Разделение потоков данных на уровне драйвера ресурсов

Назначение шаблона

Шаблон предназначен для разделения потоков данных для ограничения доступа к ресурсам на уровне драйвера ресурсов с целью обеспечения конфиденциальности, целостности и взаимного невлияния потоков данных. Примером применения шаблона является уменьшение поверхности атаки на виртуальную файловую систему (ВФС), за счет разделения одной ВФС на несколько: например, отдельно для работы с внешней сетью и отдельно для работы с внутренней сетью и блочным устройством.

Типовые цели безопасности

Типовые цели безопасности при применении шаблона включают:

- конфиденциальность данных, обрабатываемых в системе;
- целостность данных, обрабатываемых в системе;
- обеспечение режима доступа к специальным ресурсам (к примеру, единоразовый доступ к криптографическим ключам в процессе загрузки системы, однонаправленный доступ к конфигурационным данным и т.п.).

Предположения безопасности

Предположения безопасности включают:

- корректность работы драйверов и системного ПО, лежащего в основе реализации драйверов разделяемых ресурсов;
- отсутствие или ничтожность скрытых каналов доступа и управления разделяемыми ресурсами на уровне нижележащих драйверов, системного ПО, кода прошивок устройств и оборудования.

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

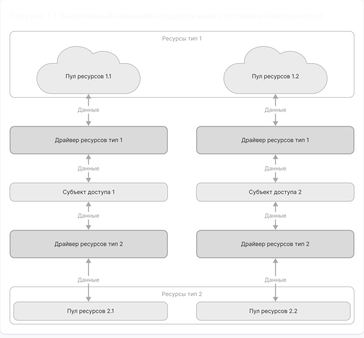
- альтернативный канал доступа к ресурсу, который позволяет обходить установленные на основе реализации шаблона ограничения доступа.

Описание решения

Элементы системы, реализующей шаблон:

- субъекты доступа к ресурсам;
- драйверы доступа к ресурсам различных типов, количество элементов определяется числом ресурсов каждого типа, требующих различных политики и/или режима доступа;
- пул ресурсов каждого типа согласно количеству элементов-драйверов ресурсов для обеспечения разделения ресурсов, пул ресурсов определяется согласно возможностям адресации ресурсов (диапазон адресов в памяти, выделенный канал связи, адресуемый как целое, и т.п.).

Взаимодействие элементов шаблона представлено на рисунке 1.



В качестве поясняющего примера рассмотрим виртуальные файловые системы (ВФС), работающие с сетью и с блочными устройствами, которые должны быть разделены и помещены в разные домены безопасности.

Сущности (субъекты, процессы), обрабатывающие данные из сетей, приходящие на разные контроллеры или адаптеры, должны использовать разные ВФС.

Компрометация сетевой ВФС не должна приводить к компрометации сущностей, с которыми она взаимодействует.

Рассмотрим угрозы безопасности на примере приложения с одной ВФС, которая обеспечивает сразу несколько типов взаимодействия:

- недоверенный компонент обменивается данными с публичной и локальной сетью;
- полученная из публичной и локальной сети информация записывается в хранилище данных на жестком диске;
- доверенный компонент обменивается высокоцелостными данными с жестким диском;
- недоверенный компонент обменивается данными с жестким диском и уведомляет об этом доверенный компонент.

Для выполнения первого требования нужно реализовать подход разделения одной ВФС на несколько, а точнее на 4 (ВФС для работы с публичной сетью для обеих сущностей, ВФС для работы с локальной сетью для обеих сущностей).

Чтение и запись данных из хранилища данных осуществляют два компонента:

1. Доверенная сущность;
2. Недоверенная сущность.

Для каждого из них требуется отдельная ВФС.

Второе требование достигается автоматически при выполнении первого требования, поскольку разделение сети на несколько подсетей в данном примере не рассматривается.

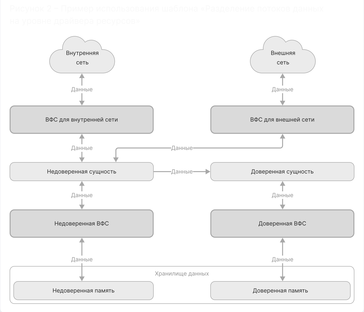
Далее, для выполнения третьего требования должны быть реализованы независимые хранилища информации.

Для этого:

- к драйверу блочного устройства необходимо подключить драйвер раздела;
- в драйвере раздела прописать два выделенных диапазона адресуемых блоков, один для субъекта «Доверенная сущность», второй для «Недоверенная сущность»;
- обеспечить взаимодействие сущности только с предопределенным для нее выделенным диапазоном адресуемых блоков посредством задания ограничения (политики безопасности) для драйвера раздела.

Для выполнения последнего требования необходимо убедиться, что доверенные компоненты, взаимодействующие с файловым хранилищем, не обращаются напрямую к сетевому драйверу, взаимодействующему с публичной сетью.

Пример показан на рисунке 2.



Требования к технологии разработки элементов системы

Необходимо реализовать разделение на разных уровнях драйверов: драйвер ВФС или драйвер раздела, чем ниже уровень, на котором проводится разделение, тем проще осуществить доказательство невлияния потоков данных.

Необходимо реализовать разделение пула ресурсов для привязки к ним раздельных драйверов доступа, что должно быть обеспечено технической возможностью адресации ресурсов определенного типа и невозможностью драйвера адресовать ресурсы того же типа вне заданного для него пула адресов.

Необходимо реализовать подходы к обеспечению корректности работы драйверов ресурсов и драйверов ниже этого уровня (если они доступны для контроля), в первую очередь методические и кооперационные подходы, обеспечивающие безопасность и корректность работы драйверов.

Ограничения на применение шаблона

Ограничения на применение шаблона определяются ограничениями на производительность и требованиями доступности ресурсов, доступ к которым реализуется с использованием шаблона.

Допустимые модификации шаблона

Допустимые модификации шаблона определяются через количество типов ресурсов и политики разграничения доступа к этим ресурсам.

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