Адаптация подхода S.T.R.I.D.E. для моделирования угроз

Андрей Моисеев
АО «ИнфоТеКС»

infotecs

План презентации

1. ИнфоТеКС SDL
2. Моделирование угроз
3. Подход S.T.R.I.D.E.
4. ИнфоТеКС S.T.R.I.D.E.
5. Результаты

infotecs


infotecs
ИнфоТеКС SDL

ИнфоТеКС SDL

- ИнфоТеКС SDL – процесс компании, реализуемый с целью повышения качества продуктов

ИнфоТеКС SDL

- сбор требований
- **проектирование**
- разработка
- проверка
- реализация и поддержка
- обучение

Проектирование

Моделирование угроз

- Позволяет превентивно найти проблемы безопасности
- Позволяет поддерживать уровень защищенности в течении ЖЦ продукта

Проектирование

Анализ поверхности атаки

- Позволяет определить наименее защищенные модули
- Позволяет снизить затраты на тестирование

Проектирование

Анализ безопасности архитектуры

- Позволяет улучшать качество выбираемых архитектурных решений


infotecs
Моделирование
угроз

Моделирование угроз

Особенности

- Выполняется на ранних этапах разработки (design)
- Является аналитическим процессом
- Носит систематический характер

Моделирование угроз

infotecs

Цели

- Соответствие парадигме shift-left
- Повышение качества продукта
- Упрощение практик безопасной разработки

Моделирование угроз

Проблематика

- Требуется выделение новых ресурсов
- Результаты субъективны
- Качество зависит от полноты анализа
- Необходимы определенные компетенции:
  - Знание угроз и их сценариев
  - Знание архитектуры
  - Критическое мышление

Моделирование угроз

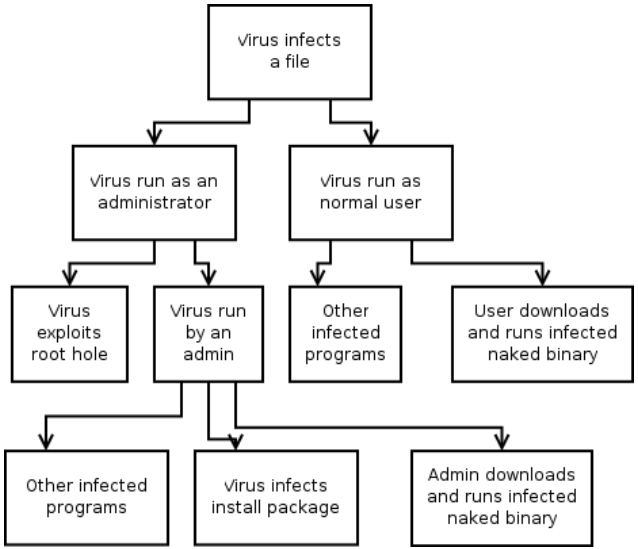
infotecs

Подходы

- Методика оценки УБИ ФСТЭК России
- Attack trees
- Security Cards
- Threatspec – автоматизированный способ моделирования
- S.T.R.I.D.E.

Моделирование угроз

Подходы




infotecs
Подход
S.T.R.I.D.E.

Моделирование угроз

S.T.R.I.D.E.

Stride		Свойство
S-Spoofing	->	Authenticity
T-Tampering	->	Integrity
R-Repudiation	->	Non-repudiability
I-Information Disclosure	->	Confidentiality
D-Denial of Service	->	Availability
E-Elevation of Privilege	->	Authorization

Моделирование угроз

infotecs

S.T.R.I.D.E.

- Анализ выполняется по Data Flow Diagramm (DFD)
- Рассматривается только 6 типов проблем
- Проблемы «накладываются» на компоненты продукта
- Анализ сфокусирован на продукте

Моделирование угроз

infotecs

S.T.R.I.D.E.

Плюсы:

- Простота реализации -> упрощает внедрение
- Наличие DFD диаграммы -> упрощает анализ
- Конечный список проблем -> сужает область анализа
- «Наложение» проблем на компоненты продукта -> выделяет критичные элементы

Моделирование угроз

infotecs

S.T.R.I.D.E.

