Генератор Фибоначчи порождает практически апериодическую последовательность шифрующих байтов. Эта последовательность невырождена, нефальсифицируема по открытому и зашифрованноиу экземплярам фрагмента текста. Она легко может быть сделана непрогнозируемой и тотальной с помощью фальсификации текущих значений ключа. По-видимому, имеются возможности обеспечить две последние характеристики без увеличения стоимости вычислений.

Литература: 1. С. Макаренко, А. Брусникин, Алгоритмы шифрования для передачи данных в открытых сетях - В зб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.– Науково-технічний збірник. – Випуск 2. – К.: НДЦ "Тезіс" НТУУ "КПІ".–2001.– 273 с. С. 223. 2. В. В. Мясоедов, Абсолютная защита данных. Know how, © В. В. Мясоедов, Киев, 2000 г, 10 с. 3. Без фамилии авт., Золотое сечение, Математическая энциклопедия, т. 2 Д-КОО – М.: "Советская Энциклопедия",–1979.–110 4стб. С. 466.

УДК 681.3.06

ШЛЮЗ БЕЗОПАСНОСТИ “КРИПТОМАРШРУТИЗАТОР 1.0” С УДАЛЕННЫМ УПРАВЛЕНИЕМ И ЕГО ВОЗМОЖНОСТИ

Иван Горбенко, Александр Волощук*, Виталий Вервейко, Юрий Горбенко, Сергей Полчанинов

*ХНУРЭ, *Укрсоцбанк*

Анотація: **Розглядається задача побудови та реалізації системи захисту міжмережевого трафіку на основі створення тунелів між локальними мережами з використанням шлюзів безпеки.**

Summary: **The task of development and implementation of the network traffic security system is considered. The system based on the inter-LAN tunnels creating using security gateways**.

Ключевые слова: **Системы защиты межсетевого трафика, шлюз безопасности, удаленное управление.**

Введение

Одной из важнейших проблем в организации эффективной системы безопасности компании является определение разделения прав доступа к данным компании. Инструменты, которые позволяют реализовывать такие решения (брандмауэры, шлюзы безопасности), должны интегрироваться непосредственно в корпоративную сеть, используемую компанией, а также в ее отдельные компоненты.

Процесс функционирования корпоративной сети сопровождается циркуляцией потоков информации в локальных или глобальных сетях. Сети, на основе которых строятся современные информационные технологии компаний и корпораций, должны быть достаточно гибкими для того, чтобы обеспечить необходимый доступ к ресурсам или данным и в то же время быть достаточно защищенными для предотвращения нежелательного проникновения в корпоративную сеть. Эта проблема становится более сложной, если компания вынуждена взаимодействовать с общедоступными сетями, такими как Интернет. Когда новые сети и домены становятся доступны со стороны Интернета, добавляются новые серверы или выпускаются новые продукты перед компанией встает проблема их безопасной интеграции и обеспечения сотрудникам компании доступа к ним.

Чтобы построить систему безопасности компания должна в первую очередь разработать политику контроля доступа для внутренних и внешних сетей и сетевых ресурсов. В большинстве компаний считают, что их внутренним сетям (например, локальным сетям внутри здания) можно доверять. При этом считают, что сети вне организации – внешние и им доверять нельзя. Поэтому для изоляции внутренней сети от внешней используются брандмауэры и шлюзы безопасности. Однако, внутренние сети также представляют определенную опасность и должны обеспечивать некоторый уровень защиты, хотя политика безопасности по отношению к внутренним сетям может сильно отличаться от политики безопасности по отношению к внешним сетям, так как в большинстве компаний поток данных внутри рабочей группы обрабатывается по-иному, чем поток данных между рабочими группами.

I Брандмауэры и шлюзы безопасности

Для обеспечения безопасности внутренних и внешних сетей и сетевых ресурсов компании существует множество средств. Одними из основных компонентов таких средств являются брандмауэры и шлюзы безопасности.

Брандмауэром называют систему (маршрутизатор или сервер), используемую для реализации правил контроля доступа к данным внутри организации или между организациями. Брандмауэр позволяет разрешать или запрещать проходящие через него потоки данных. Для того, чтобы поток данных из одной локальной сети в другую или с одной рабочей станции на другую был пропущен брандмауэром, он должен соответствовать правилам безопасности, определяемым политикой безопасности организации.

Шлюзом безопасности называют систему (маршрутизатор или рабочую станцию), обеспечивающую защищенную передачу данных через внешние каналы связи и сети. Шлюз безопасности позволяет защищать потоки данных, проходящие через него, между локальными сетями или между локальной сетью и удаленным пользователем. Безопасную передачу данных между двумя системами через внешнюю (небезопасную сеть) обеспечивает туннель безопасности.

