36. Безопасность компьютерных систем. Концепция идентификации и проверки подленности в компьютерных системах. Протоколы с нулевой передачей знаний. Стеганография и стеганоанализ. Алгоритмы криптоанализа.

Безопасность компьютерных систем.

Информационная безопасность - состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Защита информации. **Целостность** информации; **Доступность** информации.
Аутентичность - возможность достоверно установить автора сообщения. **Апеллируемость** - возможность доказать, что автором является именно данный человек
Угроза информационной безопасности
Атака Нарушение Нарушитель Злоумышленник
Безопасность АИС: 1. **Внешняя** 2. **Внутренняя**
Меры противодействия угрозам безопасности: законодательные (правовые), **административные** (организационные), **процедурные** и **программно-технические.**
Криптографическая система — это система обеспечения информационной безопасности сети или АИС, использующая криптографические средства.
. **Шифрование** — это процесс преобразования исходного сообщения M (называемого открытым текстом) в форму M' (зашифрованный текст или шифртекст). При этом провести обратное преобразование M' в M возможно только обладая некоторой дополнительной информацией, называемой ключом.
Симметричное шифрование.
В симметричных алгоритмах шифрования один и тот же ключ K используется для того, чтобы зашифровать сообщение и для его последующей расшифровки. Таким образом, и отправитель и получатель сообщения должны располагать одним и тем же клю чом. Схематично это можно записать в виде:
M' = E(M, K) ; M = D(M', K), где E — функция шифрования (encrypt), а D — функция дешифрования (decrypt), обе используют ключ K в качестве одного из параметров.
Подстановочные алгоритмы шифрования работают по следующему принципу: каждый символ (или последовательность символов) исходного сообщения заменяются другим символом (или другой последовательностью символов). *Например: 1. Шифр Цезаря. 2. Моноалфавитный шифр (шифр простой замены)*
Перестановочные алгоритмы. (в лесу родилась елочка)
Шифрование с открытым ключом (Ассиметричные криптосистемы).
Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифровывания используются различные ключи:
• *открытый ключ K* используется для шифрования информации, вычисляется из секретного ключа *к*;
• *секретный ключ к* используется для расшифровывания информации, зашифрованной с помощью парного ему открытого ключа *K*.
Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ *к* из открытого ключа *K*. Поэтому открытый ключ *K* может свободно передаваться по каналам связи.
Концепция идентификации и проверки подленности в компьютерных системах. Информация, однозначно идентифицирующая объект компьютерной системы называется ее идентификатором (идентификатором объекта). Если объект имеет идентификатор, зарегистрированный в сети, то он является легальным объектом.

Идентификация объекта выполняется, в первую очередь, когда объект делает попытку войти в сеть. Если процедура завершается успешно, данный объект считается законным для данной сети. (Пользователь

сообщает системе, по её запросу, своё имя - идентификатор).

Аутентификация объекта (проверка подлинности) устанавливает, является ли данный объект именно таким, каким он себя объявляет. (Пользователь подтверждает идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе - пароль).

После установления соединения необходимо обеспечить выполнение следующих требований защиты:

1. Получатель должен быть уверен в подлинности источника данных.

2. Получатель должен быть уверен в подлинности передаваемых данных.

3. Отправитель должен быть уверен в доставке данных получателю.

4. Отправитель должен быть уверен в подлинности доставленных данных.

Требования 1 и 2 выполняются при использовании ЭЦП, требования 3 и 4 при использовании уведомлений о вручении с ЭЦП.

Прежде чем получить доступ к компьютерной системе, необходимо пройти идентификацию и аутентификацию, для этого необходимо:

1. Наличие соответствующего субъекта (модуля аутентификации).

2. Наличие аутентифицирующего объекта, хранящего уникальную информацию для аутентификации пользователя.

Различают две формы представления объекта, аутентифицирующие пользователя:

1. Внешний аутентифицирующий объект, не принадлежащий системе.

2. Внутренний объект, принадлежащий системе, на который переносится информация из внешнего объетка.

8.2. Типовые схемы идентификации и аутентификации пользователя.

n пользователей, i-й аутентифицирующий объект i-го пользователя содержит два поля

неизменный идентификатор i-го пользователя.

идентифицирующая информация пользователя.

Описанная структура соответствует практически любому ключевому носителю. Совокупность информации на ключевом носителе можно назвать первичной аутентифицирующей информацией. Внутренний аутентифицирующий объект в открытом виде не должен существовать в системе длительное время. Для длительного хранения следует использовать данные в защищенной форме.

Схема 1: В системе выделяется некоторый объект-эталон для идентификации и аутентификации пользователей.

номер пользователя информация для идентификации информация для аутентификации

вычисляется по формуле

Функция обладает свойством невосстановимости значения по известным и

Схема протокола:

1. Пользователь предъявляет свой идентификатор id.

2. Если идентификатор не совпадает ни с одним из идентификаторов, регистрируемых в системе, то идентификация отвергается.

3. Субъект аутентификации запрашивает у пользователь его аутентификатор k.

