РАЗРАБОТКА И АНАЛИЗ ЭФФЕКТИВНОСТИ УНИВЕРСАЛЬНЫХ КРИПТОГРАФИЧЕСКИХ МОДУЛЕЙ ЗАЩИТЫ ДАННЫХ, ПЕРЕДАВАЕМЫХ В МУЛЬТИСЕРВИСНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Ушакова М.Е.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. ТКС, тел. (057) 7021320,
E-mail: Mariya.Ushakova@gmail.com ; тел. +38 097 3326967

The given work is considered the method of application the cryptographic modules, to supply the secure data storing, processing and transferring in multiservice telecommunication networks. The analysis of user channels security has been developed and the supplying of information security in multiservice systems based on the IP Security suite of protocols has been considered. Also the foundations of attestation of the cryptographic modules have been investigated. On the basis of the considered aspects the conclusions displaying the main requirements to cryptographic modules, integrated in multiservice systems have been given.

Введение: Мультисервисные сети (МС) позволяют операторам расширить свои возможности в направлении предоставления новых сервисов, формируя основу для дополнительных услуг широкому кругу пользователей. Под мультисервисностью подразумевается предоставление телекоммуникационных услуг с различными требованиями к параметрам качества обслуживания при единой инфраструктуре доступа передачи данных. МС подвержены широкому спектру потенциальных угроз несанкционированного доступа (НСД) к информации и ее разрушения, что обусловливает необходимость разработки различных средств и функций защиты. При этом для распределенных МС главной задачей видится обеспечение безопасности управляющих каналов обмена информацией. Проблема защиты этих каналов усложняется тем, что внедрение и использование процедур защиты данных не должны приводить к заметному снижению производительности телекоммуникационной системы (ТКС) в целом.

Криптографические преобразования информации являются эффективным средством обеспечения ее конфиденциальности, целостности и подлинности. Эти механизмы предполагают использование процедур шифрования (как для файлов, так и для потоковых данных), выработки цифровых отпечатков, электронной цифровой подписи, а также поддержки специализированных защищенных сетевых протоколов. Важным аспектом также является реализация мультипользовательского управления секретами (криптографическими ключами и материалом для их выработки), в том числе, и в режиме реального времени.

Все эти задачи определяют специфические требования к криптографическим модулям (КМ), встроенным в сетевые промежуточные и терминальные устройства. Использование КМ в совокупности с необходимыми техническими методами может обеспечить защиту от широкого спектра потенциальных угроз. Однако для современных МС требуется разработка именно универсальных модулей, которые могли обеспечивать выполнение всего спектра преобразований, необходимых для различных типов трафика ТКС, а также обладать многофункциональным интерфейсом ввода ключей и данных.

Поэтому основными задачами работы являются анализ существующих сетевых служб МС, сетевых протоколов, используемых в рамках объединенных сетей, применение методов и протоколов защиты сетей с помощью криптографических средств, а также нахождение общих элементарных преобразований информации, используемых в этих средствах. В работе обсуждается вопрос отказоустойчивости и реконфигурируемости КМ, а также алгоритмическая основа приоритезации криптозащищенных пакетов для соблюдения соглашений о качестве обслуживания в сети

Формирование защищенных пользовательских каналов

Все определенные выше задачи формируют высокие требования к КМ, ориентированным на применение в системах защиты МС от НСД:

- высокая стойкость при криптоанализе на основе большого объема известного или подобранного текста, зашифрованного на одном и том же ключе;
- высокая скорость шифрования при программной реализации и функционирование в режиме реального времени;
- сохранение возможности произвольного доступа к данным – определяет необходимость использования алгоритмов блочного шифрования в различных режимах.

Основным защищенным сетевым стеком, который используется на сегодняшний день в МС (и Интернет в качестве транспортной сети), является стек протоколов IP Security (IPsec). Используя его в качестве основы, становиться возможным соблюсти обозначенные требования к КМ. IPsec – это множество взаимосвязанных протоколов, обеспечивающих реализацию процедур шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов. Кроме того, IPsec включает протоколы для защищенного обмена ключами в сети Интернет. Протоколы стека IPsec работают на сетевом уровне, что делает IPsec наиболее гибким и функциональным среди других защищенных стеков, и определяет возможность его использования для защиты любых протоколов базирующихся на TCP (надежный транспорт) и UDP (транспорт с негарантированной доставкой), в том числе и ориентированных на трафик реального времени.