Минусы:

- Не предполагает поиск конкретных угроз
- Требуется определенный уровень знаний


infotecs
ИнфоТеКС
S.T.R.I.D.E.

ИнфоТеКС S.T.R.I.D.E.

Типовая команда

Менеджер проекта

Архитектор

Аналитик

Разработчик

Тестировщик

ИнфоТеКС S.T.R.I.D.E.

Участники процесса

Команда продукта

Менеджер проекта

Архитектор

Команда SDL

Эксперт SDL

ИнфоТеКС S.T.R.I.D.E.

Этапы процесса

ИнфоТеКС S.T.R.I.D.E.

Инициация процесса

- Процесс инициируется в рамках дизайна архитектуры
- Назначается исполнитель

Менеджер проекта

ИнфоТеКС S.T.R.I.D.E.

Сбор исходных данных

- Описание архитектуры
- Протоколы взаимодействия
- Бизнес-требования
- Требования регуляторов

Исходные данные упростят анализ и верификацию

Архитектор

ИнфоТеКС
S.T.R.I.D.E.

Построение диаграмм

Этап заключается в «переносе» на DFD архитектуры продукта

Плюсы DFD:

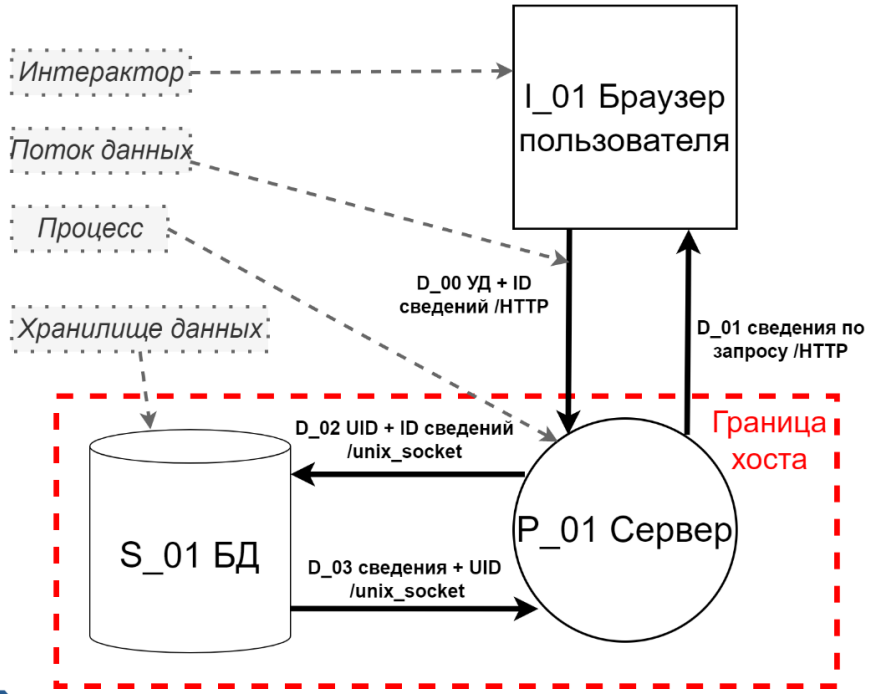
- Наглядность
- Разумная достаточность
- Прослеживаемый процесс обработки информации

Архитектор

ИнфоТеКС S.T.R.I.D.E.

Построение диаграмм

Пример DFD



ИнфоТеКС S.T.R.I.D.E.

Построение диаграмм

При отсутствии исходных данных:

- Рекомендуется построение обобщенных диаграммы
- **Необходимо поддерживать актуальность**

Архитектор

ИнфоТеКС S.T.R.I.D.E.

Построение диаграмм

Проблемы:

- Качество диаграммы зависит от исполнителя
- Ошибки на диаграмме:
  - Снижают качество моделирования
  - Повышают ресурсоемкость

Решение: проводить верификацию диаграмм

Архитектор

ИнфоТеКС S.T.R.I.D.E.

