



SECURITY
TEAM

DEVOPS/DEVSECOPS. БЕЗОПАСНАЯ РАЗРАБОТКА МОДЕЛИРОВАНИЕ УГРОЗ

2024



АЛЕКСАНДР БАКИН

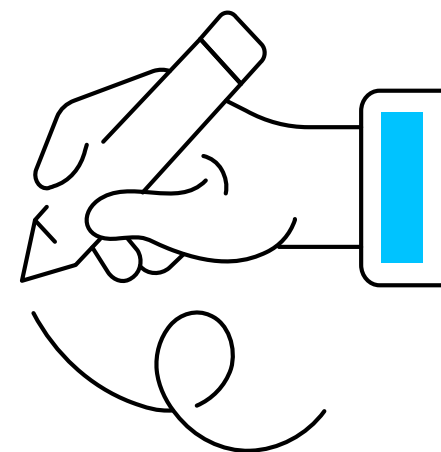
АО «Инфосистемы Джет»

Люблю шоссейный бег и безопасную разработку ПО в любых ее проявлениях.

Отвечаю за консалтинг в направлении безопасной разработки ПО в ЦИБ Джет

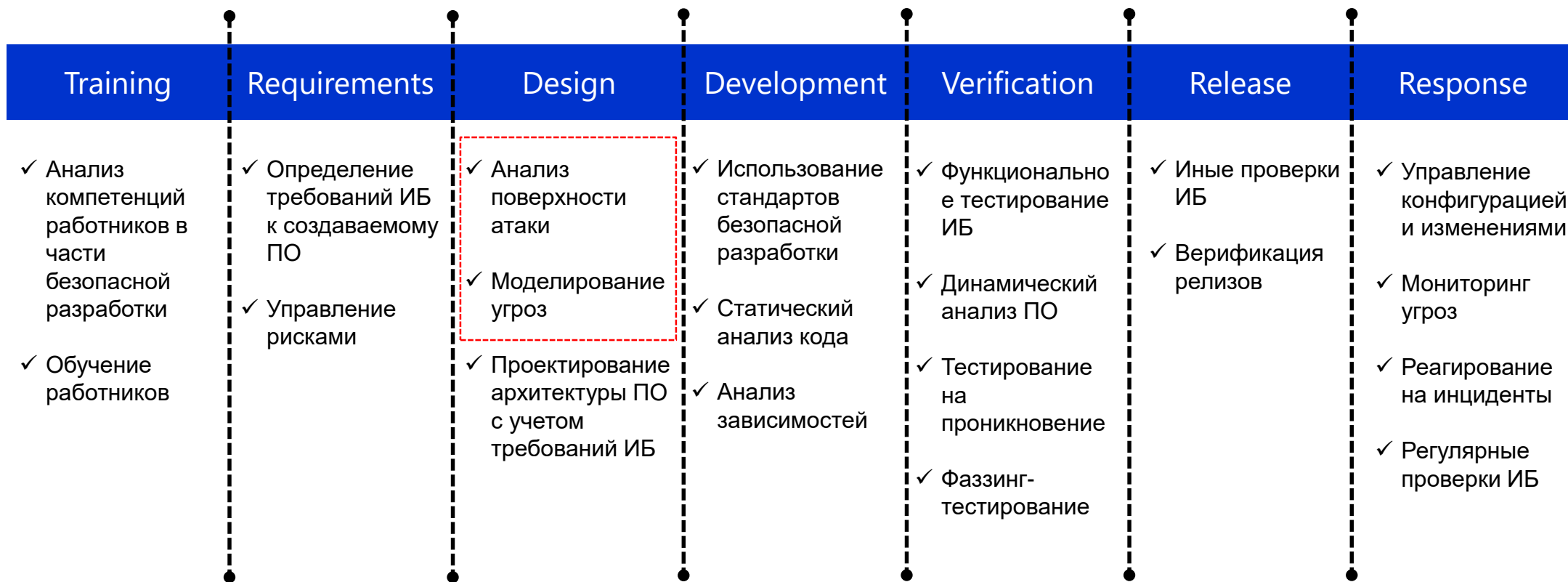
ЦЕЛИ ЗАНЯТИЯ

- ✓ Узнаем общие принципы и подходы к моделированию угроз
- ✓ Выясним, как осуществляется декомпозиция приложений для целей моделирования угроз
- ✓ Рассмотрим подход STRIDE к моделированию угроз
- ✓ Поймем, как проводить классификацию, анализ и ранжирование угроз
- ✓ Познакомимся с субъективными и количественными моделями оценки рисков
- ✓ Поймем, как формировать контрмеры



