Методы и средства защиты программ

Проблема обеспечения целостности и достоверности элек­тронных данных включает в себя решение основных взаимосвя­занных задач: подтверждения их авторства и подлинности, контр­оль целостности данных. **Решение этих задач продиктовано необ­ходимостью защиты программного обеспечения от следующих злоумышленных действий:**

* внедрение в авторскую программу РПС или полная замене­на программы на программу-носитель РПС;
* изменение атрибутов (характеристик) программы;
* злоумышленник может выдать себя за настоящего владель­ца программы;
* отказ законного владельца программы от факта правообла-дания ею.

**Наиболее действенными способами защиты от подобных зло­умышленных действий предоставляют криптографические мето­ды защиты**. Это определено тем, что хорошо известные методы контроля целостности программ, основанные на контрольной сум­ме, продольном контроле и контроле на четность представляют сравнительно простые способы защиты от внесения изменений в код программ.

Для установления подлинности программ необходимо ис­пользовать более сложные способы, к которым относится аутен­тификация кода программ, с применением криптографических методов, которые выявляют следы, остающиеся после внесения преднамеренных искажений.

В первом случае аутентифицируемой программе ставится в со­ответствие некоторый аутентификатор, полученный при помощи стойкой криптографической функции, которой может быть крип­тографический стойкая хэш-функция или функция электронной цифровой подписи. И в том, и в другом случае доводами функции может быть как код аутентифицируемой программы, так и время и дата аутентификации, идентификатор программиста и/или органи­зации- разработчика программного обеспечения, какой-либо слу­чайный параметр и прочие. Также может использоваться любой симметричный шифр в режиме генерации имитовставки. Но, это потребует наличия секретного ключа при верификации программ на целостность, что бывает не всегда удобно и безопасно. А при использовании метода цифровой подписи при верификации необ­ходимо иметь только некоторую общедоступную информацию, например открытый ключ подписи. То есть контроль целостности программного обеспечения может осуществить любое заинтересо­ванное лицо, имеющий доступ к открытым ключам, используемой схемы цифровой подписи.

**Криптографические средства контроля целостности и до­стоверности программ**

**В криптографии действует следующие требования:**

* криптоаналитик имеет полный шифротекста;
* соблюдение правила Керкхоффа «стойкость шифра должна находить только секретностью его ключа».

В этом случае задача злоумышленника сводится к попытке раскрытия шифра на основе шифр текста. Если злоумышленник имеет к тому же некоторые отрывки открытого текста и соответст­вующие им элементы шифр текста, тогда он пытается выполнить атаку на основе открытого текста. Атака на основе выбранного открытого текста заключается в том, что злоумышленник, приме­няя свой открытый текст, получает правильный шифр и пытается в этом случае вскрыть шифр. Попытку обнаружения шифра мож­но осуществить, если злоумышленник подставляет свой ложный шифр текст, а при дешифровании получает необходимый для рас­крытия шифра открытый текст. Такой способ раскрытия называет­ся атакой на основе выбранного шифр текста.

**Теоретически существует абсолютно стойкийкод,** но единст­венным таким кодом является форма так называемой ленты од­нократного использования, в которой открытый текст «**объединя­ется**» с полностью случайным ключом такой же длины. Для абсо­лютной стойкости существенным является каждое из следующих требований к ленте однократного применения:

* полная случайность ключа;
* равенство длины ключа и длины открытого текста;
* однократность использования ключа.

**Но именно эти условия и делают абсолютно стойкий код очень ресурсозатратным и непрактичным. Прежде чем пользоваться та­ким кодом, необходимо обеспечить всех абонентов достаточным запасом случайных ключей и исключить возможность их повтор­ного применения.** А это сделать необычайно трудно и дорого. Вопрос о существовании односторонней функции с секретом яв­ляется столь же гипотетическим, что и вопрос о существовании односторонней функции. Для практических целей было построено несколько функций, которые могут оказаться односторонними, а это означает, что задача инвертирования эквивалентна некоторой давно изучаемой трудной математической задаче.

**Применение односторонних функций в криптографии позво­ляет:**

* организовать обмен шифрованными сообщениями с ис­пользованием только открытых каналов связи;
* решать новые криптографические задачи, такие как элек­тронная цифровая подпись.

**В большинстве схем электронной подписи используются хэш-функции**. Это объясняется тем, что практические схемы электрон­ной подписи не способны подписывать сообщения произвольной длины, а процедура, состоящая в разбиении сообщения на блоки и в генерации подписи для каждого блока по отдельности, крайне неэффективна. Под термином «**хэш**-**функция**» понимается функ­ция, отображающие сообщения произвольной длины в значение фиксированной длины, которое называется **хэш**-**кодом**. **К наибо­лее известным схемам цифровой подписи с прикладной точки зре­ния относятся схемы:**

* RSA, схемы Рабина-Уильямса;
* Эль-Гамаля, Шнорра;
* Фиата-Шамира;
* схема электронной цифровой подписи отечественного стандарта СТ РК 34.006-2002.

