УДК 00.004

Алексеев П.А., студент 1 курса,
факультет информационных технологий,
Брянский государственный технический университет,
г. Брянск, Россия

ШИФРОВАНИЕ – НЕ ПАНАЦЕЯ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В статье рассказывается о видах и способах шифрования, дается описание проблем шифрования.*

Ключевые слова: *шифрование, информационная безопасность, виды шифрования, аппаратные и программные уязвимости.*

Annotation. *The article talks about the most and methods of encryption, a description of encryption problems.*

Keywords: *encryption, information security, types of encryption, hardware and software vulnerabilities.*

Почему шифрование данных - не панацея | информационная безопасность

Шифрование данных – это их преобразование с целью сокрытия от не имеющих авторизации лиц, но в то же время предоставляющих доступ к ним авторизованным пользователям.

Виды и способы шифрования

Существуют три вида шифровки данных, позволяющих обеспечить значительный уровень их безопасности: аппаратное, программное, программно-аппаратное. Они защищают данные посредством применения криптографических алгоритмов, но отличаются друг от друга по способу выполнения функций шифрования или дешифровки.

При выборе одной из них необходимо опираться, прежде всего, на действительные потребности. Так программное шифрование будет дешевле аппаратного, но существенно уступит в уровне надежности. К тому же при задействии алгоритмов криптографии процессорные мощности будут использоваться различно: программное шифрование возьмет на себя процессор компьютера, в то время как у аппаратного шифратора есть свой процессор. При этом программное шифрование будет более целесообразно применять для личных компьютеров и в небольшом бизнесе, а для шифрования информации значительной важности или в корпоративных целях лучше остановить свой выбор на аппаратном.

Основными способами шифрования являются симметричное и асимметричное шифрования, хеширование, и цифровая подпись.

При использовании симметричного способа ключ для шифрования и дешифровки данных одинаков. После использования установленного для шифровки ключа, проходит дешифровка сообщения и далее формируется исходная строка. Для использования асимметричного шифрования требуется генерировать два математически связанных ключа. Один из них – приватный ключ, то есть доступ к нему есть только у использующего, а второй является открытым или общедоступным. В отличие от двух предыдущих способов, хеширование представляет собой одностороннюю функцию. Она в качестве входных данных принимает определенную информацию и выводит случайную строку, которая всегда будет иметь одинаковую длину. Цифровая подпись – это комбинация хеширования и асимметричного шифрования. При данном способе сообщения сначала хешируются, после чего проходят шифровку с применением приватного ключа отправителя.

Аппаратные и программные уязвимости от производителя оборудования

Возможность нарушить условия информационной безопасности обуславливается наличием уязвимостей в информационной системе. Они

характерны для объектов информатизации, неотделимы от них и определяются недостатками в процессе функционирования, особенностями архитектуры автоматизированных систем, спецификой протоколов обмена и интерфейсов, применяемых ПО и аппаратной платформой, а также условиями их эксплуатации и расположенности.

Ошибки, допущенные при проектировании, разработке и эксплуатации программно-аппаратного обеспечения, относятся к одной из самых распространенных причин возникновения уязвимостей.

Угрозы, характерные для аппаратной части:

1) Неправильное конфигурирование аппаратных средств – при слабой защите средств конфигурирования и отсутствии проверки корректности параметров аппаратная часть может быть настроена неправильно. Это может привести к отказу аппаратных средств или их физическому повреждению.

2) Несанкционированное использование закладок разработчиков присуще для аппаратных устройств, в низкоуровневое ПО которых заложена возможность обхода аутентификации с целью получения доступа к инженерным функциям.

3) Аппаратное прослушивание среды передачи данных характерно для распределенных систем, где не применяется криптографическая защита передаваемых данных или используются алгоритмы шифрования, обладающие недостаточной криптостойкостью.

Угрозы, присущие программному обеспечению информационных систем

1) Направленные на информацию, которая находится в памяти. Примером является переполнение буфера, при котором программа записывает данные за пределами выделенного буфера, из-за чего затираются данные за или перед его границами.

2) Связанные с корректностью входных данных – ошибки форматирующей строки могут встречаться в программах, которые используют вывод при

помощи строк, формируемых пользователями при отсутствии верификации введенных параметров.

3) Связанные с неустойчивыми состояниями – ошибки в отношении времени проверки ко времени использования характерны для таких систем, где проверка контроля доступа не атомарна по отношению к защищаемым действиям. Это дает возможность обойти контроль доступа.

4) Связанные с изменением уровня доступа. Пример такого типа угрозы – эскалация привилегий, основанная на обретении доступа к ресурсам, в обычных условиях недоступным для приложений и пользователя. Эта угроза характерна для операционных систем.

Современные проблемы шифрования данных

Несмотря на значительный прогресс в деле обеспечения безопасности данных, существует немало проблем при их шифровании. Прежде всего, это дороговизна, поскольку для проведения математических сложных операций по трансформации данных в ее ходе необходимы немалые ресурсы. Следующая трудность – непрозрачность, под которой подразумевается невозможность осуществить промежуточную проверку зашифрованных сведений без их полной дешифрации. Внедрение какой-либо организацией шифрования должно проводиться серьезно, неторопливо, и применяться в строгом соответствии с заранее подготовленным планом. Как и все прочие аспекты кибербезопасности, шифровка требует проведения скрупулезного анализа, планировки и протоколирования. Для дополнительных гарантий по обеспечению целостности данных может применяться резервное копирование.

В современный период проводятся исследования большого масштаба, посвященные проблемам безопасности, которые вызваны уязвимостями в программно-аппаратном обеспечении. Однако стоит помнить, что само по себе непрерывное совершенствование технологий безопасности в информационном мире не может предоставить абсолютные гарантии абсолютной защиты компьютерных систем.

Единственный возможный способ уменьшения вероятности использования уязвимостей в интересах злоумышленников базируется на реализации постоянного мониторинга защищенности, предполагающего отслеживании появления уязвимостей, своевременной установке обновлений, и применении инструментария противодействия.

Вывод

Итак, никакие аппаратные или программные решения не способны дать гарантии абсолютной надежности и безопасности данных. Вместе с тем минимизировать риск потерь вполне возможно, но для этого требуется комплексный подход к вопросам информационной безопасности. Одним из ключевых, но не единственным из методов ее реализации является шифрование данных, которое способно внести существенный вклад в ее обеспечение.

Источники:

1. Защита информации методом шифрования – Махамбаева И.У., Бексейтова А.Б., Кабдолдина Н.О., 2017 – стр 23-29.

2. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей – Федорченко А.В., Чечулин А.А., Котенко И.В., 2014 – стр 89-93.

3. Историко-правовой аспект обеспечения информационной безопасности – Слесарев Ю. В., 2019 – стр 38-45.