МОДЕЛИРОВАНИЕ УГРОЗ

ЖИЗНЕННЫЙ ЦИКЛ БЕЗОПАСНОЙ РАЗРАБОТКИ



SSDLC (Secure Software Development Life Cycle)

МОДЕЛИРОВАНИЕ УГРОЗ

ОБЩИЕ ПРИНЦИПЫ

Моделирование угроз – это процесс, направленный на выявление актуальных угроз, их классификацию, оценку рисков и выработку мер по управлению ими

осуществляется на этапе дизайна и в следующих случаях:

- ✓ реализации новых функциональных возможностей
- ✓ возникновения инцидентов безопасности
- ✓ изменений в инфраструктуре или архитектуре

сводится к тому чтобы ответить на следующие вопросы:

- ✓ Над чем мы сейчас работаем?
- ✓ Что может пойти не так?
- ✓ Что мы можем с этим сделать?
- ✓ Как мы убедимся в эффективности принятых мер?

Моделирование угроз отвечает на вопрос:
«Что представляет собой безопасность в нашем проекте?»

МОДЕЛИРОВАНИЕ УГРОЗ ИНСТРУМЕНТАРИЙ



[Visual Paradigm](#)



[Microsoft Threat Modeling Tool](#)

МОДЕЛИРОВАНИЕ УГРОЗ

ДЕКОМПОЗИЦИЯ ПРИЛОЖЕНИЯ

Внешние зависимости

Внешние по отношению к коду элементы, которые могут представлять угрозу приложению.

Эти элементы обычно находятся под контролем организации, но, возможно, не под контролем команды разработчиков:

- ✓ компоненты операционной системы
- ✓ базы данных и хранилища
- ✓ средства защиты и обнаружения атак
- ✓ сторонние компоненты, которые используются в проекте

Точки входа

Определяют интерфейсы, через которые потенциальные злоумышленники могут взаимодействовать с приложением, предоставляя ему данные и изменяя его состояние.

Точки входа в приложение могут быть многоуровневыми.

Они показывают, где данные поступают в систему:

- ✓ поля ввода
- ✓ аргументы методов API
- ✓ параметры HTTP-запроса
- ✓ вариативные части сообщений сетевых протоколов и т. п

МОДЕЛИРОВАНИЕ УГРОЗ

ДЕКОМПОЗИЦИЯ ПРИЛОЖЕНИЯ

Точки выхода

Соответствуют местам, в которых данные передаются от приложения окружению.

- ✓ запись данных в базу данных или хранилище
- ✓ осуществление сетевых запросов
- ✓ запуск сторонних процессов
- ✓ отправка HTTP-ответа веб-сервером и т. п.

Ресурсы

Цель потенциальной атаки злоумышленника, причина существования угроз.

Ресурсы могут быть **информационными**:

- ✓ учётные или персональные данные пользователей
- ✓ информация о транзакциях
- ✓ криптографические ключи

Или **абстрактными**:

- ✓ репутация
- ✓ стоимость акций
- ✓ правовые аспекты

Уровни доверия

Представляют собой права доступа, которые приложение предоставляет внешним объектам.

Уровни доверия связаны с точками входа и ресурсами. Это позволяет определить права доступа или привилегии, необходимые для каждой точки входа и взаимодействия с каждым ресурсом







МОДЕЛИРОВАНИЕ УГРОЗ

ДИАГРАММЫ ПОТОКОВ ДАННЫХ (DATA FLOW DIAGRAM)

- ✓ DFD показывают, как данные логически проходят через приложение от начала до конца. Они позволяют идентифицировать затронутые компоненты через критические точки и поток управления через эти компоненты
- ✓ DFD имеют иерархическую структуру, поэтому их можно использовать для декомпозиции приложения на подсистемы и подсистемы более низкого уровня
- ✓ Итерации более низкого уровня позволяют сосредоточиться на определённых процессах, связанных с обработкой конкретных данных
- ✓ Существует ряд общепринятых символов, которые используются в DFD для моделирования угроз