IPsec-протоколы можно разделить на два класса: протоколы отвечающие за защиту потока передаваемых пакетов и протоколы обмена криптографическими ключами. На настоящий момент в стеке определен только один протокол обмена криптографическими ключами – IKE и два протокола обеспечивающих защиту передаваемого потока – ESP (обеспечивает целостность и конфиденциальность передаваемых данных) и AH (гарантия целостности потока). В соответствии с протоколом IPsec архитектура средств безопасности информационного обмена разделяется на три уровня. Добавление протоколов для управления ключами в многопользовательской среде в режиме реального времени производиться с привлечением других стандартов защиты (например, MIKEY). Формирование безопасных сессий для передачи трафика МС может выполняться на основе протоколов SDP, RTP/SRTP. На верхнем уровне расположены следующие протоколы:

- протокол согласования параметров виртуального канала и управления ключами (ISAKMP), обеспечивающий общее управление защищенным виртуальным соединением, включая согласование используемых алгоритмов криптозащиты, а также генерацию и распределение ключевой информации;
- протокол аутентифицирующего заголовка AH, предусматривающий аутентификацию источника данных, проверку целостности данных и их подлинности после приема, а также защиту от навязывания повторных сообщений;
- протокол инкапсулирующей защиты содержимого ESP, обеспечивающий криптографическое закрытие передаваемых пакетов сообщений и предусматривающий также выполнение всех функций протокола AH.

Гарантии целостности и конфиденциальности данных в IPsec обеспечиваются за счет использования механизмов аутентификации и шифрования. Последние основаны на предварительном согласовании сторонами информационного обмена т.н. "контекста безопасности" – применяемых криптографических алгоритмов, алгоритмов управления ключевой информацией и их параметров. Спецификация IPsec предусматривает возможность поддержки сторонами информационного обмена различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей (в том числе и многопользовательскую при применении

альтернативных механизмов). При этом результатом согласования контекста безопасности является установление индекса параметров безопасности (SPI), представляющего собой указатель на определенный элемент внутренней структуры стороны информационного обмена, описывающей возможные наборы параметров безопасности.

Функцию согласования набора применяемых алгоритмов и их параметров предусматривает протокол ISAKMP, в соответствии с которым при формировании защищенного виртуального канала должно быть выработано общий контекст безопасности SA (Security Association) с последующим использованием его элементов (алгоритмы, ключи).

АН обеспечивает целостность IP-пакетов и аутентификацию источника данных, а также защиту от воспроизведения ранее посланных пакетов. Этот протокол полностью защищает от подлога и случайного искажения содержимое пакетов, включая данные протоколов более высоких уровней. АН предоставляет меры защиты от атак, ориентированных на нарушение целостности и подлинности данных.

ESP обеспечивает выполнение следующих функций по защите информационного обмена:

- криптографическое закрытие содержимого IP-пакетов;
- формирование и проверка цифровой подписи IP-пакетов для их защиты от нарушений подлинности и целостности (IPv4, IPv6);
- защита от воспроизведения пакетов.

Наиболее используемыми в протоколах АН и ESP являются два алгоритма аутентификации – HMAC-MD5 и HMAC-SHA1, которые являются алгоритмами аутентификации с секретным ключом. Для обеспечения совместимой работы оборудования и программного обеспечения на начальной стадии реализации протокола IPsec алгоритм аутентификации HMAC-MD5 используется по умолчанию.

