АРХИТЕКТУРА МНОГОКАНАЛЬНЫХ КВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

К.В. МЕЛЬНИКОВ, С.Б. БИРЮЧИНСКИЙ

Одним из основных недостатков современных систем квантовой криптографии является низкая скорость передачи данных, что обусловлено как техническими ограничениями для существующих систем, так и ограничениями, вызванными применяемыми алгоритмами. Использование систем с малой скоростью передачи данных не позволяет полностью реализовать все возможные методы криптографической защиты.

Для обеспечения наивысшего уровня секретности в симметричных криптосистемах необходимо формировать последовательность криптографического ключа с длиной, равной длине передаваемого сообщения.

Поскольку скорость передачи данных в существующих системах квантовой криптографии низка, устойчивость систем к шумовым воздействиям является слабой.

Одним из способов повышения скорости передачи информации является переход к многоканальным системам. Авторами предложены варианты архитектуры различных многоканальных систем связи, использующих квантовую криптографию.

Одним из методов перехода к многоканальности в квантовых криптографических системах является одновременное использование на передающей стороне нескольких источников фотонов с различными длинами волн, передаваемых по одному и тому же каналу связи. Разделение фотонов по частоте в этом случае осуществляется классическими методами спектральной селекции. Преимуществами являются простота реализации системы.

Возможным направлением развития является использование псевдо-квантовокриптографических систем. Реализация такой системы основана на использовании традиционных каналов связи, как волоконно-оптических, так и атмосферных оптических линий связи.

Разработана оптическая схема детектирования направления поляризации фотона, позволяющая определить поляризацию единичного фотона с вероятностью выше 50%. Предложен способ повышения точности определения поляризации фотона.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ НЕДОКУМЕНТИРОВАННОГО ОТЛАДОЧНОГО РЕЖИМА ПРОЦЕССОРОВ ФИРМЫ AMD НА БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Е.Е. ОРЛОВ, О.К. БАРАНОВСКИЙ

Аппаратное обеспечение современных компьютерных систем создается путем интеграции большого числа базовых компонент (модулей). Сложность таких систем является причиной того, что выполняемые аппаратным обеспечением функции могут не соответствовать заявленным в спецификации. Эти отличия могут вноситься преднамеренно, например, недокументированные возможности, внедряемые для послепроизводственного тестирования компаниями-производителями, или для проведения вредоносной деятельности, либо быть вызванными ошибками в технологиях разработки и производства.

Характерным примером ошибки в аппаратном обеспечении может являться проблема с когерентностью L1 кэша многоядерных процессоров Intel Core 2 Duo [1].

Предложены сценарии атак отказа в обслуживании на основе управления модельно-специфическими регистрами, являющимися механизмом перевода компьютерных систем в недокументированный отладочный режим. Условием срабатывания упомянутых выше сценариев является обработка компьютером определённого числа.

Показано, что при некорректной настройке этого режима возможен управляемый сбой работы операционной системы. Предложенные сценарии были также реализованы на виртуальных машинах и продемонстрировали успешность атак.

Литература

1. Касперский К. Дефекты проектирования Intel Core 2 Duo / [Электронный ресурс]. Режим доступа: http://www.insidepro.com/kk/286/286r.shtml. Дата доступа: 05.04.2012.

МАРШРУТИЗАЦИЯ ПО ТРЕБОВАНИЮ С МНОЖЕСТВЕННЫМИ ПУТЯМИ НА ОСНОВЕ ВЕКТОРА РАССТОЯНИЙ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

А.А. ОХРИМЕНКО, С.Б. САЛОМАТИН

Ключевой особенностью беспроводных сенсорных сетей является способность ретрансляции сообщений от одного сенсорного узла к другому, что позволяет передавать информацию на значительное расстояние при малой мощности передатчиков.

При выборе алгоритма маршрутизации в беспроводных сенсорных сетях необходимо учитывать ограниченность вычислительных ресурсов сенсорных узлов и срок службы элементов питания. Одним из таких алгоритмов является протокол маршрутизации по требованию на основе вектора расстояний (AODV), который исключает периодическое обновление маршрутов и использует их только при необходимости.

Протокол AODV является эффективным с точки зрения производительности сети, однако позволяет злоумышленнику легко фальсифицировать маршрутную информацию для перенаправления трафика и запуска DoS-атак. Таким образом, для предотвращения подобного рода воздействий, существует необходимость защиты маршрутной информации от несанкционированных узлов.

Для повышения устойчивости к разрыву соединений предлагается использовать протокол маршрутизации по требованию с множественными путями на основе вектора расстояний (AOMDV), в котором маршруты рассчитываются таким образом, чтобы гарантированно отсутствовали петли маршрутизации и пересекающиеся пути.

Следует также отметить, что протокол AOMDV обеспечивает промежуточные сенсорные узлы альтернативными маршрутами, что способствует сокращению частоты обнаружения маршрутов, экономии ресурсов сенсорных узлов и уменьшению нагрузки на беспроводную сенсорную сеть.