4. Субъект аутентификации вычисляет значения

5. Субъект аутентификации производит сравнение значений

Схема 2. Объект-эталон имеет следующую структуру

случайный вектор, задаваемый при создании пользователя

Протокол:

1. Пользователь предъявляет свой идентификатор.

2. В случае совпадения - идентифицируется, в случае несовпадения - нет.

3. Идентификатору выделяется вектор.

4. Субъект аутентификации запрашивает у пользователя аутентификатор k.

5. Субъект аутентификации вычисляет

6. Сравнение значений.

Схема подтверждения подлинности с использованием пароля.

Схема аутентификации с помощью пароля с использованием идентификационной таблицы

1. **Протоколы с нулевой передачей знаний.**

5.4. Протоколы идентификации с нулевой передачей знаний

Широкое распространение интеллектуальных карт (смарт-карт) для разнообразных коммерческих, гражданских и военных применений (кредитные карты, карты социального страхования, карты доступа в охраняемое помещение, компьютерные пароли и ключи, и т. п.) потребовало обеспечения безопасной идентификации таких карт и их владельцев. Во многих приложениях главная проблема заключается в том, чтобы при предъявлении интеллектуальной карты оперативно обнаружить обман и отказать обманщику в допуске, ответе или обслуживании.

Для безопасного использования интеллектуальных карт разработаны протоколы идентификации с нулевой передачей знаний [121]. Секретный ключ владельца карты становится неотъемлемым признаком его личности. Доказательство знания этого секретного ключа с нулевой передачей этого знания служит доказательством подлинности личности владельца карты.

Упрощенная схема идентификации с нулевой передачей знаний

Схему идентификации с нулевой передачей знаний предложили в 1986 г. У. Фейге, А. Фиат и А. Шамир. Она является наиболее известным доказательством идентичности с нулевой передачей конфиденциальной информации.

Рассмотрим сначала упрощенный вариант схемы идентификации с нулевой передачей знаний для более четкого выявления ее основной концепции. Прежде всего выбирают случайное значение модуля n, который является произведением двух больших простых чисел. Модуль n должен иметь длину 512…1024 бит. Это значение n может быть представлено группе пользователей, которым придется доказывать свою подлинность. В процессе идентификации участвуют две стороны:

- сторона A, доказывающая свою подлинность,
- сторона B, проверяющая представляемое стороной A доказательство.

Для того чтобы сгенерировать открытый и секретный ключи для стороны A, доверенный арбитр (Центр) выбирает некоторое число V, которое является квадратичным вычетом по модулю n. Иначе говоря, выбирается такое число V, что сравнение

$$x^2 \equiv V (\mathrm{mod}\ n)$$

имеет решение и существует целое число

$$V^{-1} \bmod n.$$

Выбранное значение V является *открытым ключом* для A. Затем вычисляют наименьшее значение S, для которого

$$S \equiv \mathrm{sqrt}\,(V^{-1})\ (\mathrm{mod}\ n).$$

Это значение S является *секретным ключом* для A.

Теперь можно приступить к выполнению протокола идентификации.

1. Сторона A выбирает некоторое случайное число r, $r < n$. Затем она вычисляет

$$x = r^2 \bmod n$$

и отправляет x стороне B.

2. Сторона B посылает A случайный бит b.

3. Если $b = 0$, тогда A отправляет r стороне B. Если $b = 1$, то A отправляет стороне B

$$y = r * S \bmod n.$$

4. Если $b = 0$, сторона B проверяет, что

$$x = r^2 \bmod n,$$

чтобы убедиться, что A знает sqrt(x). Если $b = 1$, сторона B проверяет, что

$$x = y^2 * V \bmod n,$$

чтобы быть уверенной, что A знает $\mathrm{sqrt}(V^{-1})$.

Эти шаги образуют один цикл протокола, называемый *аккредитацией*. Стороны A и B повторяют этот цикл t раз при разных случайных значениях r и b до тех пор, пока B не убедится, что A знает значение S.

Если сторона A не знает значения S, она может выбрать такое значение r, которое позволит ей обмануть сторону B, если B отправит ей $b = 0$, либо A может выбрать такое r, которое позволит обмануть B, если B отправит ей $b = 1$. Но этого невозможно сделать в обоих случаях. Вероятность того, что A обманет B в одном цикле, составляет 1/2. Вероятность обмануть B в t циклах равна $(1/2)^t$.

Для того чтобы этот протокол работал, сторона A никогда не должна повторно использовать значение r. Если A поступила бы таким образом, а сторона B отправила бы стороне A на шаге 2 другой случайный бит b, то B имела бы оба ответа A. После этого B может вычислить значение S, и для A все закончено.

2. **Стеганография и стеганоанализ.**

Стеганогра́фия (от греч. στεγανός — скрытый + γράφω — пишу; буквально «тайнопись») — способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). Этот термин ввел в 1499 году Иоганн Тритемий в своем

трактате «Стеганография» (*Steganographia*), зашифрованном под магическую книгу.