II Туннель безопасности

Процесс передачи данных через туннель предполагает использование правил безопасности, принятых в системах, между которыми эти данные передаются. Эти правила (также называемые мета-характеристиками) включают в себя адреса соединяющихся сторон, методы форматирования (в соответствии с которыми информация будет помещаться в блоки данных другого протокола), криптографические алгоритмы и параметры этих алгоритмов (ключи). Данные, проходящие через шлюз безопасности, форматируются в соответствии с установленной политикой безопасности.

Настройка политики безопасности для шлюза обеспечивается настройкой таблиц туннелирования и таблиц маршрутизации (для шлюза безопасности) или таблиц трансляции сетевых адресов (на хосте удаленного пользователя). Таблицы туннелирования содержат адреса шлюзов безопасности (или хостов удаленных пользователей), между которыми создается защищенный туннель, контекст безопасности и тип форматирования потока данных. Таблицы маршрутизации (или трансляции сетевых адресов) содержат данные, необходимые для скрытия сетевых адресов хостов, работающих через шлюз безопасности, и обеспечения их прохождения между шлюзами или хостами во внешних сетях.

Существует три случая организации туннелей безопасности.

Случай 1. На рис. 1 показан вариант соединения двух шлюзов безопасности. В этом случае туннель безопасности организуется между двумя шлюзами. При этом каждый шлюз ставится на выходе локальной сети и обеспечивает защиту межсетевого потока данных.

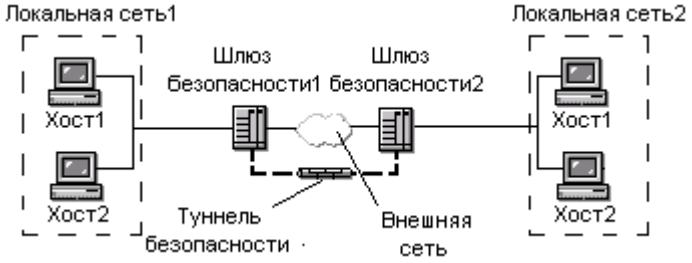

Рисунок 1 – Соединение двух шлюзов безопасности

Случай 2. На рис. 2 показан вариант соединения шлюза безопасности и хоста удаленного пользователя. В этом случае туннель безопасности организуется между шлюзом и агентом безопасности, установленном на хосте удаленного пользователя. При этом удаленный пользователь имеет доступ к данным и ресурсам локальной сети через шлюз безопасности, установленный на ее выходе.

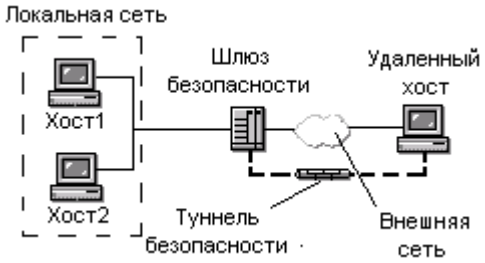

Рисунок 2 – Соединение шлюза безопасности и хоста удаленного пользователя

Случай 3. На рис. 3 показан вариант соединения двух хостов удаленных пользователей. В этом случае туннель безопасности организуется между агентами безопасности, установленными на хостах. При этом

обеспечивается сквозная защита передаваемых данных между хостами удаленных пользователей.

Рисунок 3 – Соединение двух хостов удаленных пользователей

Во всех случаях обеспечивается инкапсуляция потока данных в туннеле безопасности и защита его в соответствии с контекстом безопасности (ключом шифрования). Инкапсуляция потока данных включает защиту от повторов передаваемых в туннель инкапсулированных блоков данных. Во втором и третьем случаях обеспечивается также защищенное установление и разрыв соединения. В первом случае защищенное соединение между шлюзами безопасности осуществляется только при установке туннелей безопасности.

III Шлюз безопасности “криптомаршрутизатор”

Шлюз безопасности “криптомаршрутизатор” разработан для создания туннелей безопасности между локальными сетями или между локальной сетью и хостом удаленного пользователя. Для защиты потока данных между двумя локальными сетями используются два шлюза безопасности, устанавливаемые на выходе каждой из сетей. Вариант такого подключения приведен на рис 4. Выходной поток данных локальной сети обрабатывается, инкапсулируется и маршрутизируется на второй шлюз безопасности в соответствии с установленными правилами безопасности и ограничения доступа. Шлюз безопасности удаленной сети обрабатывает входной поток данных с первого шлюза – открывает данные и передает их в свою локальную сеть. При включении шлюзов и загрузке туннелей безопасности осуществляется их взаимная идентификация и установка контекстов безопасности и форматирования потока данных.

