Раздельное принятие и применение решений о безопасности

Назначение шаблона

Шаблон «Раздельное принятие и применение решений о безопасности» предназначен для реализации активного механизма контроля доступа и фильтрации потоков данных/потоков управления на основе заданных правил и политик безопасности. Шаблон предполагает разделение механизмов принятия решения о возможности доступа или разрешении потока и применения этого решения к потокам данных, потокам управления и выполняемым в системе операциям. Это в конечном счете позволяет улучшить гибкость работы механизма контроля доступа и/или фильтрации потоков данных/потоков управления в системе и оптимизировать доказательство корректности его работы.

Типовые цели безопасности

Типовые цели безопасности при применении шаблона включают:

- обеспечение конфиденциальности и/или целостности данных или активов путем реализации контроля доступа к этим данными и активам;
- обеспечение контроля выполнения операций в системе в соответствии с заданными правилами и политиками безопасности;
- обеспечение контроля и фильтрации сообщений (таких, как пакеты данных, команды управления, системные вызовы, служебные сигналы протоколов взаимодействия), передаваемых между сущностями в системе (сущностями могут быть процессы в ОС, вычислительные системы в компьютерной сети, виртуальные машины в среде виртуализации и пр.), в соответствии с заданными правилами и политиками безопасности.

Предположения безопасности

Предположения безопасности включают:

- известный и прозрачный формат данных и протокол доступа к данным или активам (выполнения операций в системе, обмена сообщениями);
- отсутствие скрытых каналов передачи данных / скрытых каналов управления, использование которых позволяет обходить реализуемый шаблоном монитор безопасности пересылок.

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

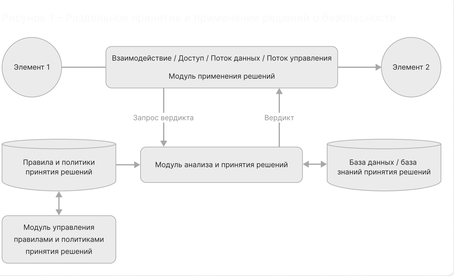
- данные и операции, которые требуется отслеживать и контролировать при помощи шаблона, подвергаются шифрованию, и нет возможности расшифровать их на уровне модуля анализа и принятия решений.

Описание решения

Элементы системы, реализующей шаблон:

- модуль анализа и принятия решений (decision point);
- модуль применения решения (enforcement point);
- правила и политики принятия решений;
- (опционально) база данных / база знаний, используемых и пополняемых алгоритмами принятия решений, которые реализуются модулем анализа и принятия решения (information point);
- (опционально) модуль управления правилами и политиками, в соответствии с которыми принимается решение о разрешении или блокировке потока данных или потока управления (операции) (authorization point).

Взаимодействие элементов монитора представлено на рисунке 1.



Требования к технологии разработки элементов системы

Модуль анализа и принятия решений должен реализовать анализ событий по факту их регистрации (runtime, проспективный анализ) или отложенный анализ на основе доступной информации о выполнении доступа к данным и активам, об обмене сообщениями, о выполняемых операциях в системе.

Модуль применения решений должен реализовать концепцию монитора безопасности пересылок, обеспечивая полное перекрытие потоков контролируемых данных, каналов выполнения операций и способов выполнения доступа к данным и активам. Невыполнение этого требования приводит к возникновению способов обхода контроля доступа к данным и контроля выполнения операций.

Технология применения решений, ограничивающая доступ, передачу команд управления для выполнения операций и передачу данных, должна быть реализована прозрачным для этих процессов образом так, чтобы минимизировать влияние на временные характеристики работы системы, показатели ее производительности, надежности и безопасности.

Ограничения на применение шаблона

Применение шаблона может быть ограничено в системах с требованиями к выполнению в реальном времени, а также в системах с повышенными требованиями к функциональной безопасности и надежности вследствие необходимости перехвата потоков данных и/или потоков управления и возможной блокировки этих потоков, что потенциально может повлиять на выполнение упомянутых требований.

Допустимые модификации шаблона

Допустимо использовать для реализации модуля принятия решений шаблон «Монитор», в котором:

- алгоритмы анализа предназначены для вычисления вердикта о разрешении или запрете доступа к данными или активам, разрешении или запрете выполнения операции или разрешении или запрете передачи данных;
- модуль реакции, который передает вычисленный вердикт модулю применения решения или совпадает с модулем применения решения (рисунок 2).

Допустимо использовать модификации, описанные для шаблона «Монитор», при условии выполнения требований к модулю принятия решений и указанных выше ограничений для настоящего шаблона.

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.