УДК 004.057.4

Реализация протокола безопасного обмена ключами для VPN.

Цебровский А. Д., Магда И. А. федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Научный руководитель – Фильченков А.А., к.ф.-м.н., доцент университета ИТМО

Введение

Сегодня одной из самых актуальных проблем в сфере информационно-вычислительных систем является защита информации в интернете. Действительно, мало кто мыслит свою жизнь без электронной глобальной сети. Люди ведут различные финансовые операции в сети Интернет, заказывают товары, услуги, пользуются кредитными карточками, проводят платежи, разговаривают и переписываются, совершают много других действий, требующих обеспечения конфиденциальности и защиты.

Защита данных волнует все больше людей. Тенденции не только не радуют, они просто ужасают — следить за нами начинают практически все гаджеты. Для защиты можно использовать SSH-туннели и SOCKS'ифицировать через них нужный трафик, можно везде, где получится, использовать HTTPS, устанавливая для этого плагины. Однако наиболее подходящей для этого технологией был, есть и еще долгое время будет VPN. Наиболее действенными методами защиты от несанкционированного доступа по компьютерным сетям являются виртуальные частные сети (VPN – Virtual Private Network). Виртуальные частные сети обеспечивают автоматическую защиту целостности и конфиденциальности сообщений, передаваемых через сети общего пользования.

Существует достаточно большое количество разных VPN реализаций – каждый со своими плюсами и минусами. Существующие решения имеют, могут даже не иметь реализации под операционную систему Linux, для использования на производстве, что является огромным минусом. Также с точки зрения разработчика программного обеспечения данные реализации слишком сложны и имеют посредственное качество кода. Широкие возможности данных решений порождают недостаток – по сравнению с нашей реализацией первичная настройка может оказаться сложнее. В работе авторов эта проблема нивелируется за счет использования стандартных конфигураций и способности сервера автоматически передавать существенную часть параметров подключения клиентам.

При реализации использовалась библиотеке с открытым исходным кодом SoftEther VPN. SoftEther VPN – надежное VPN решение, использующее стойкое шифрование AES 256-bit и RSA 4096-bit. Наша реализация имеет реализацию готовую к использованию на производстве под операционную систему Linux, также хорошо спроектированную архитектуру, гибкость и качество кода, обеспечивающее легкую поддержку и добавление нового функционала.

Цель работы

Целью данной работы является реализация протокола безопасного обмена ключами, для защиты от несанкционированного доступа по компьютерным сетям.

Результаты

В данной работе реализованы средства защиты от несанкционированного доступа по компьютерным сетям, с реализацией под различные операционные системы. Программа была написана на языке C++. Дальнейшие исследования могут быть направлены на разработку дополнительных функциональности для обеспечения информационной безопасности более высокого уровня, с учетом различных характерных рисков.

Список литературы

1. Design and implementation of SoftEther VPN [Электронный ресурс] // URL https://www.softether.org/4-docs/9-research/Design_and_Implementation_of_SoftEther_VPN
2. SoftEther VPN manual [Электронный ресурс] // URL https://www.softether.org/4-docs/1-manual
3. An illustrated guide to IPsec [Электронный ресурс] // URL http://www.unixwiz.net/techtips/iguide-ipsec.html
4. IKEv2 packet exchange and protocol level debugging [Электронный ресурс] // URL https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/115936-understanding-ikev2-packet-exch-debug.html#topic1
5. IPSec guide [Электронный ресурс] // URL http://www.tech-invite.com/fo-ipsec/pdf/tinv-ipsec-ikev2-formats.pdf
6. Internet Key Exchange Protocol Version 2 (IKEv2) [Электронный ресурс] // URL https://tools.ietf.org/html/rfc7296