



ElcomSoft переводит продукты на архитектуру OpenCL, обеспечивая совместимость с картами семейства AMD Radeon 7000 и ускоряя перебор паролей

Москва, Россия - 8 марта 2012 - Компания ElcomSoft Co. Ltd. обновляет линейку продуктов [Phone Password Breaker](#) и [Wireless Security Auditor](#), добавляя поддержку кроссплатформенного открытого стандарта OpenCL для обеспечения совместимости с последними моделями графических ускорителей производства AMD. С помощью OpenCL компания не только получает доступ к аппаратному ускорению вычислений, доступному в платформах AMD с использованием графических акселераторов семейства AMD Radeon 7000, но и обеспечивает совместимость с будущими моделями ускорителей как производства компании AMD, так и от независимых производителей.

Оба продукта поставляются с обновлённым ядром, увеличивающим скорость перебора паролей на видеокартах производства AMD на 20-50%. Кроме того, в Elcomsoft Wireless Security Auditor добавлено несколько новых типов атак, использующих уязвимости в выборе пароля, вносимые человеческим фактором. Новые типы атак позволяют существенно повысить вероятность успешного и своевременного раскрытия сетевого пароля.

Переход на архитектуру с кроссплатформенным открытым стандартом OpenCL

Переход на открытую архитектуру OpenCL открывает продуктам компании полноценный доступ к мощным вычислительным ресурсам последних моделей игровых видеокарт производства AMD. В частности, продукты ElcomSoft могут использовать мощные графические процессоры видеокарт семейства AMD Radeon HD 7000 (модели 7750, 7770, 7950, 7970). В дополнение к этому, новое ядро продуктов ElcomSoft оптимизировано для использования аппаратуры AMD, предоставляя дополнительный выигрыш в производительности порядка 20-50% в сравнении с предыдущими версиями.

«Поддержка OpenCL – это важно», считает ведущий аналитик компании Андрей Беленко. «С тем разнообразием аппаратных архитектур и программных платформ, который сложился в последние годы, говорить о какой-либо универсальности не приходилось. Каждую новую модель видеокарт приходилось

тестировать на предмет совместимости с нашими продуктами, и далеко не всегда с положительным результатом. С переходом на открытую кроссплатформенную архитектуру OpenCL исчезает проблема совместимости. Продукты ElcomSoft, переведённые на эту архитектуру, уже получили возможность работы с аппаратным ускорением последнего поколения видеокарт AMD Radeon 7000. При этом обеспечивается полная совместимость как с уже существующими, так и будущими моделями ускорителей. Новые версии видеркарт AMD с нашими продуктами заработают сразу, без необходимости обновления».

«Мы не являемся слепыми поклонниками открытых архитектур», говорит Владимир Каталов, президент ElcomSoft. «Архитектура OpenCL даёт реальное преимущество в производительности и совместимости с платформой AMD, и мы с удовольствием используем эту архитектуру. В то же время на платформах, собранных на основе графических ускорителей от NVIDIA, такого выигрыша в производительности не наблюдается; напротив, производительность OpenCL с ускорителями NVIDIA получается ниже, чем при использовании архитектуры CUDA, собственной разработки NVIDIA. Для нас важен каждый лишний процент скорости перебора, поэтому мы не пошли по пути унификации и упрощения наших продуктов. Оптимизированный код для видеокарт NVIDIA продолжает работать под управлением архитектуры CUDA».

Даже с использованием графических ускорителей скорость перебора паролей Wi-Fi по алгоритму WPA/WPA2 PSK остаётся невысокой. С учётом минимально возможной длины пароля в 8 знаков восстановление таких паролей методом полного перебора в разумные сроки невозможно. В связи с этим компания продолжает разработку алгоритмов, позволяющих использовать потенциальные уязвимости и слабость паролей, вносимые человеческим фактором. В новую версию Elcomsoft Wireless Security Auditor вошло четыре новых типа атак, позволяющих как комбинировать слова из нескольких разных словарей, так и использовать различные мутации словарных слов. «Новые методы атак позволяют выявлять слабые пароли», комментирует президент ElcomSoft Владимир Каталов. «Целью продукта является выявление слабых мест в защите беспроводных сетей. На сегодня самое слабое звено – это люди.»

Предыстория

Современные трёхмерные игры требуют всё больших вычислительных ресурсов, повышая требования к производительности видеокарт. Это послужило причиной того, что производительность современных графических ускорителей, обычных игровых видеокарт, в десятки раз превосходит скорость вычислений центрального процессора.

