Методы обеспечения безопасности информационных систем, функционирующих в сети Интернет

И.В. Александров[a], Н.А. Богачев[a], И.А. Парфёнов[a]

[a] *Московский Технологический Университет (МИРЭА), 119454, проспект Вернадского, 78, Москва, Россия*

Аннотация

В настоящее время огромное значение приобретает обеспечение безопасности удаленной работы в информационных системах. Встает вопрос не только об осуществлении защищенного соединения, но и создании различного рода ограничений на средства управления распределенных систем. Это задает новый уровень сложности как для разработки, так и для дальнейшей эксплуатации ИС. Поиск необходимого баланса между сохранностью и эффективной обработкой данных является ключевым аспектом в усовершенствовании существующей или разработке новой ИС.

В качестве возможного решения существует способ составления свода правил, по которым должны регулироваться действия и возможные варианты использования функционала ИС, к которой они применяются. Выстраивание такой стратегии поможет облегчить формализацию создания информационной системы.

Ключевые слова: безопасность функционирования; интернет; веб-технологии; информационная безопасность

1. Введение

В настоящее время огромное значение приобретает обеспечение безопасности работы в рамках информационных систем (ИС), функционирующих поверх Интернет. Встает вопрос не только об осуществлении защищенного соединения, но и создание различного рода ограничений на средства управления географически распределенных систем. Это задает новый уровень сложности как для разработки ИС, так и для дальнейшей эксплуатации и поддержки.

В области информационных технологий, прочно вошедших в сферу деятельности многих предприятий, решение этой проблемы критически важно для предоставления сервиса конечному пользователю. Достижение приемлемого уровня безопасности накладывает дополнительные рамки на задачи в контексте их выполнения. Поиск необходимого баланса между сохранностью данных и эффективной их обработкой является ключевым аспектом в усовершенствовании уже существующей или разработке новой ИС.

2. VPN

Одним из возможных вариантов создания условий для передачи информации внутри распределенной информационной системы (РИС) является использование технологии VPN (Virtual Private Network - виртуальная частная сеть). VPN позволяет построить сеть поверх общедоступных каналов связи.

Построение виртуальной частной сети можно также можно произвести различными способами. К примеру в большинстве операционных систем UNIX-семейства довольно давно используется сочетание ssh (Secure Shell) и ppp (Point-to-Point Protocol). Однако в силу малой распространенности, больший интерес представляют стандартные решения. Они не привязаны к конкретной платформе, в чем и проявляется дополнительное преимущество. Наиболее известные из них:

- PPTP (Point-to-Point Tunneling Protocol), разработанный совместно Microsoft, 3Com и Ascend Communications. Этот протокол стал достаточно популярен благодаря его включению в операционные системы фирмы Microsoft.
- L2F (Layer-2 Forwarding) — разработка фирмы Cisco.
- L2TP (Layer-2 Tunneling Protocol) — разрабатываемый официальный стандарт Интернет.
- SKIP (Simple Key-management for Internet Protocols) — разработка фирмы Sun.
- IPsec (Internet Protocol Security) — официальный стандарт Интернет.

Стандартом для Интернета является набор протоколов IPsec. Согласно стандарту все устройства, работающие с новым IP- протоколом IPv6, обязаны поддерживать IPsec.

Виртуальная частная сеть строится на основе использования криптографических протоколов. Использование криптографии позволяет достичь нескольких целей, одновременно или по отдельности:

- Скрыть информацию, передаваемую по сети.
- Убедиться, что информация послана именно тем, кто обозначен отправителем в пакете.
- Обеспечить неизменность информации в процессе передачи.
- Предотвратить повторное использование информации

В режиме построения VPN (режиме туннелирования) IPsec обеспечивает безопасность связи в Интернете «упаковкой» IP-пакета в новый

IP-пакет с применением к нему различных преобразований — шифрации и электронных подписей. Сетевая инфраструктура предприятия может быть подготовлена к использованию VPN как с помощью программного, так и с помощью аппаратного обеспечения. Выбор способа зависит прежде всего от конкретной ситуации и характеристик информационной системы.