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо или судоку. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых запрещена криптография[1]. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

Стеганоанализ – это выявление стеганографии, принципы и методы. Исследователи А.С. Сизова, Е.И. Никутина, С.В. Котенко, предлагая новые методы стегоанализа, уделяют внимание именно методам, предназначенным для решения первичной задачи стегоанализа – задачи обнаружения факта присутствия скрытой информации [3]. В связи с этим выделяются следующие методы стеганографического анализа:

- статистические;
- сигнатурные;
- целенаправленные;
- слепые;
- количественные.

Статистические методы стегоанализа основываются на анализе таких статистических характеристиках, как коэффициенты корреляции, оценки энтропии, условные распределения, вероятности появления и зависимости между элементами последовательностей и др.

Сигнатурные методы стегоанализа основываются на поиске предопределённых сигнатур – последовательностей битов, с высокой вероятностью указывающих на присутствие в анализируемом файле информации, скрытой соответствующей стегосистемой.

Целенаправленные методы стегоанализа используют знания о методах стеганографического скрытия информации и опираются на концепцию различающих статистик.

3. Алгоритмы криптоанализа.

Основные методы криптоанализа:

- Атака на основе шифротекста
- Атака на основе открытых текстов и соответствующих шифротекстов
- Атака на основе подобранного открытого текста (возможность выбрать текст для шифрования)
- Атака на основе адаптивно подобранного открытого текста

Дополнительные методы криптоанализа:

- Атака на основе подобранного шифротекста
- Атака на основе подобранного ключа
- Бандитский криптоанализ

Атаки на основе шифротекста

Допустим, криптоаналитик обладает некоторым числом шифротекстов, полученных в результате использования одного и того же алгоритма шифрования. В этом случае криптоаналитик может совершить только атаку на основе шифротекста. Целью криптографической атаки в этом случае является нахождение как можно большего числа открытых текстов, соответствующих имеющимся шифротекстам, или, что ещё лучше, нахождение используемого при шифровании ключа.

Входные данные для подобного типа атак криптоаналитик может получить в результате простого перехвата зашифрованных сообщений. Если передача осуществляется по открытому каналу, то реализация задачи по сбору данных сравнительно легка и тривиальна. Атаки на основе шифротекста являются самыми слабыми и неудобными.

Атака на основе открытых текстов и соответствующих шифротекстов

Пусть в распоряжении криптоаналитика есть не только шифротексты, но и соответствующие им открытые тексты.

Тогда существуют два варианта постановки задачи:

Найти ключ, использованный для преобразования открытого текста в шифротекст

Создать алгоритм, способный дешифровать любое сообщение, закодированное с помощью этого ключа

Получение открытых текстов играет решающую роль в осуществлении этой атаки. Открытые тексты извлекают из самых различных источников. Так, например, можно догадаться о содержимом файла по его расширению.

В случае взлома переписки можно сделать предположение, что письмо имеет структуру типа:

- «Приветствие»
- «Основной текст»
- «Заключительная форма вежливости»
- «Подпись»

Следовательно, атака может быть организована путём подбора различных видов «Приветствия» (например, «Здравствуйте!», «Добрый день» и т. д.) и/или «Заключительной формы вежливости» (таких как «С уважением», «Искренне Ваш» и т. п.). Легко заметить, что данная атака сильнее атаки на основе одного лишь шифротекста.

Атака на основе подобранного открытого текста

Для осуществления такого типа атаки криптоаналитику необходимо иметь не только какое-то количество открытых текстов и полученных на их основе шифротекстов. Помимо прочего в данном случае криптоаналитик должен обладать возможностью подобрать несколько открытых текстов и получить результат их шифрования.

Задачи криптоаналитика повторяют задачи для атаки на основе открытого текста, то есть получить ключ шифрования, либо создать дешифрующий алгоритм для данного ключа.

Получить входные данные для такого вида атаки можно, например, следующим образом:

Создать и отправить поддельное не зашифрованное сообщение якобы от одного из пользователей, которые обычно пользуются шифрованием.

В некоторых случаях можно получить ответ, в котором будет содержится зашифрованный текст, цитирующий содержание поддельного сообщения.

При осуществлении атаки подобного типа криптоаналитик имеет возможность подбирать блоки открытого текста, что при определённых условиях может позволить получить больше информации о ключе шифрования.

Атаки на основе адаптивно подобранного открытого текста

Атака такого типа является более удобным частным случаем атаки на основе подобранного открытого текста. Удобство атаки на основе адаптивно подобранного открытого текста состоит в том, что помимо возможности выбирать шифруемый текст, криптоаналитик может принять решение о шифровании того или иного открытого текста на основе уже полученных результатов операций шифрования. Другими словами, при осуществлении атаки на основе подобранного открытого текста криптоаналитик выбирает всего один большой блок открытого текста для последующего шифрования, а потом на основе этих данных начинает взламывать систему. В случае организации адаптивной атаки криптоаналитик может получать результаты шифрования любых блоков открытого текста, чтобы собрать интересующие его данные, которые будут учтены при выборе следующих отправляемых на шифрование блоков открытого текста и так далее. Наличие обратной связи даёт атаке на основе адаптивно подобранного шифротекста преимущество перед всеми вышеперечисленными типами атак.