АНАЛИЗ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кохно П.М.
Ярмолик В. Н. – д-р. техн. наук, профессор

Рассмотрим классификацию угроз безопасности STRIDE и методы борьбы с ними. Для выбора эффективного метода защиты применяются различные методики количественной оценки риска опасности для вычислительных систем. Расширим одну из популярных методик DREAD еще одним показателем – затраты финансов и ресурсов на устранение последствий успешной атаки.

Процесс предотвращения или снижения критичности грозящих вычислительной системе опасностей состоит из следующих этапов:

1) Классификация угроз безопасности, грозящих системе;
2) Определение методов защиты от опасностей;

Для классификации угроз безопасности (первый этап) может быть использована классификация, называемая STRIDE, разработанная фирмой Microsoft и успешно применяемая для определения опасностей, грозящих разрабатываемым системам [1]:

• **Подмена сетевых объектов (Spoofing identity)** Атаки подобного типа позволяют взломщику выдавать себя за другого пользователя или подменять настоящий сервер подложным. Пример подмены личности пользователя — использование чужих аутентификационных данных (имени пользователя пароля) для атаки на систему. Типичный пример подобной уязвимости - применение ненадежных методов аутентификации.

• **Модификация данных (Tampering with data)** Данные атаки предусматривают преднамеренную порчу данных. Например, изменение информации, пересылаемой между компьютерами через открытую сеть (Интернет).

• **Отказ от авторства (Repudiation)** Пользователь отказывается от совершенного им действия (или бездействия), пользуясь тем, что у другой стороны нет никакого способа доказать обратное. Например, в системе, где не ведется аудит, пользователь может выполнить запрещенную операцию и отказаться от ее «авторства», а администратору не удастся ничего доказать.

• **Разглашение информации (Information disclosure)** Подразумевается раскрытие информации лицам, доступ к которой им запрещен, например, прочтение пользователем файла, доступ к которому ему не предоставлялся, а также способность злоумышленника считывать данные при передаче между компьютерами.

• **Отказ в обслуживании (Denial of service)** В атаках такого типа взломщик пытается ограничить доступ к сервису пользователей, например, сделав Web-сервер временно недоступным или непригодным для работы. Необходимо защищаться от определенных видов DoS-атак — это повысит доступность и надежность системы.

• **Повышение привилегий (Elevation of privilege)** В данном случае непривилегированный пользователь получает привилегированный доступ, позволяющий ему «взломать» или даже уничтожить систему. К повышению привилегий относятся и случаи, когда злоумышленник удачно проникает через защитные средства системы и становится частью защищенной и доверенной подсистемы.

На следующем этапе следует определить методы защиты от угроз безопасности. Для решения данной задачи был проведен анализ атак на объекты вычислительных систем и определены возможные методы защиты. Результаты исследований приведены в таблице 1, в которой перечислены методы, применяемые для борьбы с опасностями, описанными в модели STRIDE [1].

Таблица 1. Основные методы борьбы с опасностями

Тип опасности	Средства борьбы
Подмена сетевых объектов (S)	• Надежный механизм аутентификации • Защита секретных данных • Отказ от хранения секретов
Модификация данных (T)	• Надежный механизм авторизации • Использование хешей • Цифровые подписи • Протоколы, предотвращающие прослушивание трафика
Отказ от авторства (R)	• Цифровые подписи • Метки даты и времени • Контрольные следы
Разглашение информации (I)	• Авторизация • Протоколы с усиленной защитой от несанкционированного доступа • Шифрование • Защита секретов • Отказ от хранения секретов

Отказ в обслуживании (D)	• Надежный механизм аутентификации • Надежный механизм авторизации • Фильтрация • Управление числом входящих запросов
Повышение уровня привилегий (E)	• Выполнение с минимальными привилегиями

Предложенные в таблице 1 средства борьбы с опасностями можно свести к следующим:

- Аутентификация;
- Авторизация;
- Защита от несанкционированного доступа;
- Аудит;
- Фильтрация.

