных в сеть);
– максимально полный учет информации, известной о пароле до начала атаки.

Доклад будет посвящен рассмотрению архитектуры вычислительных кластеров, постренных на базе программного продукта *Passware Kit Forensic* и предназначенных для решения указанной задачи.

Основными требованиями, предъявляемыми к рассматриваемой системе, являются производительность, надёжность, удобство эксплуатации, низкая стоимость владения и масштабируемость. Специфической особенностью переборных кластеров на базе Passware Kit является то, что их развертывание и эксплуатация производятся полностью силами пользователя; при этом команда разработки сопровождает продукт удаленно.

* Работа второго автора выполнена при финансовой поддержке РФФИ (проект 13-01-00923) и программы № 3 фундаментальных исследований ОМН РАН.

2 Описание переборных атак

Настройки переборной атаки описываются древовидной иерархической структурой. Каждой вершине дерева настроек соответствует определенная последовательность паролей; корень дерева задает множество паролей для перебора в рамках данной атаки.

Концевые вершины (листья) дерева настроек могут иметь один из следующих типов: *«Constant»* — фиксированное слово; *«Brute Force»* — полный перебор всех слов в заданном диапазоне длин с буквами из заданного алфавита; *«Dictionary»* — перебор по словарю; *«Previous Passwords»* — перебор по списку паролей, найденных продуктом в ходе предыдущих атак; *«Xieve»* — специальный эвристический алгоритм, порождающий «произносимые» сочетания букв.

«Модификаторы» — это вершины дерева настроек с одним потомком: *«Mix Casing»* — преобразования регистра, например $[test] \mapsto [Test]$ или $[ab] \mapsto [ab, aB, Ab, AB]$ и т п.; *«Reverse Password»* — переворачивание слова, $[abc] \mapsto [cba]$.

Комбинирование атак производится с помощью вершин дерева с двумя и более потомками: *«Join»* — конкатенация паролей, $([a, b], [c, d]) \mapsto [ac, ad, bc, bd]$; *«Append»* — слияние списков паролей, $([a, b], [c, d]) \mapsto [a, b, c, d]$.

Вершины указанных типов могут комбинироваться произвольно с соблюдением правил о количестве потомков.

Переборная атака заключается в том, чтобы максимально быстро проверить все пароли, заданные настройками атаки. Никакой пароль из списка не должен быть пропущен даже в случае сбоев и ошибок. Состояние атаки периодически сохраняется так, чтобы при остановке переборного процесса атака могла быть продолжена приблизительно с того же места с минимальными потерями затраченных ресурсов.

3 Общая архитектура распределенной системы

В распределенной системе перебора паролей участвуют сущности двух типов: серверы и агенты. Потенциально в кластере может присутствовать неограниченное количество серверов и агентов.

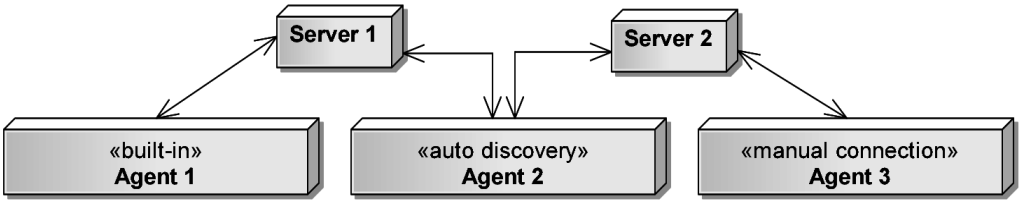

Рис. 1. Схема подключения агентов и серверов в кластере Passware Kit.

В качестве сервера выступает экземпляр приложения Passware Kit Forensic. Функции сервера заключаются в следующем: управление переборными атаками; отслеживание состояния агентов; распределение вычислительной нагрузки между доступными агентами; дополнительная проверка результатов вычислений, произведенных агентами, в тех случаях, когда для вынесения вердикта о правильности пароля требуется расшифровка целевого документа, хранящегося только на сервере. Агент выполняет следующие функции: выполнение заданий, поступающих от сервера; мониторинг аппаратных ресурсов, доступных на данной физической машине; эффективное использование располагаемых вычислительных ресурсов для целей атаки.

На каждой физической машине, выделенной под вычисления, работает один Passware агент. Функциональность агента включена в приложение Passware Kit Forensic, в этом случае говорят о встроенном (*built-in*) агенте. Иной тип агента — удаленный (*remote*), выполняется в рамках отдельного приложения *Passware Kit Agent*. Серверы взаимодействуют с удаленными агентами по некоторому сетевому протоколу.

Различные серверы могут одновременно осуществлять атаки на разные защищенные документы независимо друг от друга. В процессе работы над атакой сервер делит общий объем работ по перебору на относительно небольшие части — *задания*, каждое из которых может быть выполнено одним агентом в течение времени порядка 1 минуты. Каждый агент может выполнять несколько заданий параллельно в зависимости от доступных ему вычислительных ресурсов. Задание является минимальной единицей сохранения состояния переборной атаки.

Имеется два режима подключения агента к серверам: *автоматический* и *ручной*. При ручном подключении агент может выполнять задания, приходящие только от одного сервера, к которому данный агент прикреплен; для прочих серверов в системе этот агент недоступен. В автоматическом режиме агент подключается ко всем серверам, доступным по локальной сети. Агент выполняет задания в рамках некоторой атаки вплоть до ее завершения. После окончания атаки агент может подключиться к другой атаке, возможно, выполняемой на другом сервере.