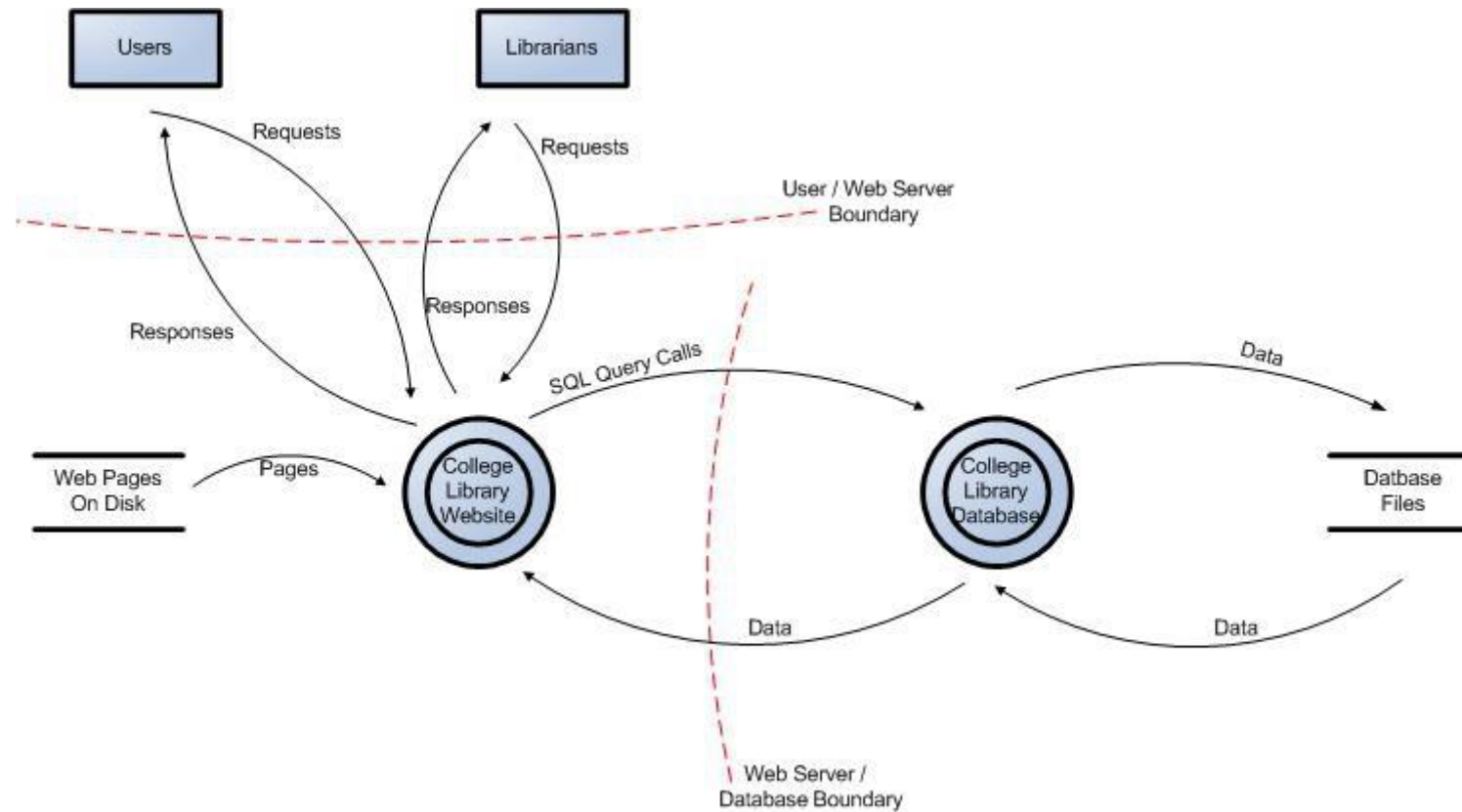
МОДЕЛИРОВАНИЕ УГРОЗ

СИМВОЛЫ DFD

Символ	Название	Описание
	Внешняя сущность	Используется для представления любого объекта вне приложения, который взаимодействует с ним через точку входа
	Процесс	Представляет задачу, которая обрабатывает данные в приложении. Она может обрабатывать данные или выполнять действие на основе данных
	Множественный процесс	Используется для представления набора подпроцессов. Множественный процесс может быть разбит на подпроцессы в другом DFD
	Хранилище данных	Используется для представления мест, где хранятся данные. Хранилища данных не изменяют данные
	Поток данных	Представляет движение данных внутри приложения. Направление изображено стрелкой
	Граница доверия	Используется для представления изменения уровней доверия по мере прохождения данных через приложение. Границы показывают любое место, где изменяется уровень доверия

