УДК 330.4:330.46

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОЦЕССА ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Касьян А.С.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Бойправ О.В. – канд. техн. наук

Современные информационные системы (ИС) не могут работать изолированно. Взаимодействие между ИС – важная часть жизненного цикла каждой из них. Одним из требований, предъявляемым к такому взаимодействию, – его безопасность. Безопасность может быть реализована на уровне межсетевых коммуникаций или на уровне сервисов и приложений. Первое является более фундаментальным аспектом защищённого взаимодействия и поэтому всё внимание в рамках данной работы будет уделено именно ему.

Большинство угроз, реализуемых на уровне сетевого взаимодействия ИС, связаны с перехватом сетевого трафика и просмотром его содержимого или подменой доверенного участника взаимодействия. В результате чего нарушаются такие аспекты информационной безопасности (ИБ), как конфиденциальность и подлинность (неразрывно связано с целостностью) информации. В рамках противодействия нарушению этих аспектов ИБ, были разработаны специализированные протоколы безопасности сетевого взаимодействия.

Основными протоколами обеспечения безопасности процесса взаимодействия информационных систем являются SSH, IPsec и SSL/TLS. Сравнение данных протоколов приведено в таблице 1.

Таблица 1 – Сравнение протоколов обеспечения безопасности процесса взаимодействия информационных систем

	SSH	IPsec	SSL/TLS
Основное назначение	Обеспечение защищённого удалённого управления операционной системой и защищённого туннелирования TCP-соединений	Обеспечение защиты данных, передаваемых по протоколу IP	Обеспечение защиты данных, передаваемых протоколами уровня приложений модели OSI
Конфиденциальность	Симметричные алгоритмы шифрования	Симметричные алгоритмы шифрования	Симметричные алгоритмы шифрования
Аутентификация	Сервер – по ключу. Клиент – по паролю либо по ключу	По общему ключу либо по сертификатам	В основном по сертификатам SSL
Масштабируемость	Нет	Да, для VPN	Да
Поддержка VPN	В виде туннелирования TCP-соединений	Да	Да
Поддержка протоколов с клиент-серверной архитектурой	В виде туннелирования TCP-соединений	Прозрачен для уровня приложений	Да

Из данных таблицы можно заключить, что каждый из протоколов обладает своими преимуществами и недостатками и подходит для реализации вполне конкретных задач. Механизмы безопасности всех рассмотренных протоколов имеют схожие черты. Однако более продуманным и универсальным протоколом из всех является именно SSL/TLS. С помощью него можно организовывать как легко масштабируемые VPN туннели, так и взаимодействие протоколов клиент-серверной архитектуры, а аутентификация по сертификату представляется наиболее надёжной на сегодняшний день.

Стоит понимать, что SSL/TLS достаточно сложный протокол и обладает большим количеством параметров. Правильная настройка этих параметров позволит защитить ИС от атак, направленных на нарушение конфиденциальности и подлинности (целостности) информации.

Список использованных источников:

1. Bulletproof SSL and TLS / Ivan Ristic // Feisty Duck Limited, 2014. – P. 23-63, 247-269.
2. Компьютерные сети / Э. Танненбаум, Д. Уэзеролл – СПб.: Питер, 2012. – С. 854-871, 896-910.
3. SSL, SSH and IPsec [Электронный ресурс]. – Режим доступа: https://www.cs.swarthmore.edu/~mgagne1/teaching/2016_17/cs91/SSL_IPsec.pdf