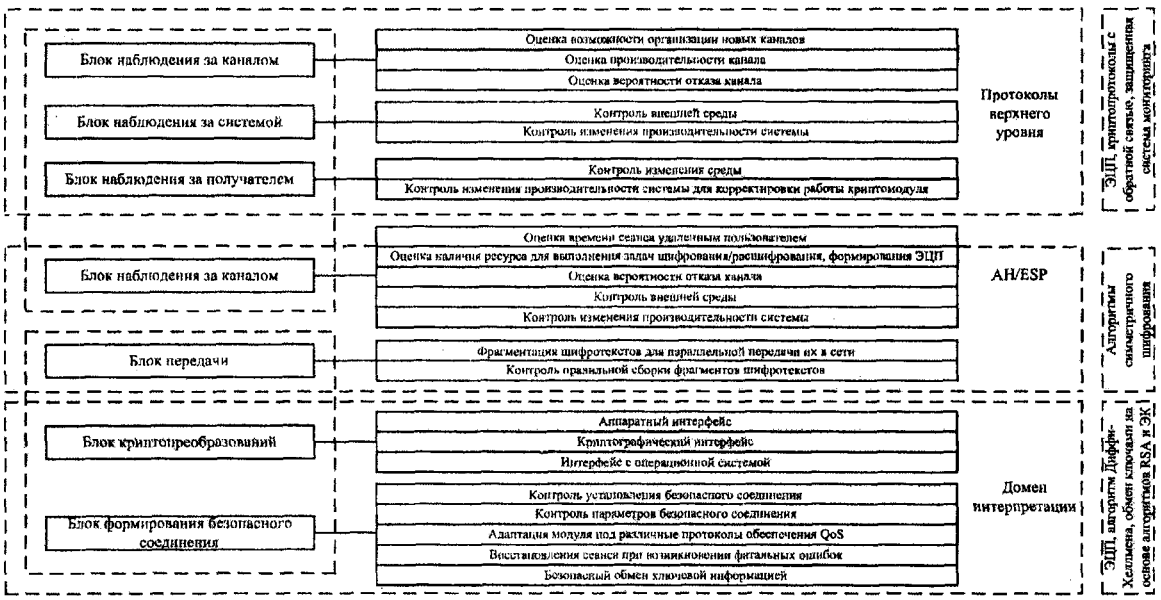

Рис.1. Использование криптографического модуля в стеке IPsec

Для протокола ESP алгоритм HMAC-MD5 принят по умолчанию и необходим для обеспечения IPSec-совместимости. В качестве альтернативы AES (DES для устаревшего варианта стандарта) определены алгоритмы CAST-128 и RC5. Могут быть рекомендованы к применению алгоритмы MARS, RC6, Twofish, GOST, SNOW и другие.

Вариант использования КМ в стеке IPsec и реализация функций КМ представлены на рис.1.

Функции стека IPsec могут дополняться механизмами более высоких уровней (TLS, S/MIME), что требует возможности КМ по формированию электронных цифровых подписей. Все определенные выше требования формируют функцию эффективности (полезности) работы КМ. Целью разработчика является максимизация значения функции эффективности при ограничениях, определяемых в рамках задачи аттестации КМ, при условиях наличия определенной алгоритмической и элементной базы.

1. Аттестация универсального криптографического модуля

Стандартом FIPS 140-2 (FIPS 140-3 вводится в действие) предусмотрено четыре уровня защищенности КМ, что позволяет экономически целесообразным образом защищать данные разной степени критичности в разных условиях. Перед КМ ставятся следующие высокоуровневые функциональные цели безопасности:

1) применение и безопасная реализация утвержденных функций безопасности для защиты информации ограниченного доступа;
2) обеспечение защиты модуля от несанкционированного использования и нештатных методов эксплуатации;
3) предотвращение несанкционированного раскрытия содержимого модуля (криптографических ключей и других данных, критичных для безопасности);
4) обеспечение отображения (индикации) режима работы (состояния) модуля;
5) обеспечение доверия тому, что модуль функционирует должным образом при работе в утвержденном режиме;
6) обнаружение ошибок в функционировании модуля и предотвращение компрометации информации ограниченного доступа и данных модуля, критичных для безопасности, вследствие подобных ошибок.

В ходе проведения аттестации необходимо дать оценку, относительно эффективности интеграции КМ в окружение ТКС. Оценка производится при использовании мажоритарного принципа, рекомендуемого NIST. Также рекомендуется использовать аппарат субъективной логики, который состоит в том, чтобы дать экспертам возможность выразить свое отношение, относительно степени надежности системы, использующей КМ, а затем сформировать обобщающее мнение. Возможным также является анализ эффективности интеграции КМ в информационную систему, например, с использованием стандарта Common Criteria v 2.2 (v 3.0).

Выводы:

Для защиты данных, передаваемых в МС, актуальным является использование универсальных КМ. Это позволит удовлетворить потребности в защите сетевых устройств, ориентированных на передачу и обработку трафика с различными характеристиками. В работе предложены методы интеграции КМ в информационные системы без понижения общего уровня защиты. КМ способен поддерживать популярные на сегодняшний день сетевые протоколы: IPsec, TLS, S/MIME и др, а также управлять приоритезацией пакетов для соблюдения соглашений о качестве обслуживания в криптозащищенных туннелях. Совмещение функций маршрутизации и криптографической защиты позволит решать задачу защищенной многоточечной многопутевой маршрутизации.

Возможна как аппаратная, так и программная реализация функций КМ. От этого зависит уровень надежности модуля, его скоростные характеристики и возможности настройки. Спецификация модуля, включает определение криптографического периметра, реализуемых функций и режимов, описание модуля, его аппаратных и программных компонентов, а также документированную политику безопасности, которая увязывается с политикой безопасности сети.