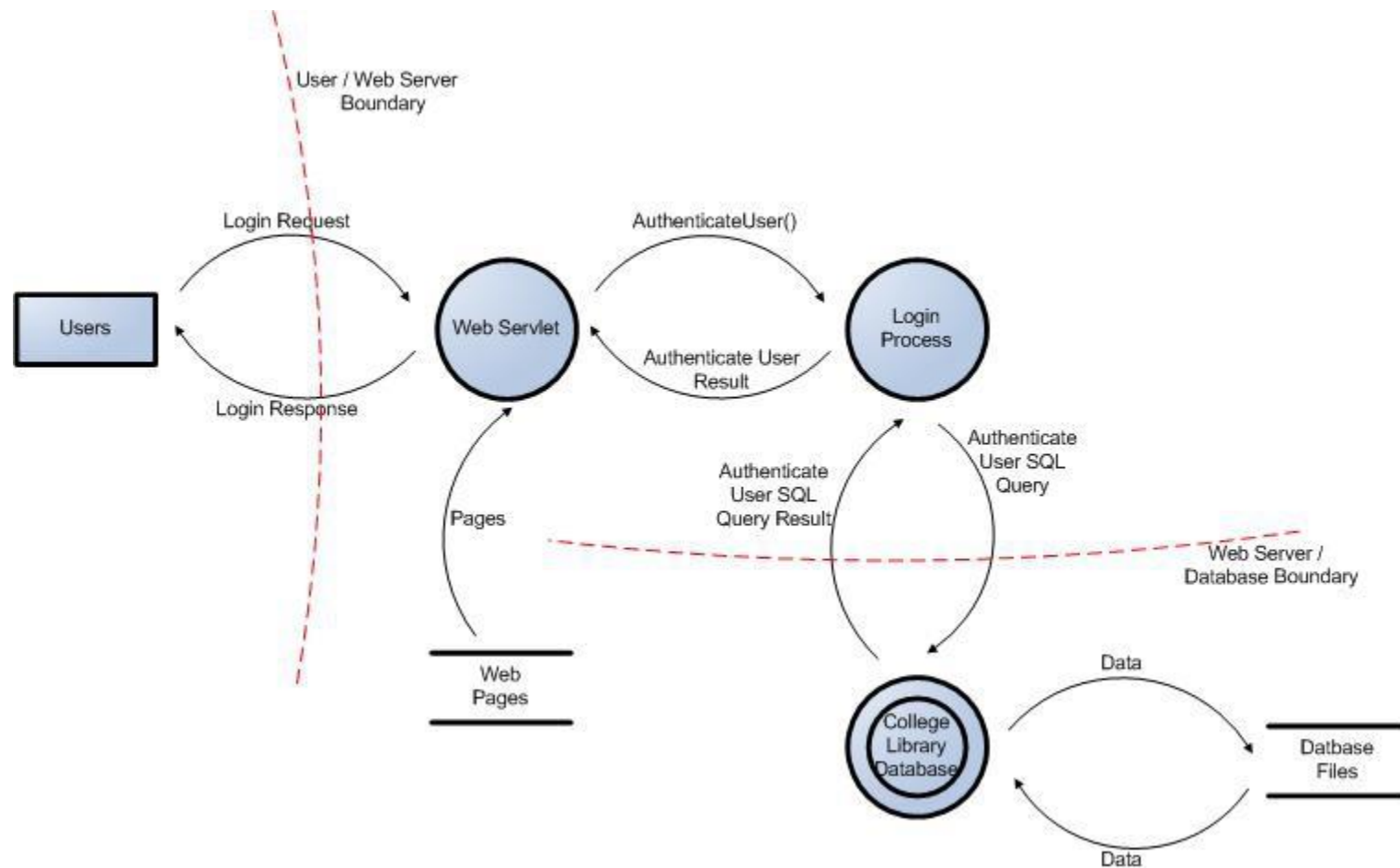
МОДЕЛИРОВАНИЕ УГРОЗ

ПРИМЕР DFD (ОБЩАЯ)



