07:39 / 9 Октября, 2015

Эксперты: Использование хэш-алгоритма SHA-1 нужно немедленно прекратить

Теги: хэш-алгоритм, шифрование, коллизия, SHA-1

SHA-1 настолько слаб, что хакеры могут взломать его в ближайшие три месяца.

Одной из наиболее распространенных криптографических хэш-функций в интернете, SHA-1, предположительно приходит конец. Количество времени и финансовые затраты, необходимые для взлома SHA-1, снизились значительно быстрее, чем было рассчитано изначально. По словам ИБ-исследователей, SHA-1 - настолько слабая хэш-функция, что может быть взломана хакерами в ближайшие три месяца.

Алгоритм SHA-1 был разработан в 1995 году специалистами из АНБ в качестве части алгоритма цифровой подписи. Как и другие хэш-функции, SHA-1 преобразует любое входящее сообщение в длинную строку чисел и букв, которая служит в роли криптографических отпечатков пальцев для сообщения.

Такие криптографические отпечатки несут пользу, если являются уникальными. В случае, если два разных сообщения генерируют один и тот же хэш (данные случаи также известны, как коллизия хэш-функции), он может предоставить злоумышленникам возможность для проникновения в системы безопасности банковских операций, процессы загрузки ПО или в любое соединение web-сайтов.

Исследователи из Centrum Wiskunde & Informatica (Нидерланды), Inria (Франция) и Наньянского технологического университета (Сингапур) опубликовали доклад, согласно которому, SHA-1 уязвима к атакам, названным экспертами Freestart Collision. Злоумышленники ищут коллизии хэш-функций, когда одно хэш-значение относится сразу к двум сообщениям. Коллизия может быть использована для подделывания цифровой подписи, позволяя хакерам нарушить соединения, зашифрованные с помощью SHA-1.

В настоящее время взлом SHA-1 стоит всего от $75 тысяч до $120 тысяч. В 2012 году исследователи утверждали, что такая атака обойдется хакерам в 2015 году не меньше чем в $700 тысяч, а в 2018 году - $173 тысячи. Стоимость упала в связи с новой техникой, известной под названием «бумеранг», которая позволяет быстро обнаружить коллизии SHA-1.

ИБ-исследователи настоятельно рекомендуют администраторам переходить с SHA-1 на безопасные хэш-алгоритмы SHA-2 и SHA-3. Стоит отметить, что SHA-2 также создан экспертами из АНБ, а SHA-3 – группой независимых специалистов.