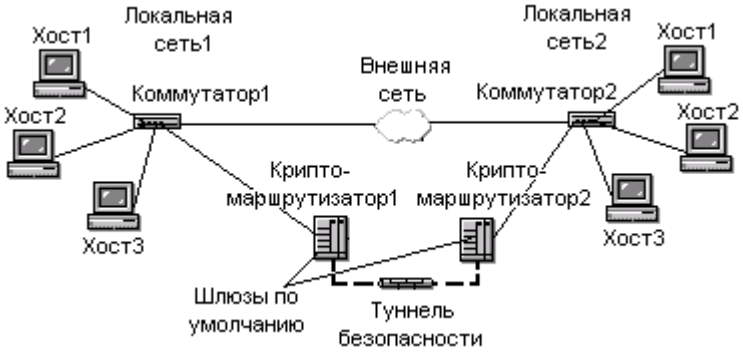

Рисунок 4 – Соединение двух “криптомаршрутизаторов”

Удаленный пользователь может подключиться к локальной сети через шлюз безопасности с помощью программного агента, установленного на его хосте. Вариант такого подключения приведен на рис 5. При первом установлении соединения осуществляется аутентификация удаленного пользователя и создание контекста безопасности соединения шлюза с хостом.

Рисунок 5 – Соединение “криптомаршрутизатора” и удаленного пользователя

Шлюз безопасности “криптомаршрутизатор” реализован в виде дополнительной рабочей станции, устанавливаемой на выходе локальной сети. В качестве программной платформы шлюза используется операционная система Windows 2000 Professional. В реализации шлюза используется часть встроенных сетевых компонентов (в частности программный маршрутизатор) операционной системы. Шлюз безопасности построен на основе разработанного сетевого драйвера, встраиваемого в подсистему сетевых драйверов NDIS. Шлюз выполняет обработку IP-трафика и совместим с локальными сетями (в данной версии только стандарта IEEE 802.3).

Создание защищенного туннеля между шлюзами безопасности или шлюзом безопасности и агентом удаленного пользователя обеспечивается за счет шифрования, имитозащиты и инкапсуляции пакетов с использованием сеансовых ключей. В процессе инкапсуляции пакетов исходный IP-заголовок заменяется на новый, обеспечивая передачу инкапсулированного пакета на шлюз безопасности или хост удаленного пользователя. Контекст туннеля безопасности содержит счетчик пакетов, обеспечивающий защиту от повторов инкапсулированных пакетов. Кроме того, шлюз безопасности может автоматически отключать “поврежденные” туннели.

Криптографическая защита в туннеле безопасности осуществляется с использованием поточного шифрования каждого пакета и вычисления имитовставки на сеансовых ключах. В качестве базовых используются алгоритмы ГОСТ 28147-89 и Х-ГОСТ. Сеансовые ключи защищаются с использованием алгоритмов Х-ГОСТ, причем каждый пакет защищается на отдельном сеансовом ключе. Криптографический контекст туннеля содержит транспортный ключ, на котором передаются заголовки инкапсулированных пакетов, включая и сеансовый ключ.

Управление шлюзом безопасности “криптомаршрутизатор” может осуществляться локально или удаленно. При удаленном управлении шлюз безопасности функционирует в автоматическом режиме. Администратор безопасности сети выполняет настройку шлюза безопасности через своего программного агента установленного на шлюзе. При подключении удаленного администратора к шлюзу безопасности вначале выполняется их взаимная идентификация. Удаленный администратор может управлять работой шлюза, настраивая правила безопасности (таблицы туннелирования и маршрутизации) и форматирования потоков данных, проходящих через шлюз. Установка транспортных ключей в криптографический контекст туннеля безопасности осуществляется удаленно. Для защиты данных управления используются многоэтапные состоятельные протоколы, базирующиеся на ГОСТ 28147-89, ГОСТ 34310-95, ГОСТ 34311-95, а также X9.42.

Заключение

Разработанный шлюз безопасности применяется для защиты потока данных между локальными сетями, обеспечивая управление доступом к ресурсам локальной сети из других сетей или с хостов удаленных пользователей, в соответствии с устанавливаемыми правилами безопасности. Однако реализованный проект требует доработки. Среди основных – реализация поддержки дополнительных протоколов канального уровня, используемых в современных локальных сетях (так как данная версия поддерживает только Ethernet). Кроме того, необходима реализация возможности сбора статистической информации и информации о состоянии туннелей со шлюзов безопасности, а также возможности быстрого восстановления всей сети шлюзов безопасности в случае сбоя.

УДК 681.3.06:519.248.681

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОКАЗАТЕЛЕЙ СЛОЖНОСТИ И СТОЙКОСТИ ЦИФРОВЫХ ПОДПИСЕЙ ECSS И ECDSA

Станислав Збитнев, Игорь Коновалов*, Даниил Меалковский**, Андрей Поляков
*Харьковский Национальный Университет Радиоэлектроники,*АТ “ИИТ”, **ДСТСЗИ СБУ*

Анотація: **Здійснюється порівняльний аналіз RSA-подібних систем з цифровими підписами на еліптичній кривій у скінченних полях. Аналізуються основні алгоритми цифрових підписів побудованих на основі еліптичної кривої (ECDSA і ECSS). Даються рекомендації з використання цифрових підписів.**

Summary: **Produce comparative analysis RSA – similar systems with digital signatures on elliptic curves in finite fields. Analyzed main algorithms of digital signatures on elliptic curves (ECDSA and ECSS). Given recommendations on using the digital signatures.**