МОДЕЛИРОВАНИЕ УГРОЗ

ПРИМЕР LOGIN DFD



МОДЕЛИРОВАНИЕ УГРОЗ

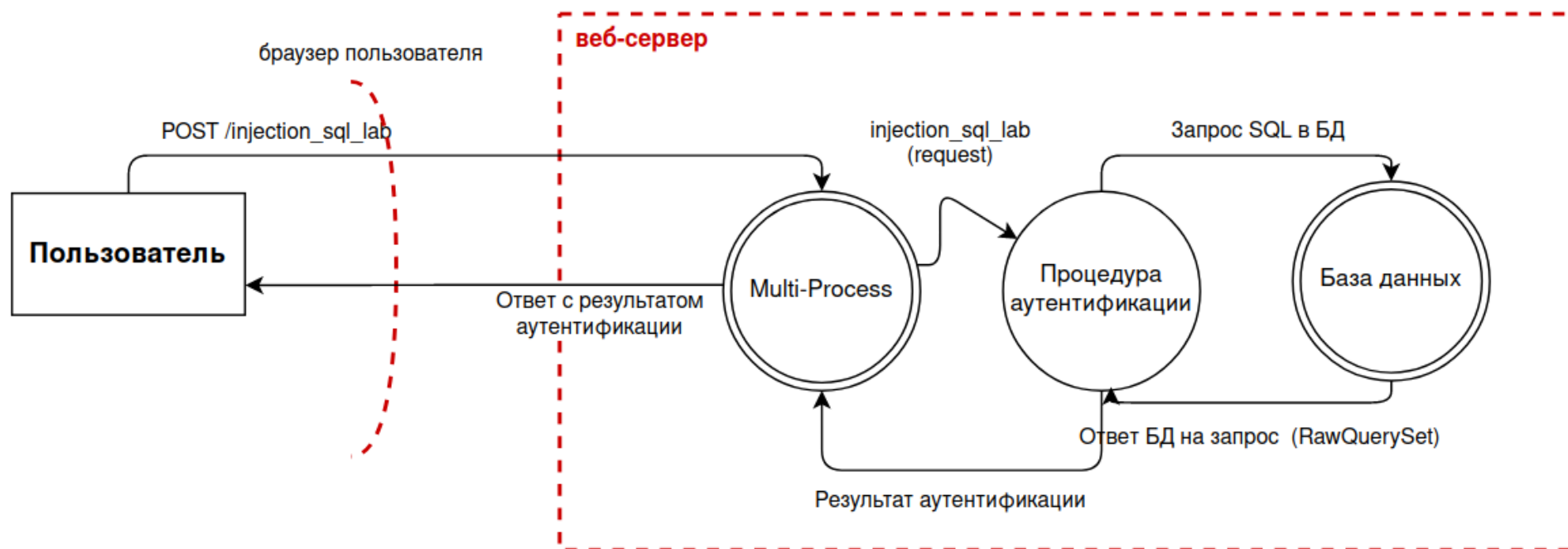
КЛАССИФИКАЦИЯ УГРОЗ STRIDE

Тип	Описание	Контроль
Spoofing	Доступ и использование учётных данных другого пользователя: имени пользователя и пароля	Authentication
Tampering	Злонамеренная модификация постоянных данных, таких как записи в базе данных, а также изменение данных, которые передаются между двумя компьютерами по открытой сети	Integrity
Repudiation	Выполнение запрещённых операций в системе, в которой отсутствует возможность отслеживания операций	Non-repudiation
Information disclosure	Получение хранящихся данных, к которым не было предоставлено доступа, или на чтение данных в ходе их передачи	Confidentiality
Denial-of-service	Запрет доступа авторизованным пользователям через нарушение нормального функционирования приложения	Availability
Elevation of privilege	Получение привилегированного доступа к ресурсам, чтобы получить несанкционированный доступ к информации или скомпрометировать систему	Authorization

ПРАКТИЧЕСКАЯ ЗАДАЧА

ПРАКТИЧЕСКАЯ ЗАДАЧА

- ✓ Идентифицируйте актуальные угрозы
- ✓ Классифицируйте их в соответствии с методологией STRIDE



