ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Глава 1. Безопасность в компьютерной сфере

1.1. Значение компьютерной безопасности

Значение термина компьютерная безопасность менялось в течение последних лет. До того, как проблема информационной безопасности стала широко освещаться, большая часть людей думала о компьютерной безопасности в контексте физических устройств. Традиционно компьютерное оборудование было физически защищено по трём причинам:

- чтобы предотвратить кражу или повреждение железа;
- чтобы предотвратить кражу или повреждение информации;
- чтобы предотвратить сбои в работе.

Определение 1.1. ***Компьютерная безопасность*** *это безопасность компьютерных устройств, таких как компьютеры и смартфоны, а также компьютерных сетей, таких как публичные и частные сети, включая весь интернет. Эта область охватывает все процессы и механизмы, с помощью которых цифровое оборудование, информация и сервисы защищаются от непреднамеренного или несанкционированного доступа, изменения или уничтожения.*

Иногда это также называется “кибербезопасностью” или “IT безопасностью”. Важными терминами в этой области являются:

Уязвимость

Уязвимость это слабость, которая позволяет злоумышленнику снизить системные гарантии для информации. Уязвимость это пересечение трёх элементов: несовершенности в системе или ошибки; доступ злоумышленника к этой ошибке; и способность злоумышленника эксплуатировать эту ошибку. Чтобы эксплуатировать уязвимость, злоумышленник должен иметь хотя бы один подходящий инструмент или методику, которая может дать ему доступ к системной слабости. В этом контексте уязвимость также называется местом атаки.

Управление уязвимостями это циклическая работа по идентификации, классификации, устранению и уменьшению уязвимостей. Обычно такая работа проводится над программными уязвимостями в компьютерных системах.

Бэкдор

Бэкдор (backdoor) в компьютерной системе это метод обхода обычной аутентификации, обеспечивающей удаленный доступ к компьютеру, для получения доступа к исходному тексту и т.п., в то же время оставаясь незамеченным.

Бэкдор может принимать форму установленной программы, или может быть модификацией к уже существующей программе или аппаратному устройству.

DoS атака

В отличие от других способов эксплуатации, DoS (Denial-of-service) атаки не используются для получения несанкционированного доступа или контроля системы. Вместо этого они используются для приведение системы к нерабочему состоянию. Злоумышленники могут помешать доступу к сервису для индивидуальных жертв посредство специального ввода неправильного пароля достаточное количество раз для того, чтобы заблокировать аккаунт жертвы; либо же они могут перегрузить возможности машины или всей сети и заблокировать всех пользователей разом. Эти типы атак на практике очень трудно превратить, потому что требуется анализ поведения всей сети, а не только какого-то куска кода.

DDoS (Distributed DoS) атаки распространены там, где большое количество скомпрометированных хостов (также называемых “зомби компьютерами”, используемыми для создания бот-сетей с помощью, например: червей, троянов или бэкдоров для получения контроля над ними) используются для закидывания целевой системы сетевыми запросами, тем самым пытаясь сделать её недоступной из-за истощения ресурсов.

Direct-access атака

Несанкционированный пользователь, получивший физический доступ к компьютеру, может совершить множество действий, установить различные типы устройств, компрометирующих безопасность, включая модификации операционной системы, программные черви, кейлоггеры и скрытые подслушивающие устройства. Злоумышленник может также легко скачивать большие объемы данных на свои носители информации. Другой распространенной методикой является загрузка операционной системы, содержащейся на каком-либо загрузочном устройстве, и считывание данных с жесткого диска. Единственный способ победить такую атаку это использование шифрования данных и хранения

ключа в другой системе.

Подслушивание

Подслушивание это процесс тайного прослушивания частных разговоров, обычно между хостами внутри сети. Например, такие программы как Carnivore и NarusInsight были использованы ФБР и АНБ для подслушивания систем интернет провайдеров.

Спуфинг

Спуфинг личности пользователя это ситуация, в которой человек или программа успешно притворяется другим с помощью фальсификации данных, тем самым получая незаконное преимущество.

Подделка

Подделка это умышленная модификация продукта таким образом, чтобы сделать его вредоносным для потребителя.

Отказ

Отказ это ситуация, когда подлинность подписи ставится под сомнение.

Раскрытие информации

Раскрытие информации (нарушение конфиденциальности или утечка данных) это ситуация, в которой информация, подразумевающаяся в безопасности, публикуется в ненадежной среде.

