ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ WPA2

Ю.С. Камышев, Ю.А. Скудняков

Одним из современных способов защиты информациив сетях Wi-Fi является протокол WPA второго поколения. WPA2 заменил WPA. WPA2, который требует тестирования и сертификации Wi-Fi Alliance, реализует обязательные элементы IEEE 802.11i. Со стандартом 802.11i вся цепочка модуля безопасности (вход в систему, обмен полномочиями, аутентификация и шифрование данных) становится более надежной и эффективной защитой от ненаправленных и целенаправленных атак. Стандарт 802.11r является модификацией стандарта 802.11i. Данный стандарт был ратифицирован в июле 2008 года. Технология стандарта более быстро и надежно передает ключевые иерархии, основанные на технологии Handoff (передача управления) во время перемещения пользователя между точками доступа. Стандарт 802.11r является полностью совместимым с WiFi стандартами 802.11a/b/g/n. Также существует стандарт 802.11w, предназначенный для усовершенствования механизма безопасности на основе стандарта 802.11i. Этот стандарт разработан для защиты управляющих пакетов.Стандарты 802.11i и 802.11w – механизмы защиты сетей WiFi стандарта 802.11n [1]. Но в данной технологии, как и, естественно, во всем есть недостатки, а именно: слабая стойкость пароля на взлом, отсутствие прямой секретности (дешифровка по разделенному ключу), hole196 (по GTK), атака KRACK (Key Reinstallation Attack) и т.д. Также 16 октября 2017 г. эксперты по бесопасности сообщили, что WPA2 официально взломан и больше не может обеспечивать необходимый уровень безопасности. Исходя из вышеизложенного, можно сделать вывод о том, что WPA2 на сегодняшний день является весьма небезопасным протоколом, которым люди вынуждены пользоваться, так как альтернатив пока нет. С другой стороны, в январе 2018 года Wi-Fi Alliance сообщила, что ведутся работы над новым протоколом WPA3. Остается надеяться, что все эти недостатки будут устранены в новой версии.

Литература

1. Geier, J. WPA Security Enhancements. 2003. 137 p.

ОЦЕНКА СОСТОЯНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА БАЗЕ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Е.В. Кармаз, Г.А. Пухир

Для того чтобы обезопасить информационную систему, ряд организаций регулярно проводят тестирование на проникновение в рамках аудита информационной безопасности, что позволяет получить объективную оценку возможности осуществить несанкционированный доступ к ресурсам корпоративной сети или сайта. Процесс тестирования на проникновение является моделированием реальных действий злоумышленника с целью поиска уязвимостей системы защиты. Эта услуга позволяет получить независимую оценку и экспертное заключение о состоянии защищенности информации ограниченного распространения.

Технологии тестирования на проникновение могут осуществляться на базе технических методов и/или социотехнических методов, а также с применением методов социальной инженерии. С их помощью осуществляются санкционированные попытки получения несанкционированного доступа к корпоративной сети и защищаемым активам целевой организации. Методы, как правило, направлены на пользователей конечных систем и позволяют определить реакцию персонала в штатных и нештатных ситуациях, уровень знаний персонала о требованиях безопасности. К некоторым из таких методов можно отнести:

1. Фишинг (побуждение пользователей к вводу конфиденциальных данных (например, паролей) на фальшивой веб-странице легального сервиса.
2. Троянский конь (побуждение пользователя к открытию писем с вредоносными вложениями за счет целевых сопроводительных писем, звонков, наименований файлов и др.).
3. Претекстинг (моделирование определенного сценария, предполагающего вход в доверие к пользователю (за счет предварительного сбора данных об организации, отдельных работниках и их зонах ответственности), с целью побудить выполнить определенное действие).

4. Дорожное яблоко (подбрасывание в общедоступных местах организации (лифт, столовая, парковка) инфицированных носителей информации с мотивирующими к их запуску логотипами/бирками/именами файлов).

После окончания тестирования, специалистами проводится сбор и обработка данных. Часто заказчик хочет знать, кто именно попался на ту, или иную уловку теста. Однако данная информация не передается руководству компании, т.к. проводится тестирование не одного человека, а группы лиц. Соответственно, речь идет об информационной системе, как о едином целом. Исследования показывают, что «человеческий фактор» остается одной из самых распространенных угроз информационной безопасности. Для снижения рисков, связанных с этим обстоятельством, используются различные технические и административные механизмы защиты. Один из них – повышение осведомленности работников, в области информационной безопасности.

ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ХЭШ-ФУНКЦИИ SHA-256 НА БАЗЕ FPGA

М.В. Качинский, А.В. Станкевич

Криптографическая хэш-функция SHA-256 описана в документе RFC 4634 [1] и предназначена для получения хэш-значения фиксированной длины для входного сообщения произвольной длины. Данная функция используется в различных приложениях, связанных с защитой информации, а также в большинстве криптовалют. В указанных приложениях возникает необходимость высокопроизводительных аппаратных реализаций SHA-256. В докладе рассматривается полностью конвейерная реализация хэш-функции SHA-256 для одного блока данных (512 бит) на базе FPGA.

Характерной особенностью алгоритма SHA-256 является длинная цепочка последовательных сложений при вычислении новых значений переменных A и E. Для уменьшения числа сложений в одном такте реализации и, следовательно, повышения тактовой частоты конвейерного процессора вычисление переменных E-H на такт опережает вычисление переменных A-D. Кроме того используется предварительное вычисление сумм W_t, K_t, H и D. Одна ступень конвейерного процессора производит вычисления за один такт частоты синхронизации. Общее число ступеней конвейера с учетом 64 раундов алгоритма SHA-256 и завершающего сложения со значением вектора инициализации равно 67.

Характеристики реализации по отчету средств синтеза пакета ISE 14.7 для кристалла FPGA семейства Kintex7 XC7K160T-3: 27477 триггеров секций, 35161 просмотровая таблица (LUT), тактовая частота – 352 МГц.

При обработке сообщения, длина которого превышает один блок SHA-256 необходимо либо последовательно включить требуемое число процессорных ядер для реализации полностью конвейерного вычислителя, либо организовать итеративные вычисления на одном процессорном ядре, коммутируя с помощью мультиплексора выходные данные процессора на его вход требуемое число раз.

Литература

1. RFC 4634. US Secure Hash Algorithms (SHA and HMAC-SHA). [Электронный ресурс]. – URL: https://tools.ietf.org/pdf/rfc4634.pdf (дата обращения: 26.04.2018).

ДОСТУП К ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Р.В. Кислинский

Под информацией ограниченного распространения в Республике Беларусь понимаются государственные секреты, т. е. сведения, защищаемые государством в целях предотвращения их несанкционированного распространения и создания угрозы национальной безопасности Республики Беларусь, а также конституционным правам и свободам граждан.

Что касается перечня сведений, составляющих государственные секреты Республики Беларусь, то он определен как совокупность категорий сведений в области экономики,