Терминатор TLS

Назначение шаблона

Шаблон предназначен для безопасной передачи данных между системой и удаленным сервером по протоколу TLS с использованием изолированного доверенного компонента.

Типовые цели безопасности

Типовые цели безопасности при применении шаблона включают:

- обеспечение конфиденциальности, целостности и аутентичности данных при взаимодействии с удаленным сервером;
- защита ключевой информации (закрытых ключей шифрования, сертификатов) от раскрытия.

ЦБ могут уточняться в зависимости от области применения шаблона, к примеру, целью может быть обеспечение целостности и аутентичности данных бинарных образов программных модулей при выполнении процедуры обновления системы.

Предположения безопасности

Предположения безопасности включают:

- отсутствие известных уязвимостей в криптографических алгоритмах, используемых в криптонаборах TLS;
- отсутствие известных уязвимостей в алгоритмах и технических средствах генерации криптографических ключей и сертификатов;
- проведение должных испытаний программного обеспечения, реализующего алгоритмы и протокол TLS, и иные мероприятия по обеспечению соответствия его поведения спецификациям.

Предположения и условия, при которых шаблон не может быть применен:

- неэффективность организационных и технических методов обеспечения доверия к реализации протокола TLS в изолированном компоненте;
- неэффективность организационных и технических методов обеспечения доверия к взаимодействию защищаемого ресурса и изолированного компонента, реализующего TLS;
- наличие множественных уязвимостей в реализации протокола TLS и в реализации протоколов, на основе которых он работает.

Описание решения

Шаблон основан на реализации другого шаблона проектирования «Разделение потоков данных на уровне драйвера ресурсов» и реализует раздельный доступ к сетевому интерфейсу и к двум разделам файлового хранилища. Один из разделов файлового хранилища предназначен для ключей и других секретов шифрования, второй – для прочих данных, обмен которыми происходит по TLS.

Это позволяет реализовать следующие требования:

- изоляция и раздельное хранение доверенных данных (сертификатов и ключей шифрования) и недоверенных (данные, полученные по сети);
- гарантированное подключение компонента, реализующего транспортную логику, только к тому серверу, с которым производилась аутентификация;
- минимизация возможностей компрометации ключей и секретов шифрования посредством эксплуатации уязвимостей.

Элементы системы, реализующей шаблон:

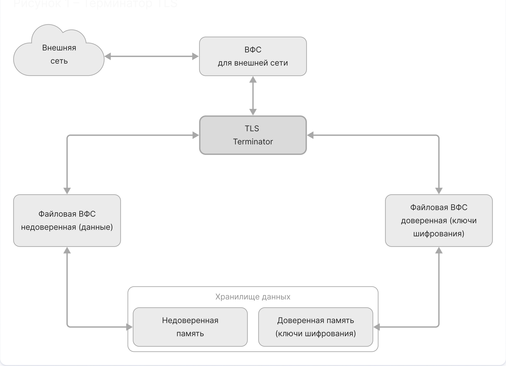
- элемент, реализующий обмен данными с внешней сетью (к примеру, реализующий ВФС для внешней сети);
- элемент, реализующий обмен данными с недоверенным хранилищем данных (файловая ВФС);
- элемент, реализующий обмен данными с доверенным хранилищем данных (файловая ВФС);
- файловое хранилище для общих данных системы (недоверенное);
- файловое хранилище для секретов шифрования (доверенное);
- элемент, выполняющий терминацию TLS (инкапсуляцию в протокол TLS).

Терминатор TLS (точнее, тот его элемент, который выполняет непосредственно терминацию TLS) является монитором безопасности пересылок между приложением и внешней сетью. Для снижения сложности рекомендуется реализовать этот элемент из двух независимых компонентов, один из которых отвечает за установку соединения, а другой реализует передачу данных.

С точки зрения приложения терминатор TLS выглядит как обычный сетевой интерфейс, обращение к которому осуществляется с помощью стандартных запросов (к примеру, POSIX-совместимых системных вызовов – connect, accept и т.п.).

Взаимодействие элементов шаблона представлено на рисунке 1.

Рисунок 1 - Терминатор TLS



Требования к технологии разработки элементов системы

Элемент, реализующий терминацию TLS, должен реализовать концепцию монитора безопасности пересылок, обеспечивая полное перекрытие потоков данных в/из сети.

Поскольку шаблон реализуется на основе шаблона «разделение потоков данных на уровне драйверов устройств», применяются требования к технологии, определенные для базового шаблона.

Необходимо реализовать подходы к обеспечению корректности реализации протокола TLS, в первую очередь методические и кооперационные подходы, обеспечивающие безопасность и корректность работы программного кода, реализующего установление соединения и обмен данными по протоколу TLS.

Ограничения на применение шаблона

Поскольку шаблон реализуется на основе шаблона «разделение потоков данных на уровне драйверов устройств», применяются ограничения, определенные для базового шаблона.

Допустимые модификации шаблона

Допустимость модификаций шаблона должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.