Повышение привилегий

Повышение привилегий описывает ситуацию, в которой человек или программа хотят получить повышенные привилегии для доступа к ресурсам, которые для него недоступны.

Эксплойты

Эксплойт это часть программы, кусок данных или последовательность команд, которая использует программный баг или глитч для того, чтобы вызвать непредусмотренное или неожиданное поведение в компьютерной программе, железе или чем-то электрическом (обычно компьютеризированном). Это ча-

сто включает в себя такие вещи как получение контроля над компьютерной системой или получение повышенных привилегий или DoS атаки. Термин “эксплойт” (exploit) обычно относится к маленьким программам, созданным для использования уязвимостей, которые были найдены в системе. Код от “эксплойт” программ часто используется в троянах и компьютерных вирусах.

Indirect атака

Indirect атак это атака запущенная с помощью стороннего компьютера. Используя чей-то чужой компьютер для проведения атаки, становится гораздо сложнее вычислить настоящего злоумышленника. Также бывают случаи, когда злоумышленник использует публичные анонимизирующие системы.

Компьютерные преступления

Компьютерные преступления это любые преступления, которые вовлекают использование компьютера или сети.

1.2. Топ 10 советов для предотвращений киберпреступлений

1. **Используйте сложные пароли**. Используйте различные комбинации пользовательских ID и паролей для различных аккаунтов и избегайте их сохранения. Сделайте пароли более сложными, комбинируя буквы, цифры, спец символы, и регулярно их меняйте.
2. **Обезопасьте свой компьютер**
   - **Включите фаервол**. Фаервол это первая линия киберзащиты; они блокируют подключения к неизвестным и подозрительным сайтам и защищают от некоторых типов вирусов и хакеров.
   - **Используйте антивирусное обеспечение**. Предотвратите заражение вашего компьютера вирусами с помощью установки и регулярного обновления антивирусного обеспечения.
   - **Блокируйте шпионские атаки**. Предотвратите проникновение в ваш компьютер шпионских программ установив и регулярного обновляя антишпионское обеспечение.
3. **Будьте осторожны в соцсетях**. Сделайте доступ к своим социальным профилям приватным. Будьте аккуратно в том, какую информацию вы размещаете онлайн. Один раз в интернете – навсегда в интернете!

4. **Обезопасьте свои мобильные устройства**. Мобильные устройства также подвержены вирусам и хакерам. Устанавливайте приложения только из проверенных источников.
5. **Устанавливайте самые свежие обновления для операционной системы**. Поддерживайте приложения и операционные системы в свежем состоянии. Включите автоматические обновления для предотвращения потенциальных атак на более устаревшие версии.
6. **Защищайте свои данные**. Используете шифрование для самой важной информации, например, финансовой отчетности. Делайте регулярные бэкапы всей своей самой важной информации и храните её в другом месте.
7. **Обезопасьте свою беспроводную сеть**. Wi-Fi сети в домах уязвимы для проникновения, если они недостаточно защищены. Проверьте и модифицируйте дефолтные настройки. Публичные Wi-Fi также уязвимы, избегайте обмен финансовой или корпоративной информацией через такие сети.
8. **Защищайте свою электронную личность**. Будьте на чеку, когда передаёте свою личную информацию, такую как имя, адрес, телефонный номер или финансовую информацию в интернете. Убедитесь, что сайт безопасен (например, когда производите онлайн покупку) или что вы включили настройки безопасности (например, когда используете соцсети).
9. **Избегайте мошенничества**. Всегда думайте прежде чем кликнуть на ссылку или файл неизвестного происхождения. Не испытывайте давления ни от каких писем. Проверяйте источник сообщения. Если сомневаетесь, то верифицируйте источник. Никогда не отвечайте на письма, которые просят вас подтвердить информацию о вашем ID или пароле.
10. **Позовите правильного человека на помощь**. Не паникуйте! Если вы жертва, или если вы столкнулись с нелегальным контентом в интернете, или если вы подозреваете компьютерное преступление, сообщите об этом в полицию. Если вам нужна помощь с поддержкой или установкой программного обеспечения на ваш компьютер, проконсультируйтесь со своим провайдером или сертифицированным компьютерным специалистом.