Для выбора одного из предложенных методов желательно выполнить количественную оценку риска опасности для конкретной вычислительной системы. Как правило, применяют следующие методы количественной оценки риска:

1. Способ оценки риска (Risk) — умножить важность (величина потенциального ущерба) уязвимого места на вероятность того, что им воспользуются. Критичность и вероятность оценивают по шкале от 1 до 10:

<Risk>=<Потенциальный ущерб> * <Вероятность возникновения>

Чем больше полученное число, тем больше угроза системе. Так, максимально возможная оценка риска равна 100 — произведению максимальной важности (10) и вероятности возникновения (10).

2. Еще один способ оценки риска –DREAD назван так по первым буквам английских названий описанных далее категорий:

- **Потенциальный ущерб (Damage potential) —** мера реального ущерба от успешной атаки. Наивысшая степень (10) опасности означает практически беспрепятственный взлом средств защиты и выполнение практически любых операций. Повышению привилегий обычно присваивают оценку 10. В других ситуациях оценка зависит от ценности защищаемых данных. Для медицинских, финансовых и военных данных она обычно высока.
- **Воспроизводимость (Reproducibility) —** мера возможности реализации опасности. Некоторые уязвимости доступны постоянно (оценка — 10), другие — только в зависимости от ситуации, и их доступность непредсказуема, то есть нельзя наверняка знать, насколько успешной окажется атака. Уязвимости в устанавливаемых по умолчанию функциях характеризуются высокой воспроизводимостью.
- **Подверженность взлому (Exploitability) —** мера усилий и квалификации необходимых для атаки. Так, если ее может реализовать неопытный программист на домашнем компьютере - 10. Если же для ее проведения надо потратить 1 000 000 долларов, оценка опасности - 1. Атака, для которой можно написать алгоритм (а значит, распространить в виде сценария среди любителей), также оценивается в 10 баллов. Следует также учитывать необходимый для атаки уровень аутентификации и авторизации в системе. Например, если это доступно любому удаленному анонимному пользователю, подобная опасность оценивается 10 баллами. А вот атака, доступная только доверенному локальному пользователю, менее опасна.
- **Круг пользователей, попадающих под удар (Affected users) —** доля пользователей, работа которых нарушается из-за успешной атаки. Оценка выполняется на основе процентной доли: 100% всех пользователей соответствует оценка 10, а 10% — 1 балл. Чрезвычайно важно проводить границу между сервером и клиентским компьютером: от ущерба, нанесенного серверу, пострадает больше клиентов и, возможно, другие сети. В этом случае балл значительно выше, чем оценка атаки только на клиентские компьютеры. Также не следует забывать о размерах рынка и абсолютном, а не только процентном, количестве пользователей. Один процент от 100 млн. пользователей — это все равно много.
- **Вероятность обнаружения (Discoverability) —** самая сложная для определения оценка. Как правило, любая опасность поддается реализации, поэтому можно ставить всегда 10 баллов. Суммарная DREAD-оценка равна среднему арифметическому всех оценок. Способ оценки риска DREAD предложен М. Ховардом и Д. Лебланком.

Так же предлагаю включить в методику DREAD еще один показатель - затраты денег и ресурсов на устранение последствий успешной атаки, условно названный C (Cost). Таким образом, для количественной оценки риска используется модель DREADC и суммарная DREADC-оценка равна сумме всех оценок деленной на 6).

Таким образом были рассмотрены методы оценки безопасности вычислительных систем, которые постоянно обновляются и совершенствуются. Мной была расширена одна из методик и дополнена новым параметром.

Список использованных источников:

1. Ховард М., Лебланк Д. Защищенный код. Пер. с англ. – 2-е изд., испр. М.: Издательско-торговый дом «русская редакция», 2004. – 704 стр.: ил.
2. Ахмад Д.М., Дубровский И., Флинн Х и др. Защита от хакеров корпоративных сетей. Пер. с англ. – 2-е изд. М.: Компаний АйТи; ДМК- Пресс, 2005. – 864 стр.: ил.