3. Брэндмауэр

Другим возможным вариантом обеспечения защиты информации является фильтрация потока данных на основе адреса отправителя или получател данных. Такой подход обеспечивает брандмауэр (или межсетевой экран).

Межсетевой экран представляет собой однин из компонентов сети, контролирущий прохождение пакетов. Это часть программного или аппаратно-прораммного обеспечения, позволяющая обеспечить фильтрацию на основе заданной политики безопасности. Применение правильно настроенного брэндмауэра в соответствии с политикой безопасности гарантирует ограниченный доступ к данным. Дополнительную гибкость к построению защиты предоставляет большое число настраиваемых параметров.

Фильтрация контролируемого трафика происходит без инспекии состояния, что означает просматривание каждого пакета как независимого объекта. Реализация механизма работы происходит на основе правил, состаящих из:

- условия, которому должен соответствовать текущий обрабатываемый пакет;
- действия, которому подвергнется пакет: будет пропущен или заблокирован (allow или deny соответственно)

Межсетевой экран анализирует поток данных, основываясь на IP-адресах узлов, обменивающихся данными, а также номере их портов и используемом протоколе. Если пакет удовлетворяет условиям правила, то выполняется указанное в правиле действие.

Брандмауэр — неотъемлемая часть любой конфигурации сети или отдельно взятых серверов. Он обеспечивает дополнительный уровень защиты, даже если используемое ПО уже предусматривает свои внутренние меры. Те части ИС, которые могут быть потенциально уязвимы для атаки, могут быть закрыты, что позволит еще больше укрепить безопасность.

В большинстве операционных систем уже встроена воможность настройки контроля трафика. В семействе операционных систем UNIX такая возможность реализуется при помощи, например, iptables или ipfw. Семейство ОС Windows оснащенно приложением «Брэндмауэр Windows». Однако существует большое множество реализаций межсетевых экранов и от сторонних разработчиков, также позволяющих надежно защитить сеть от нежелательного доступа.

4. SSL

SSL — это сокращение от Secure Socket Layer — это стандартная интернет технология безопасности, которая используется, чтобы обеспечить зашифрованное соединение между веб-сервером (сайтом) и браузером. SSL сертификат позволяет нам использовать https протокол. Это безопасное соединение, которое гарантирует, что информация которая передается от вашего браузера на сервер остается приватной; то есть защищенной от хакеров или любого, кто хочет украсть информацию. Один из самых распространенных примеров использования SSL — это защита клиента во время онлайн транзакции (покупки товара, оплаты).

Для того, чтобы получить SSL сертификат самое первое, что нужно сделать, это сформировать специальный запрос на выпуск сертификата, так называемый Certificate Signing Request. При формировании этого запроса вам будет задан ряд вопросов, для уточнения деталей о вашем домене и вашей компании. После завершения ваш веб сервер создаст 2 типа криптографических ключей — приватный ключ и публичный ключ.

В сертификате хранится следующая информация:

- полное (уникальное) имя владельца сертификата
- открытый ключ владельца
- дата выдачи SSL сертификата
- дата окончания сертификата
- полное (уникальное) имя центра сертификации
- цифровая подпись издателя

5. Заключение

Была проведена работа по изучению основных способов повышения уровня безопасности систем, функционирующих в сети Интернет. Как по отдельности, так и вместе рассматриваемые методы позволяют выстроить такую стратегию функционирования, которая поможет облегчить решение множественных проблем разработки, администрирования и поддержки в эксплуатации информационных систем в дальнейшем.

Литература

[1] Cheswick, W., Bellovin, S., Rubin, A. Firewalls and Internet Security: Repelling the Wily Hacker. 2nd ed. / Cheswick W., Bellovin S., Rubin A. — New York City: Addison Wesley Professional, 2003. — 464 p.

[2] FreeBSD Handbook [Electronic resource]. — Access mode: http://www.freebsd.org/doc/handbook/ (14.01.2017.)

[3] IETF Policy Framework (policy) Working Group [Electronic resource]. — Access mode: http://www.ietf.org/html.charters/policy-charter.html (16.01.2015)