ОЦЕНКА РИСКОВ И РАНЖИРОВАНИЕ УГРОЗ

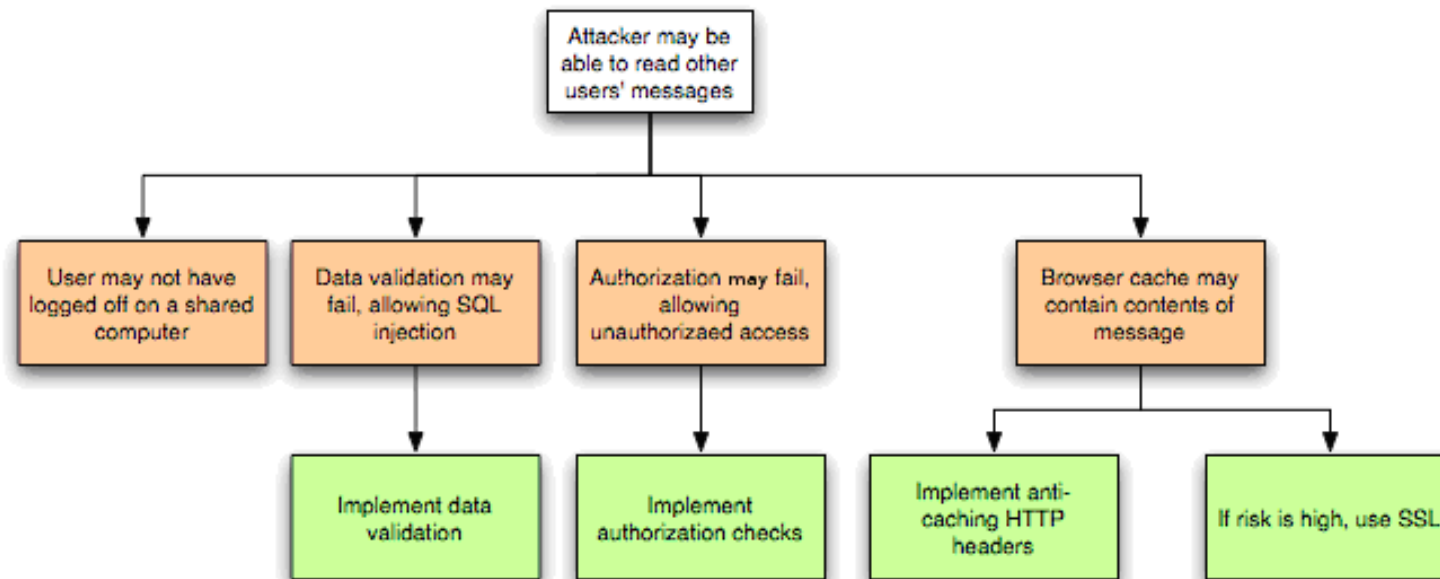
ОЦЕНКА РИСКОВ

АНАЛИЗ УГРОЗ

- ✓ **Риск** — это возможность потерь. Определяется двумя факторами: вероятностью того, что произойдёт нападение, и потенциальным влиянием или стоимостью такой атаки. Риск рассчитывается так:
(вероятность возникновения угрозы) x (ожидаемый ущерб)
- ✓ **Анализ угроз** — идентификация угроз для приложения, включающая анализ каждого аспекта функциональности, архитектуры и дизайна приложения с точки зрения целей атакующего
- ✓ Угрозы анализируются через изучение возможных путей атаки и необходимых средств противодействия ей
- ✓ Результаты анализа угроз удобно представлять визуально: в виде дерева угроз и графа кейсов угроз