Глава 2. Программная безопасность

2.1. Безопасная программа

Давайте подумаем, что значит, когда мы говорим, что программа “безопасна”. Мы знаем, что безопасность подразумевает некоторую степень уверенности, что программа соблюдает ожидаемую конфиденциальность, честность и доступность. С точки зрения программы или программиста, как мы можем, глядя на программную компоненту или фрагмент кода, оценить его безопасность? Этот вопрос похож на проблему оценивая качества программного обеспечения в целом. Один из способов для оценки безопасности в таком случае будет опрос людей характеристик программы, которые обеспечивают общую безопасность. Однако, мы наверняка получим разные ответы от разных людей. Например, один человек может считать код безопасным, если для взлома его контроля безопасности потребуется очень много времени. Кто-то другой может посчитать код безопасным если он работает в течение какого-то времени без видимых поломок. А кто-то третий может решить, что любая потенциальная ошибка в соблюдении требований безопасности делает код небезопасным.

Ранние работы в компьютерной безопасности были основаны на парадигме “проникнуть и залатать”, в которой аналитики искали и исправляли ошибки. Часто собиралась команда профессионалов, чтобы попытаться сломать программу. Этот тест считался подтверждением безопасности; если система выдерживала атаку, то она считалась безопасной. К несчастью, зачастую подтверждение становилось опровержением, в результате которого находилось несколько серьезных проблем с безопасностью. Нахождения проблемы в свою очередь превращалось в быструю попытку “залатать” систему, чтобы восстановить безопасность. Однако попытки залатать часто были бесполезными, так как привносили в систему новые ошибки.

Недостатки такого подхода привели исследователей к поиску лучшего способа быть уверенным, что код соответствует требованиям безопасности. Один из таких способов это сравнение требований с поведением. Чтобы понять безопасность программы, мы можем проанализировать программу, чтобы увидеть, ведёт ли она в соответствии с тем, как было задумано и тем, что ожидают пользователи. Неожиданное поведение называется дефектом безопасности программы.

Чтобы лучше понимать проблемы и пути их решений, мы можем разделить возможные дефекты на несколько категорий:

1. валидационные ошибки (неполные или неверные): проверка доступов
2. доменные ошибки: контролируемый доступ к данным
3. сериализация и наложение: программный порядок исполнения
4. недостаточная идентификация и аутентификация: основа авторизации
5. нарушение граничных условий: ошибки на первом или последнем случае
6. другие эксплуатируемые ошибки логики

2.2. Безвредные программные ошибки

Будучи людьми, программисты и другие разработчики допускают множество ошибок, многие из которых неумышленные и безвредные. Многие такие ошибки приводят к ошибкам исполнения в программе, но не ведут к более серьезным уязвимостям в безопасности. Однако некоторые классы ошибок докучали программистам и специалистам по безопасности в течение десятилетий, и нет ожидания, что они в скоро времени исчезнут.

Переполнение буфера

Переполнение буфера это компьютерный вариант попытки налить два литра воды в одно литровое ведро: часть воды прольется и причинит беспорядок.

Буфер это область памяти, в которой может располагаться информация. Так как память ограничена, то и буфер тоже ограничен. Во многих языках программирования необходимо ещё до исполнения программы задать максимальный размер буфера.

2.3. Вредоносный код

Сами по себе программы редко представляют угрозу безопасности. Программы оперируют данными, выполняя действия только тогда, когда данные и изменения состояние тригерят её. Большая часть работы, выполняемой программой, не видная для пользователя, так что они скорее всего не догадываются о вредоносных действиях.

Почему нам стоит беспокоиться о вредоносном коде?

Никто из нас не любит неожиданности, особенно в наших программах. Вредоносный код ведёт себя непредсказуемо, благодаря вредоносным намерениям разработавшего его программиста.

Вредоносный код может нанести много ущерба

Вредоносный код может делать что угодно с другими программами, например, выводить текст на экран, останавливать работающие программы, производить звуки или удалять сохраненные файлы. Или же вредоносный код может не делать ничего прямо сейчас; он будет тихо лежать, пока какое-то событие не заставит его действовать. Вредоносный код может даже выполнять разные действия в разное время.

Вредоносный код исполняется с пользовательскими правами. Таким образом, вредоносный код имеет доступ ко всему, к чему имеет доступ пользователь. Пользователи обычно имеют полный контроль над своим программным кодом и файлами с данными; они могут читать, писать, модифицировать, добавлять или удалять их. Вредоносный код может всё то же самое, но без пользовательского разрешение или ведома.

Вредоносный код может существовать долгое время

Вредоносный код вокруг нас, и нам важно понимать, как он выглядит и как работает, чтобы мы могли предпринимать шаги по предотвращению его от нанесения урона, или хотя бы снижения его уровня.