Блог

И все же главная уязвимость мобильных устройств — это пользователь!

В своих заметках о обновлении операционных систем мобильных устройств я уже писал о проблемах при об ...

Google удалила в 2015 году 780 млн. экземпляров "плохой рекламы"

Компания Google опубликовала отчет о своей борьбе со спамом в 2015 году, из которого следует, что об ...

Так ли уж необходима дискриминация владельцев пластиковых карт по стране пребывания?

В любом деле важно не перегнуть палку и не стрелять из пушки по воробьям.

Рейтинг самых плохих паролей

Для того, чтобы получить несанкционированных доступ к чужим аккаунтам, злоумышленникам совсем не обя ...

Конфиденциальность Microsoft Skype, пункт первый

Запускаем Skype, обращаемся к меню программы:
Помощь > Положение о конфиденциальности
Итак, дава ...

Интересно

Редакция PC Week/RE приглашает к сотрудничеству авторов новостных, обзорных и методических статей по корпоративной ИТ-тематике. Ставка гонорара зависит от оперативности и качества материала. Предложения можно присылать по адресу editorial@pcweek.ru.

Статьи

Только на 1,91% всех ПК полностью исправлены все уязвимости

Об уязвимостях операционных систем и прикладного ПО написаны тысячи статей. Необходимо обновлять …

В 2015-м Panda Security добавила в базу более 80 млн. новых вредоносов

Исследователи испанского поставщика систем обеспечения безопасности утверждают, что в прошлом году обнаружили …

Измениться вслед за рынком: какие средства сетевой защиты будут пользоваться спросом в кризис

Развитие технологий сетевой

Алгоритм SHA1 может быть скомпрометирован до конца года

Автор: Владимир Безмалый
09.10.2015

SHA1, один из наиболее востребованных в Интернете криптографических алгоритмов, оказался уязвим к недавно усовершенствованной атаке. Как заявила международная исследовательская группа, он может быть скомпрометирован на протяжении следующих трех месяцев.

SHA1 получил широкое распространение после отказа от гораздо менее стойкого алгоритма MD5. Однако в 2012 г. шифровальщики предупредили что к 2018 г. криптоалгоритм SHA1 может быть скомпрометирован. Теперь, как считают исследователи Centrum Wiskunde & Informatica (Нидерланды), Inria (Франция) и Технологического университета Nanyang (Сингапур), алгоритм будет скомпрометирован задолго до указанного срока. Результаты реальных подделок подписей на его основе могут быть катастрофическими, ведь сегодня, по оценке исследователей, SHA1 используется более чем в 28% всех существующих сертификатов.

Новое исследование показало, что SHA1 намного более уязвим, чем ожидалось, поэтому центры сертификации рассматривают предложение, согласно которому разрешенный выпуск сертификатов SHA1 будет продолжен на 12 месяцев, что фактически означает использование этого алгоритма до конца 2016 г. Ведь на сегодня некоторым крупным организациям сложно использовать более безопасный криптографический алгоритм хеширования для своих цифровых сертификатов и потребуется дополнительный год для осуществления перехода.

Безусловно, исследование международной группы должно быть подтверждено другими исследователями для обеспечения веских доказательств необходимости перехода к использованию более стойкого алгоритма SHA2.

Автор статьи — Microsoft MVP, Microsoft Security Trusted Advisor.

Решения

Маленькая грязная тайна отрасли безопасности

В последние годы центральное место в обсуждении вопросов сетевой безопасности занимают постоянные угрозы повышенной …

Упрощение аварийного восстановления в сложных виртуальных средах

В данном техническом документе рассматривается Выбор правильной стратегии резервного копирования виртуальных машин для эффективного управления...

Непрерывная защита данных

Данный технический документ позволит ответить на вопрос, соответствует ли технология непрерывной защиты данных (CDP …

Скрытые издержки виртуализации

Для того чтобы проект по виртуализации позволил достичь ожидаемых результатов и предполагаемой рентабельности …

Решение проблем аварийного восстановления

Сегодня информация считается одним из

Новости компаний

Каждый пятый пользователь забывает гаджеты в барах

Киберргруппировка BlackEnergy придумала новый вид атак

Десятки игр из Google Play содержат Android-троянец

Больше половины российских компаний в 2015 году столкнулись с утечками информации

ESET: число уязвимостей в Windows выросло в четыре раза