**Стойкость схемы цифровой подписи заключается в стойко­сти подписи в теоретико-сложностном смысле, указывающий на отсутствие эффективных алгоритмов ее подделки или раскрытия. Подразделяются атаки на следующие основные разновидности:**

* атака с открытым ключом, когда злоумышленник знает только открытый ключ схемы;
* атака на основе известного открытого текста (известно­го кода программы), когда злоумышленник получает под­писи для ограниченного количества известных ему кодов, но при этом злоумышленник никак не может повлиять на выбор этих кодов;
* атака на основе выбранного открытого текста, когда злоумышленник может получить подписи для некоторого ограниченного количества выбранных им кодов програм­мы (предполагается, что коды выбираются независимо от открытого ключа, например, до того как открытый ключ станет известен);
* направленная атака на основе выбранного открытого текста, когда злоумышленнику доступны подписи для не­которых кодов программ, причем выбирая код программы злоумышленник, уже знает открытый ключ;
* адаптивная атака на основе выбранного открытого тек­ста, когда злоумышленник выбирает коды программы по­следовательно, зная открытый ключ и зная на каждом шаге подписи для всех ранее выбранных кодов.

**Разновидности атак приведены по возрастающей степени на­несения ущерба владельцу программы.**

Угрозами для схем цифровой подписи являются раскрытие схемы или подделка подписи.**Определяются следующие типы уг­роз:**

* полного раскрытия, когда злоумышленник в состоянии вы­числить секретный ключ подписи;
* универсальной подделки, когда злоумышленник находит алгоритм, функционально эквивалентный алгоритму вычи­сления подписи;
* селективной подделки, когда осуществляется подделка под­писи для кода программы, выбранного злоумышленником априори;
* экзистенциональной подделки, когда осуществляется под­делка подписи хотя бы для одного кода программы, когда злоумышленник не контролирует выбор этого кода, которое может быть вообще случайным или бессмысленным.

**Разновидности угроз перечислены в порядке ослабления.** Стойкость схемы электронной подписи определяется относитель­но типов атаки и угрозы.

Принимая вышеописанную классификацию атаки и угрозы, можно сделать вывод, что наиболее привлекательной является схема цифровой подписи, стойкая против самой слабой из угроз, но предполагая, что злоумышленник может провести самую силь­ную из всех атак. Тогда, такая схема должна быть стойкой против экзистенциональной подделки с адаптивной атакой на основе вы­бранного открытого текста.

**Криптографические протоколы относятся к базовым объек­там изучений в криптологии и относятся к сравнительно новому направлению в криптографии. Но криптографические протоколы являются достаточно нетривиальным объектом исследований, и даже их формализация на сегодняшний день выглядит весьма за­труднительной.** Под криптографическим протоколом неформаль­но понимается распределенный алгоритм, т. е. совокупность алго­ритмов для каждого из участников вычислений, включая специфи­кации форматов сообщений, пересылаемых между участниками, спецификации синхронизации действий участников и описание действий при возникновении сбоев.

Объектом изучения теории криптографических протоколов являются удаленные абоненты, взаимодействующие по открытым каналам прием-передачи. Целью взаимодействия абонентов яв­ляется решение какой-то задачи. **Имеется также злоумышленник, который преследует собственные цели. При этом злоумышленни­ками могут быть один или даже несколько абонентов, вступивших в сговор.**

**Список использованной литературы**

1. Корнеев И.К. Защита информации в офисе: учебник / И. К. Кор-неев. Гос. ун-т управления. - М.: Проспект, 2008. - 336 с.
2. Кузнецов А.А. Защита деловой переписки (секреты безопасно­сти). - М.: Экзамен, 2008. - 239 с. - (Технология успеха).
3. Мельников В.П. Информационная безопасность и защита ин­формации : учебное пособие. ред. С. А. Клейменов. - 2-е изд., стер. - М.: Академия, 2007. - 336 с.
4. Шаньгин В.Ф. Комплексная защита информации в корпоратив­ных системах: учебное пособие / В. Ф. Шаньгин. - М.: ФОРУМ, 2010. -592 с.
5. О. А. Логачёв, А. А. Сальников, С. В. Смышляев, В. В. Ященко. Булевы функции в теории кодирования и криптологии. Изд. 2-е, доп. -М.: МЦНМО, 2012.
6. Введение в криптографию. Под общей редакцией В. В. Ященко.Издание 4-е, доп. - М.: МЦНМО, 2012.

Фамилия автора: Гайратбеков Арафат Жарасканович

Год: 2019

Город: Байконур

Категория: Информатика