УДК 004.042

УЧЕТ ПРОБЛЕМ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Давыдова С.А., Григорьев М.Д.

ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Научный руководитель: Кривоносова Н.В.

ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

В работе рассмотрены подходы к разработке безопасного программного обеспечения. Кроме того, представлены основные проблемы безопасности при работе с программным обеспечением.

Информационная безопасность в наши дни с учетом глобальной цифровизации - это одна из наиболее важных задач при разработке программного обеспечения. Безусловно больше всего утечек информации происходит в среде передачи, но защита отправителя и получателя так же крайне важна. Все компоненты инфокоммуникационных сетей связи, включая программное обеспечение, работают с защищаемыми информационными активами с разной степенью секретности, поэтому разработка безопасного программного обеспечения - одно из важных направлений не только области программной инженерии, но и Национальной безопасности страны в целом.

Основной принцип при разработке безопасного ПО – учитывать требования безопасности на протяжении всего жизненного цикла разработки программ. Этапы жизненного цикла программы:

1. анализ требований
2. проектирование
3. кодирование (программирование)
4. тестирование и отладка
5. эксплуатация и сопровождение

Важно заранее анализировать и моделировать возможные угрозы и атаки на ПО и разрабатывать варианты защиты от них. Необходимо создавать определенные условия, для оценки рисков:

1. проводить различные виды тестирования (тестирование подсистемы безопасности и тестирование на граничные или близкие к граничным значения параметров);
2. определить специалистов в области безопасности ПО, которые будут участвовать в его разработке на протяжении всего цикла;
3. по формуле (SD3C), определить основные принципы разработки безопасного ПО.

Существует различные технологии для создания безопасного программного обеспечения, такие как шифрование, архитектура программного обеспечения, предполагающая безопасную передачу данных и др.

Шифрование используется для аутентификации источника информации и утверждения того, что информация отправлена конкретным лицом.

Архитектура программного продукта должна обеспечить безопасность функционирования системы при различных видах угроз и надежную защиту данных от ошибок проектирования, разрушения или потери информации. Так же базовые принципы разработки программного обеспечения должны обеспечить управление рабочей загрузкой, резервированием данных и вычислительных ресурсов, максимально быстрым восстановлением функционирования информационной системы.

При разработке программного обеспечения важно сделать акцент на безопасность(защиту) данных. Например, при разработке приложения, в котором предусмотрена регистрация пользователей, необходимо разработать правила, которые позволят совершать безопасную аутентификацию пользователей, а именно:

- при регистрации пользователь должен ввести пароль, который будет с помощью хэш-функции преобразовываться в набор битовых символов и уже полученный набор будет храниться в базе данных, что позволит защитить пользователей от несанкционированного доступа к данным пользователей;
- необходимо установить определенные критерии для задания пароля, например, пароль должен состоять из различных символов (буквы и цифры, символы), длина пароля не должна быть короткой, чтобы избежать создание слишком простых для взлома паролей, необходимо задавать длину количества символов;
- установить password field для ввода пароля пользователями, для исключения того, что третьи лица могут случайно увидеть вводимый пользователем пароль.

Так же, при разработке ПО необходимо провести ограничение в доступе получаемых данных на основе привилегий пользователя:

- при возникновении опасности получения доступа к конфиденциальным HTTP – данным или их модификациям, появляется необходимость настройки HTTP – сервера для использования закрытого ключа сертификата;
- при возникновении опасности просмотра, изменения конфиденциальных cookie-файлов – на веб-сайте потребуется добавить код для шифрования.

Уровень информационной безопасности зависит в первую очередь от защищенности каналов, по которым сведения из информационной базы компании могут попасть в сеть Интернет. Специально разрабатываемые программные средства, например, DLP-системы, способны перекрыть эти каналы и снизить риск утечки, похищения или несанкционированного доступа к информации.

Разработка и усовершенствование средств информационной безопасности не стоит на месте, т.к. возникают все новые и новые угрозы. И хотя, с некоторыми угрозами (хакеры, спамеры) есть способ борьбы и защиты, но сейчас при появлении такой темы как Интернет вещей, угроза информационной безопасности перешла на новый уровень.

Моделирование опасностей крайне важно при разработке ПО, без построения модели невозможно выяснить, устранены ли самые критичные опасности, грозящие приложению. Для каждого вида опасности с которым сталкиваются разработчики при проектировании ПО, должен быть проработан метод предотвращения данной угрозы.

Процесс модернизации систем, отвечающих за безопасность не должен останавливаться, а наоборот, постоянно улучшаться, таким образом не давай возможности и время злоумышленникам находить брешь в защитной системе и взламывать ее. Так же очень важно предотвращать как внешние угрозы, так и внутренние, к которым относятся ошибки и случайные утечки информации, связанные с человеческим фактором. Так же необходимо озаботится разделением уровнем полномочий, прав доступа к данным. Это поможет снизить круг лиц у которых есть доступ к наиболее важной информации.