ELCOMSOFT
PROACTIVE SOFTWARE

ElcomSoft исследует 17 мобильных утилит для защищённого хранения паролей. Безопасности не обнаружено

Москва, Россия, 16 марта 2012. Компания ElcomSoft Co. Ltd. провела исследование семнадцати популярных утилит для защищённого хранения паролей в мобильных телефонах на платформах Apple iOS и BlackBerry. Ни один из исследованных продуктов не показал заявленного уровня безопасности. По результатам тестирования лишь один продукт признан относительно безопасным. Пароли, хранящиеся в остальных утилитах, можно восстановить менее, чем за сутки протым последовательным перебором мастер-ключа. Более того, семь из семнадцати утилит никак не защищают хранимые с их помощью пароли; пароли хранятся в открытом виде и могут быть получены моментально.

«Использование алгоритмов стойкого шифрования – необходимое, но совершенно не достаточное условие», говорит Андрей Малышев, криптоаналитик компании ElcomSoft. «Для компрометации всей модели безопасности достаточно единственного слабого звена. Лучшие из протестированных нами утилит могли бы стать действительно безопасными при условии усиления защиты в 10-20 тысяч раз. И это не шутка и не преувеличение: системные хранилища iOS и BlackBerry именно настолько более безопасны».

«Грамотная реализация системы безопасности требует несколько большего, чем навыки программирования», полагает Владимир Каталов, президент ElcomSoft. «Наличие на рынке готовых компонентов, реализующих стойкие криптографические алгоритмы, создаёт у разработчиков иллюзию всемогущества. На самом деле, создание по-настоящему защищённой программы невозможно без грамотного учёта всех особенностей системы».

Предыстория

«Пароли должны быть стойкими. То есть – длинными и сложными для отгадывания, а следовательно – и запоминания. Для доступа к нескольким ресурсам нельзя использовать один и тот же пароль.» Эти требования типичны для обеспечения разумной политики безопасности, но каково приходится пользователям, вынужденным запоминать десятки длинных паролей, состоящих из случайных наборов букв, цифр и специальных символов?

Для решения этой проблемы был создан целый класс программ. Утилиты для хранения паролей призваны не только сохранять введённые в них пароли, но и обеспечивать удобный к ним доступ. Подавляющее большинство подобных программ защищает хранимую информацию одним единственным паролем – мастер-ключом.

В идеале такие программы должны обеспечивать стойкую защиту хранимой информации, используя все возможные методы для обеспечения безопасности. В частности, необходимо использовать уже существующие защищённые хранилища соответствующих программных платформ (iOS и BlackBerry); при этом желательно иметь и дополнительный уровень защиты.

Криптоаналитики компании ElcomSoft решили проверить, насколько желаемое совпадает с действительным, проанализировав работу семнадцати приложений для хранения паролей на смартфонах Apple iPhone (iOS) и BlackBerry.

Результат исследования

Несмотря на громкие рекламные заявления, ни один из исследованных продуктов не обеспечивает сколько-нибудь значимого уровня защиты хранимых с их помощью паролей. Только один из семнадцати продуктов использует встроенные средства защиты iOS; авторы остальных утилит предпочли использовать собственноручно созданную систему защиты. К сожалению, почти в половине случаев защита является чисто декларативной. Оставшиеся утилиты делают попытки использования стойкого шифрования, не достигая, тем не менее, приемлемых с точки зрения безопасности результатов в силу безграмотного или непоследовательного использования готовых алгоритмов.

Результат – мгновенное чтение паролей из хранилищ семи из семнадцати исследованных утилит. Получить пароли из остальных утилит можно атакой простым перебором. При использовании пользователем мастер-ключа максимальной длиной 10-14 цифр продолжительность атаки – менее суток.

Почему утилиты для хранения паролей настолько слабо защищены?

Вопрос о том, почему 7 из 17-ти утилит хранят пароли в открытом, незащищённом виде оставим на совести их разработчиков. В чём же причина того, что утилиты, использующие, казалось бы, правильные шифры и алгоритмы, не обеспечивают заявленного уровня безопасности?

Причина – в отсутствии у рассмотренных продуктов внятной модели безопасности и систематического подхода в её реализации. В настоящее время существует множество готовых библиотек, реализующих алгоритмы стойкого шифрования. Любой разработчик может скачать и использовать такие библиотеки, зачастую – совершенно бесплатно. Тем не менее, использование даже самых стойких алгоритмов абсолютно не гарантирует безопасности всей системы в целом – что и показало исследование ElcomSoft.

Самые современные криптографические алгоритмы устойчивы лишь настолько, насколько стойким является пароль. Использование короткого, нестойкого пароля позволяет восстановить зашифрованные данные методом простого перебора паролей. Чем проще и короче пароль, тем быстрее можно перебрать все возможные варианты, и тем быстрее будет получен доступ к зашифрованной информации.

Разработчики утилит по хранению паролей не учли нескольких важных моментов. Во-первых, все утилиты за исключением одной полностью игнорируют наличие весьма совершенного и достаточно защищённого хранилища информации в платформах iOS и BlackBerry. Просто разместив данные в защищённом хранилище, разработчики получили бы достаточно высокий уровень безопасности совершенно «бесплатно», не предпринимая каких-либо дополнительных усилий. Правда, для того, чтобы разместить хранимые пароли в системном хранилище, нужно как минимум о наличии такого хранилища знать.

Во-вторых, те разработчики, которые предпочли использовать готовые алгоритмы шифрования, совершенно не приняли во внимание особенностей мобильных платформ. Ввод длинных текстов – непростое занятие, если используется миниатюрная клавиатура или небольшой чувствительный к нажатию экран. В силу эргономических причин пользователи мобильных телефонов предпочитают короткие, простые пароли, зачастую состоящие из одних цифр. Такие пароли очень легко взломать методом простого перебора. Использование такого простого, короткого пароля в качестве мастер-ключа позволяет злоумышленнику легко получить доступ к паролем из «защищённого» таким образом хранилища.

Третье и самое главное: способность написать простую утилиту, равно как и доступ к готовым библиотекам стойкого шифрования, отнюдь не делает из обычного программиста квалифицированного специалиста по безопасности.

Выводы

Что могут сделать разработчики для усиления безопасности продуктов для хранения паролей? В идеале – нанять специалиста по компьютерной безопасности. Как минимум – изучить существующую модель безопасности устройтв под управлением BlackBerry и Apple iOS; научиться использовать и использовать системные хранилища, уже имеющиеся в данных системах. Для усиления защиты по сравнению с той, что доступна грамотным разработчикам «по уполчанию», требуется замедление алгоритма генерации крипто-ключей из вводимого пользователем пароля в 10-20 тысяч раз (в скобках - именно так и работает стандартная модель безопасности в iOS и BlackBerry).

Пользователям же мобильных телефонов рекомендуется воздержаться от использования утилит для хранения паролей в их существующей реализации.

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» находятся в Москве. Для получения более подробной информации посетите http://www.elcomsoft.ru

Более подробная информация доступна по адресу http://www.elcomsoft.com/download/BH-EU-2012-WP.pdf