Верификация диаграмм

Проводится экспертом SDL и позволяет:

- Отследить ошибки до этапа моделирования угроз
- Обучать исполнителей

Эксперт SDL

ИнфоТеКС S.T.R.I.D.E.

Моделирование

Моделирование угроз представляет собой:

- Поиск угроз по DFD
- Анализ угроз на применимость, критичность

Архитектор

ИнфоТеКС
S.T.R.I.D.E.

Моделирование. Поиск угроз

Заключается в поиске ***возможных*** угроз и включает:

- Определение поверхности атаки
- Анализ проблем STRIDE
- Документирование угроз

Архитектор

ИнфоТеКС
S.T.R.I.D.E.

Моделирование. Поиск угроз

Поверхность атаки – доступные нарушителю entrypoint

- внешние интерфейсы доступные пользователю
- интерфейсы обрабатывающие информацию после расшифрования
- интерфейсы, обрабатывающие зашифрованную информацию
- интерфейсы, доступные только администратору

Архитектор

ИнфоТеКС
S.T.R.I.D.E.

Моделирование. Поиск угроз

Поиск угроз, выполняется по типам проблем

Stride	Свойство
S-Spoofing	Authenticity
T-Tampering	Integrity
R-Repudiation	Non-repudiability
I-Information Disclosure	Confidentiality
D-Denial of Service	Availability
E-Elevation of Privilege	Authorization

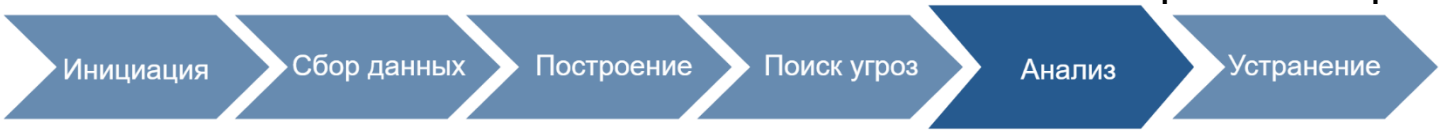
Архитектор

ИнфоТеКС
S.T.R.I.D.E.

Моделирование. Анализ угроз

- Анализ применимости угрозы к продукту
- Оценка критичности угроз

Архитектор



ИнфоТеКС S.T.R.I.D.E.

Итоговая верификация

Проводится экспертом SDL и позволяет:

- Дополнить анализ
- Скорректировать результаты
- Обучать исполнителей

Эксперт SDL

ИнфоТеКС S.T.R.I.D.E.

Устранение угроз

- Менеджер проекта организует работы по устранению угроз
- Угрозы устраняются в порядке их критичности

Менеджер проекта

ИнфоТеКС
S.T.R.I.D.E.

Основные проблемы при моделировании угроз:

- Сложно формализовать описание угрозы
- Часто анализ не полный

Решения:

- Создание чеклиста с угрозами
- Верификация модели экспертом
- Периодическое обучение

ИнфоТеКС S.T.R.I.D.E.

Контроль

Контроль проводится:

- При разработке новых технических решений
- Перед выпуском релиза

При необходимости **модель дорабатывается**

Менеджер проекта

Эксперт SDL

ИнфоТеКС S.T.R.I.D.E.

Контроль

- При разработке новых решений – проверяется актуальность МУ
- Перед выпуском релиза - проверяется факт устранения угроз

Менеджер проекта

Эксперт SDL

Результаты

Результаты

Затраты составили: 2-6% от всех запланированных работ

Результаты

Для 5 продуктов:

- Обнаружено - 87 угроз
- Актуальных - 72 угрозы
- Критичных - 43 угрозы
- Доработок - 21 решение

Спасибо за внимание!

Моисеев А.Ю.

e-mail: Andrey.Moiseev@infotecs.ru

Telegram: https://t.me/try_s0m3_s3c

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news