# ОБНОВЛЕНИЕ ХЕШ БЕЗОПАСНОСТИ

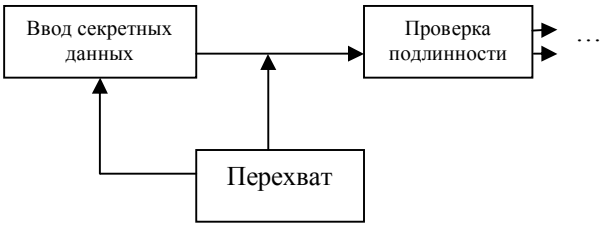
Р.И. Рахимов, Д.Г. Абдуллаев

Узбекистан, Ташкент

На сегодняшний день в связи с развитием информационных и коммуникационных систем, информационная безопасность приобретает более активный характер. Нам известно, что информационная безопасность включает в себя широкий спектр направлений, таких как сетевая безопасность, аудит безопасности и криптографию. Именно этой области посвящена данная статья, а если точнее, данная статья посвящена хеш-функциям, которые на сегодняшний день считаются слабым звеном информационной безопасности.

НИСТ организовала конкурс для нахождения наилучшую замену для текущего стандарта хеширования SHA(Secure Hash Algorithms) – SHA-1 и SHA-2. Криптографы отправляют новые математические алгоритмы, которые в свою очередь усиливают криптостойкость хеш-функций которые используются в электронной цифровой подписи, в сообщениях аутентификации и в некоторых безопасных протоколах Интернета.

Криптографы впервые обсуждали поколение атак в ежегодной Интернациональной Криптологической конференции проходивший в 2004 году, НИСТ работала с криптографическим сообществом для создания более безопасного алгоритма который мог заменить оба алгоритма, SHA-1 который был атакован и ранен китайскими криптоаналитиками, а также SHA-2 потомок алгоритма SHA-1.




Некоторые криптографы говорят, что SHA-3 может быть быстрее и эффективнее чем SHA-2 но оно не может быть далеко лучшее чем SHA-2 потому что она остаётся потомком SHA и в лучшем случае будет более безопасным чем SHA-2.

НИСТ ожидает множество кандидатов на новый хеш-алгоритм, но организаторы даже не надеются что финальный победитель не найдется до 2012 года.

SHA-1 самый широко используемый алгоритм, оно используется во многих приложениях для обеспечение безопасности, а также в таких протоколах как TLS (Transport Layer Security) и SSL (Secure Sockets Layer), S/MIME (Secure/Multipurpose Internet Mail Extinctions), PGP (Pretty Good Privacy), SSH (Secure Shell), и IPsec. Контрольная система исходных кодов, разработанная Линусом Торвальдсом для управления ядра Linux, тоже использует SHA-1 для предотвращения изменения данных. Многие из этих приложений используют SHA-1 для аутентификации, и пока эти приложения безопасны. Многие приложения цифровой подписи тоже используют SHA-1.

Конечно SHA и остальные криптографические стандарты, такие как ECC (Elliptic Curve Cryptography), AES (Advanced Encryption Standard) и RSA имеют официальные требования как компьютерным сетям выполняющие процесс и хранение больших количеств данных.

В самом деле, криптография это технология, которую мы можем встретить во всех приложениях, которые запускаются в мобильных телефонах, в ноутбуках и в DVD устройствах.

И так криптография используется во всех системах, которые можно вообразить. Криптография используется при проектировании низкоуровневых силиконовых–чипов или же в продуктах, написанных на языках программирования высокого уровня.

Итак, на сегодняшний день в системах обеспечивающих безопасность все равно происходит взломы. Это не значит что, криптографический алгоритм установленный в этой системе взломан. Например, из самых последних произведенных успешных взломов несут название “Hannaford Brothers Co. computer systems”, которое под свой потенциал включает уязвимость 4.5 миллионов номеров кредитных и дебитных карт.

Как утверждают специалисты метод Hannaford не взламывает ни шифрограмму и уж точно не хеш-значение данных. Этот метод перехватывает данные в полетной позиции. Во время полета данные отправляются открыто.

В операционных системах для того чтобы поймать это состояние нужно произвести некое торможение процессов. Например в операционной системе Linux для того чтобы получить такое состояние приложения хватит написания не сложного модуля который будет переводить процесс в состояние “sleep” а после прочтения данных вызовет “wake up” для этого процесса, и данные будут считаны как с обычного открытого документа.