До недавнего времени использовать эти немалые вычислительные ресурсы могли только разработчики компьютерных игр, работающие с трёхмерной графикой в режиме реального времени. Причиной этого было принципиальное ограничение, присущее распространённым на тот момент видеркартам: их процессоры не были способны производить точные целочисленные вычисления, всегда выдавая лишь приблизительный результат с плавающей точкой. Такой «приблизительной точности» было вполне достаточно для вывода на экран быстро движущегося изображения, но использовать приблизительные вычисления для каких-то практических нужд возможности не было.

Ситуация изменилась с выпуском компанией NVIDIA нового поколения графических ускорителей, способных к целочисленным вычислениям. Одновременно с выходом нового поколения видеокарт NVIDIA анонсировала программную архитектуру CUDA, позволяющую разработчикам использовать вычислительные ресурсы графических процессоров для ускорения задач любого типа. ElcomSoft была одной из первых компаний, использовавших процессоры видеокарт для ускорения перебора паролей.

Основной конкурент NVIDIA, компания ATI (не так давно приобретённая AMD), также выпустила на рынок ускорители, способные производить целочисленные вычисления. Однако с программной поддержкой у компании не заладилось. Многочисленные семейства видеркарт были слабо совместимы с собственной программной платформой компании; зачастую поддержка новых видеокарт так и не добавлялась.



Разработчики ElcomSoft делали всё возможное для поддержки ускорителей от AMD, но поддержка последней серии ускорителей (AMD Radeon HD 7000) так и не была добавлена.

С выходом кроссплатформенной архитектуры OpenCL проблема совместимости была решена. Использование новой архитектуры позволило ElcomSoft получить доступ к вычислительным мощностям последнего поколения видеокарт AMD. Помимо этого, поддержка OpenCL означает и совместимость со всеми будущими моделями ускорителей AMD.

Есть у архитектуры OpenCL и недостатки. Как всякая кросс-платформенная среда, являющаяся по сути прослойкой, дополнительным уровнем абстрагирования от непосредственно аппаратных ресурсов, данная архитектура страдает некоторым общим падением производительности по сравнению с использованием низкоуровневого доступа. Это послужило причиной того, что ElcomSoft продолжает использовать архитектуру CUDA для работы с видеокартами NVIDIA.

О программе Elcomsoft Phone Password Breaker

[Elcomsoft Phone Password Breaker](#) предоставляет доступ к зашифрованной информации, хранящейся в популярных устройствах Apple и BlackBerry. Программа анализирует резервные копии данных, создаваемые программами синхронизации и резервирования устройства, и обеспечивает быстрый доступ к защищенной информации, включая сообщения, электронную почту, историю звонков, контакты, данные органайзера, историю просмотра веб-страниц, голосовую почту, учетные записи и настройки электронной почты, сохранённые учётные записи (включая пароли), историю перемещений, а также пароль к резервной копии.

О программе Elcomsoft Wireless Security Auditor

[Elcomsoft Wireless Security Auditor](#) производит аудит безопасности сетей на основе беспроводной архитектуры Wi-Fi. С помощью Wireless Security Auditor системный администратор может произвести масштабную атаку на все устройства сети, отследив в результате все слабые с точки зрения безопасности узлы. Программа пытается раскрыть пароли шифрования WPA/WPA2 PSK, с помощью которых защищаются беспроводные коммуникации. Использование аппаратного ускорения на основе графических акселераторов AMD и NVIDIA позволяет производить более массированные атаки. Добавленные в последнюю версию виды атак с использованием уязвимостей, вносимых человеческим фактором, позволяют находить пароли, которые могут быть отгаданы злоумышленником.

Наличие и стоимость

Новые версии Elcomsoft Phone Password Breaker и Elcomsoft Wireless Security Auditor уже в продаже. Стоимость предоставляется по запросу; обладателям других продуктов компании предлагаются скидки.

О компании «ЭлкомСофт»

Компания «ЭлкомСофт» – российский разработчик программного обеспечения и поставщик услуг в области восстановления паролей и данных. Решения компании «ЭлкомСофт» используются корпорациями, входящими в список Fortune 500, а также правительственными организациями, правоохранительными органами и спецслужбами по всему миру. Компания «ЭлкомСофт» является членом Российской Криптологической Ассоциации, имеет статус сертифицированного партнера Microsoft (Microsoft Gold Certified Partner) и Intel (Intel Software Partner). Компания основана в 1990 году, головной офис «ЭлкомСофт» находится в Москве. Для получения более подробной информации посетите <http://www.elcomsoft.ru>