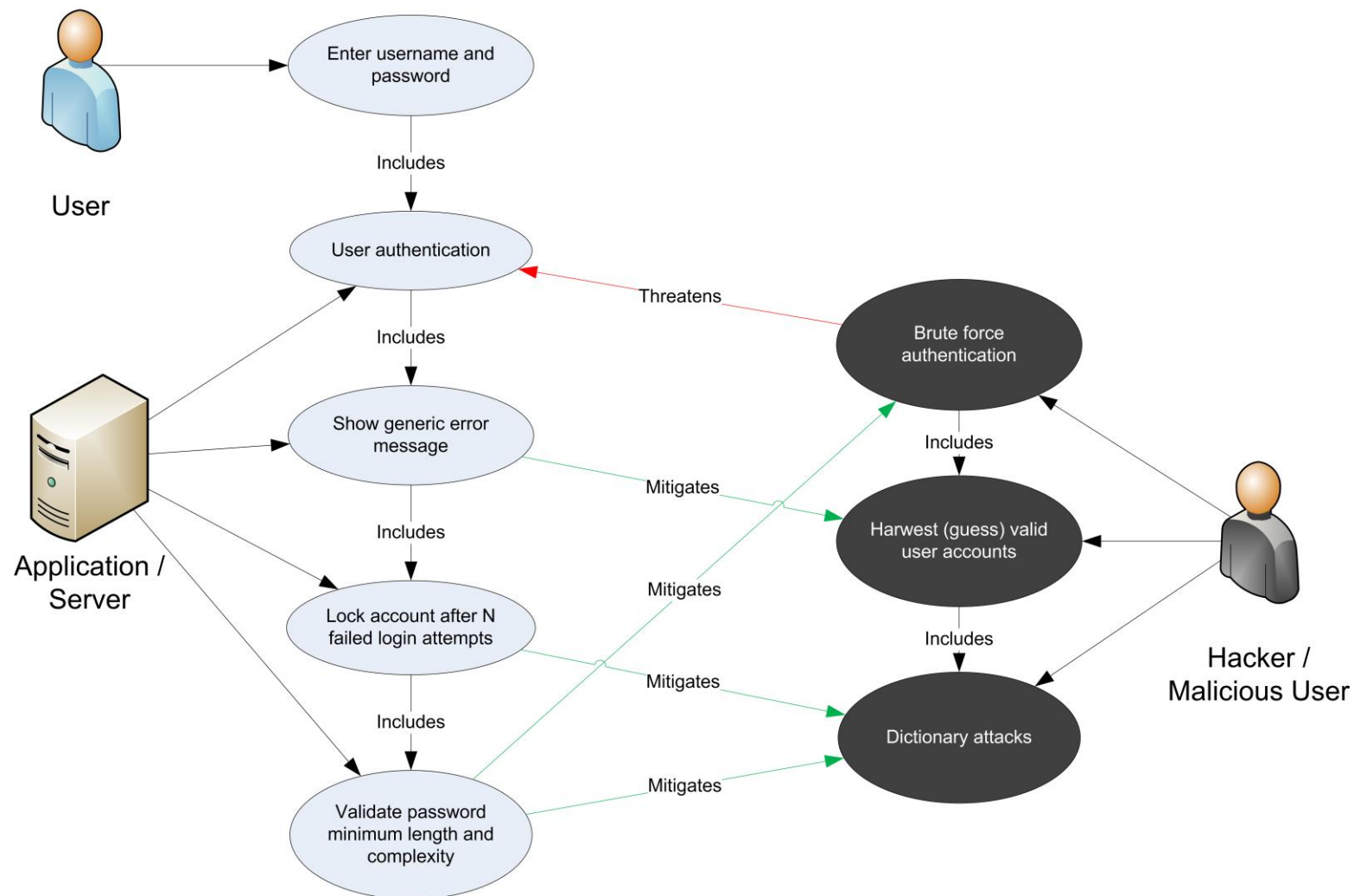
ОЦЕНКА РИСКОВ

ПРИМЕР ДЕРЕВА УГРОЗ



ОЦЕНКА РИСКОВ

ПРИМЕР ГРАФА КЕЙСОВ УГРОЗ



ОЦЕНКА РИСКОВ

РАНЖИРОВАНИЕ УГРОЗ























Субъективная модель: DREAD

В модели оценки рисков DREAD факторизация рисков позволяет присваивать значения различным влияющим факторам угрозы. Чтобы определить рейтинг угрозы, аналитик отвечает на вопросы по каждому фактору риска, субъективно оценивая их по 10-бальной шкале:

- ✓ **Damage:** насколько большим будет ущерб, если атака увенчается успехом?
- ✓ **Reproducibility:** насколько легко воспроизвести атаку?
- ✓ **Exploitability:** сколько времени, усилий и опыта необходимо для эксплуатации угрозы?
- ✓ **Affected Users:** если угроза будет использована, какой процент пользователей будет затронут?
- ✓ **Discoverability:** насколько легко злоумышленнику обнаружить эту угрозу?

Количественная модель: CVSS

Более точную оценку рисков позволяют получить количественные модели, которые учитывают множество измеримых факторов риска. Они позволяют достичь воспроизводимых оценок, не зависящих от мнения конкретного аналитика. Наиболее распространённая количественная модель - CVSS (Common Vulnerability Scoring System)

ATTACK VECTOR	ATTACK COMPLEXITY	PRIVILEGES REQUIRED	USER INTERACTION
 Network	 Low	 None	 None
 Adjacent	 High	 Low	 Required
 Local		 High	
 Physical			
SCOPE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
 Changed	 High	 High	 High
 Unchanged	 Low	 Low	 Low
	 None	 None	 None