4 Архитектура агента

Для ускорения процесса перебора паролей помимо CPU могут использоваться различные устройства (*акселераторы*). Passware Kit поддерживает работу со следующими акселераторами: Nvidia GPU, AMD GPU, Tableu TACC1441; также имеется возможность задействовать Amazon EC2 GPU Cluster.

Агент периодически измеряет производительность каждого из доступных акселераторов и вычисляет некоторую интегральную характеристику общей производительности агента. Эта характеристика передается серверу, который использует ее при распределении заданий.

GPU. Для работы с GPU–акселераторами Passware Kit Forensic использует технологии CUDA (Nvidia GPUs) [1], CAL/IL и OpenCL (AMD GPUs) [2]. Особенностью использования GPU является необходимость определения параметров, обеспечивающих максимальную производительность для каждого файла.

Рассмотрим эту задачу более подробно. Исполняемый код (*ядро*) загружается на GPU и может исполняться параллельно несколькими *потоками*. Потоки объединяются в b *блоков*, каждый из которых содержит ровно t потоков. За выполнение потоков в блоке отвечает *потоковый процессор*. Пусть w — максимальное количество потоков, исполняемых одним потоковым процессором параллельно, а s — количество потоковых процессоров. Параметры w и s зависят только от устройства. Процесс вычислений на GPU основан на следующем допущении: каждый потоковый процессор работает ровно с одним блоком, пока все потоки в блоке не закончат работу. Под *калибровкой* будем понимать определение значений параметров t и b, оптимальных с точки зрения производительности. Практика показывает, что максимальная производительность GPU достигается при выполнении двух условий: t кратно w, b кратно s. При этом производительность равна $N_{GPU} = t \cdot b/\Delta$, где Δ — время выполнения ядра на GPU. Процесс калибровки заключается в последовательном выполнении ядра при возрастающих значениях параметров (t, b) и нахождении максимума функции N_{GPU}.

Для повышения надежности работы системы и контроля целостности результатов вычислений предусмотрен механизм самотестирования. Суть его заключается в следующем: вместе с перебираемыми паролями на обсчет на GPU отправляются контрольные значения, правильные результаты обсчета которых известны заранее. Необходимость применения такого рода механизма продиктована тем, что GPU–акселераторы более подвержены сбоям по сравнению с CPU.

Tableu TACC1441. Программируемые логические интегральные схемы (ПЛИС, FPGA) широко применяются для выполнения ресурсоемких операций. Достоинством таких схем является низкое энергопотребление в сравнении с другими устройствами (к примеру, GPU) и гибкость в настройке под конкретный алгоритм. Одной из самых первых ПЛИС, предназначенных для ускорения перебора паролей, является Tableu TACC1441. Именно это устройство получило наибольшее распространение среди криминалистов. К достоинствам TACC1441 можно также отнести возможность объединения нескольких устройств в цепочку в целях увеличения производительности системы.

Amazon EC2. Облачные технологии позволяют развернуть высокопроизводительный кластер без необходимости закупки аппаратного обеспечения. Встроенный Passware Kit Agent предоставляет возможность использования Amazon EC2 GPU cluster для ускорения перебора паролей. Для этого дополнительно необходимо иметь доступ к аккаунту Amazon и оплатить использование кластера. Особенностью использования Amazon EC2 GPU cluster является большое время отклика при отправке задания в облако, сопоставимое с временем обсчета самого задания. Для того, чтобы уменьшить эти временные издержки, используется конвейер: в облако следующее задание отправляется без ожидания прихода результатов обсчета предыдущего задания. Такой подход применим к любому облачному сервису, поэтому, теоретически, распределенная атака Passware Kit Forensic масштабируема на любое облако.

Сравнение различных акселераторов. Приведем результаты тестирования различных акселераторов в Passware Kit Forensic на примере файла формата MS Office 2007 [5]:

Акселератор	Скорость перебора (паролей в секунду)	Цена	Соотношение производительность/цена
CPU Intel Core i5 750 @ 2.67GHz (4 ядра)	981	$ 190*	1
Tableau TACC1441	3373	$ 3820**	0,17
GPU NVIDIA GeForce GTX 470	10113	$ 150*	13,06
GPU AMD Radeon HD 7850	20800	$ 180*	22,38

* цены взяты с сайта http://www.amazon.com

** цены взяты с сайта http://www.forensicpc.com/proddetail.asp?prod=TACC1441.

Приведенные данные демонстрируют возможность многократного увеличения производительности кластера за счет использования GPU при сопоставимой стоимости владения.

Список литературы

[1] J. Balfour: Introduction to CUDA. *CME343/ME339*, 2011.

[2] OpenCL. Introduction and Overview. *Khronos Group*, 2010.

[3] А. А. Чиликов: Неравномерные распределения ключей, схемы парольной защиты и цепи Маркова. *Материалы конференции РусКрипто'2013.*

[4] А. А. Чиликов: Алгоритмические и инженерные аспекты анализа защищенных данных. *Материалы конференции РусКрипто'2010.*

[5] http://www.lostpassword.com/hardware-acceleration.htm

[6] С. А. Лупенко, А. М. Луцків: Криптоаналітична віртуальна лабораторія у грід-середовищі. *Тези міжнародної конференції «Кластерні обчислення»*. Київ: 2012. С. 40–44.