Выделенный обработчик для очистки данных

Назначение шаблона

Шаблон предназначен для проверки целостности и безопасности потока данных, поступающих на вход системы, которая позволяет снизить поверхность атаки на сложные элементы системы за счет вынесения функции проверки в специальный изолированный компонент.

Типовые цели безопасности

Типовые цели безопасности при применении шаблона включают:

- защита элементов системы от некорректных, плохо сформированных данных, способных нанести ущерб при злонамеренной эксплуатации уязвимостей этих элементов;
- очистка данных от конфиденциальной информации перед передачей их внешнему недоверенному агенту, в том числе перед размещением в сетях общего доступа.

Предположения безопасности

Предположения безопасности включают известный формат данных и известный протокол обмена данными.

Предположения и условия, при которых шаблон не может быть применен: данные, которые требуется контролировать, подвергаются шифрованию, и нет возможности расшифровать их на уровне компонента, реализующего проверку и обработку данных.

Описание решения

Крупные и сложные элементы системы (такие как базы данных, микросервисы и т.д.) обладают обширной поверхностью атаки, **в связи с чем усложняется задача обеспечения безопасности и проведения проверок для установления доверия**. Для уменьшения поверхности атаки следует заранее проводить проверку входных данных на их безопасность относительно этих элементов, в том числе, требуется проводить необходимую очистку этих данных от лексических и синтаксических конструкций, представляющих опасность в отношении потенциальных уязвимостей элементов системы. **Подобные проверку и очистку следует вынести в отдельный, небольшой, изолированный компонент, отвечающий следующим требованиям**:

- реализацию монитора безопасности пересылок (режим работы «в разрыв» - перехват всего входящего потока данных без возможности обхода компонента);
- получение на вход, проверку, очистку и передачу на выход потока данных с приемлемым уровнем задержки и потери;
- применение правил проверки и очистки данных на основе обновляемого набора правил.

Элементы системы, реализующей шаблон:

- источник данных;
- получатель данных;
- компонент, реализующий проверку и обработку данных перед передачей получателю.

Взаимодействие элементов шаблона представлено на рисунке 1.

Рисунок 1 – Выделенный обработчик для очистки данных

Требования к технологии разработки элементов системы

Необходимо исключить каналы передачи данных между источником и получателем данных, которые могут быть использованы для передачи необработанных данных. Гарантии отсутствия скрытых каналов или невозможности использования таких каналов элементами системы, реализующими шаблон, могут быть предоставлены на низком уровне относительно реализации шаблона.

Необходимо обеспечить аутентичность и целостность канала передачи данных между компонентом, реализующим очистку данных, и получателем данных для исключения подделки данных и атаки «человек посередине». Гарантии аутентичности и целостности канала передачи данных могут быть предоставлены на низком уровне относительно реализации шаблона.

Необходимо реализовать подходы к обеспечению корректности производимой обработки (очистки) данных, в первую очередь методические и кооперационные подходы, обеспечивающие безопасность и корректность работы программного кода компонента, реализующего проверку и обработку (очистку) данных.

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 обработки данных и возможного изменения данных, что потенциально может повлиять на выполнение упомянутых требований.

Допустимые модификации шаблона

Допустимо применять шаблон не только для обработки (очистки) данных, но также с целью нормализации или изменения формата данных для обеспечения их корректной интерпретации получателем;

Допустимо применять шаблон с целью мониторинга безопасности данных без их обработки (очистки), только для проверки данных, как показано на рисунке 2.

Рисунок 2 – Выделенный обработчик для очистки данных

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.