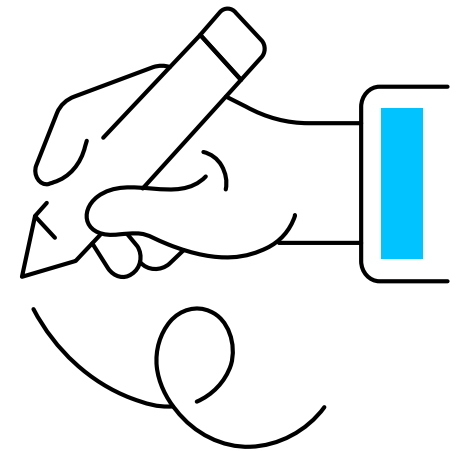
ОЦЕНКА РИСКОВ

КОНТРОЛЕРЫ

Тип угрозы	Способы противодействия	
Spoofing	<ul style="list-style-type: none">✓ Надлежащая аутентификация✓ Защита секретных данных	<ul style="list-style-type: none">✓ Отказ от хранения секретов
Tampering	<ul style="list-style-type: none">✓ Надлежащая авторизация✓ Хеши✓ MACs	<ul style="list-style-type: none">✓ Цифровые подписи✓ Протоколы защиты от подделки данных
Repudiation	<ul style="list-style-type: none">✓ Цифровые подписи✓ Временные метки	<ul style="list-style-type: none">✓ Журналы аудита
Information disclosure	<ul style="list-style-type: none">✓ Авторизация✓ Протоколы с усиленной конфиденциальностью	<ul style="list-style-type: none">✓ Шифрование✓ Защита секретных данных✓ Отказ от хранения секретов
Denial-of-service	<ul style="list-style-type: none">✓ Надлежащая аутентификация✓ Надлежащая авторизация✓ Фильтрация	<ul style="list-style-type: none">✓ Троттлинг✓ QoS
Elevation of privilege	<ul style="list-style-type: none">✓ Запуск с наименьшими привилегиями	

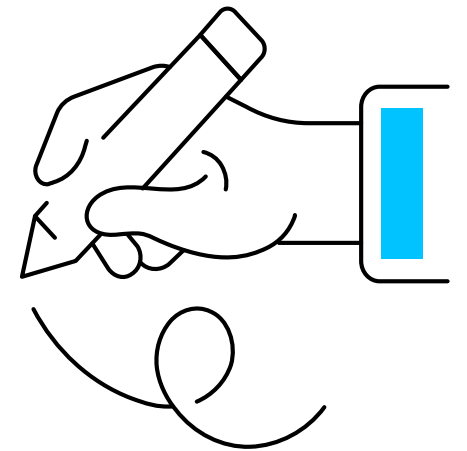
ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ

- ✓ [Online Drawing Tool](#)
- ✓ [Microsoft Treat Modeling Tool](#)
- ✓ [Threat Modeling Process](#)



ВЫВОДЫ

- ✓ Узнали, как проводить декомпозицию приложения
- ✓ Изучили какие сущности архитектуры следует рассматривать
- ✓ Поняли, как строить диаграммы потоков данных
- ✓ Рассмотрели подход STRIDE к классификации угроз
- ✓ Поняли, как проводить анализ угроз
- ✓ Рассмотрели деревья и графы кейсов угроз
- ✓ Познакомились с принципами ранжирования угроз, изучили модели DREAD и CVSS
- ✓ Узнали, как формулировать контрмеры



ДОМАШНЕЕ ЗАДАНИЕ

ДОМАШНЕЕ ЗАДАНИЕ

Цель: получить практические навыки моделирования угроз

Инструмент: Online Drawing Tool или любой другой подходящий редактор диаграмм, doc.google

Формат выполнения: doc.google, проверьте настройки доступа к документу, ссылку на работу присылать на pokprobaks@gmail.com

Результат: понимание принципов архитектурной декомпозиции, оценки угроз и анализа рисков

Контекст/описание: построить модель угроз для учебного приложения

Сроки выполнения: до 29 августа 2024 включительно

1. Загрузите репозиторий любого приложения с открытым исходным кодом.
2. Выделите в приложении основные архитектурные компоненты, представляющие интерес с точки зрения задач обеспечения защищенности и найдите границы уровней доверия. Используйте пример структуры из статьи OWASP [Threat Modeling Process](#).
3. Опишите актуальные для приложения угрозы, оцените риск реализации каждой из них и сформулируйте контрмеры