Мы живем в информационную эпоху. Мы должны внимательно сохранять информацию о каждом аспекте нашей жизни. Другими словами, *информация* — собственность, и, подобно любой другой собственности, имеет важное *значение*. И в этом качестве *информация* должна быть защищена от нападений.

Информация должна быть сохранена от неправомочного доступа (*конфиденциальность*), защищена от неправомочного изменения (*целостность*) и доступна только разрешенному объекту, когда это ему необходимо (*доступность*).

Несколько десятилетий назад *информация* собиралась на физических носителях. *Конфиденциальность* этих носителелй достигалась строгим ограничением доступа, который предоставлялся только людям, имеющим на это право, и тем из них, кому можно было доверить эту информацию. Также нескольким правомочным субъектам разрешалось изменение содержания этих файлов. Готовность была обеспечена тем, что по меньшей мере одному человеку всегда разрешался *доступ* к этим носителям.

С появлением компьютеров хранение информации стало электронным. *Информация* хранилась уже не в физической неэлектронной среде — она накапливалась в электронной среде (компьютерах). Однако три *требования безопасности* не изменились. Файлы, записанные в компьютере, требовали конфиденциальности, целостности и доступности. Реализация этих требований возможна различными методами и требует решения сложных задач.

В течение прошлых двух десятилетий *компьютерные сети* произвели революцию в использовании информации. *Информация* теперь распределена. Люди при наличии полномочий могут передавать информацию и искать ее на расстоянии, используя *компьютерные сети*. Но три уже упомянутых требования — конфиденциальности, целостности и доступности — не изменились. Они лишь приобрели некоторые новые аспекты. Теперь недостаточно того, что *информация* должна быть конфиденциальной, когда она сохраняется в компьютере. Должен также существовать способ поддержки конфиденциальности, когда эта *информация* передается от одного компьютера к другому.

В этой лекции мы сначала обсуждаем три главных цели поддержки *безопасности информации*.

Когда будет понятно, какие атаки могут угрожать этим трем целям, тогда можно обсудить службы безопасности, предназначенные для этих целей. Потом определяются *механизмы* обеспечения службы безопасности и методы, которые могут использоваться, чтобы осуществить эти *механизмы*.

1.1. Цели поддержки безопасности

Рассмотрим **три цели поддержки информационной безопасности: конфиденциальность, целостность и готовность**.

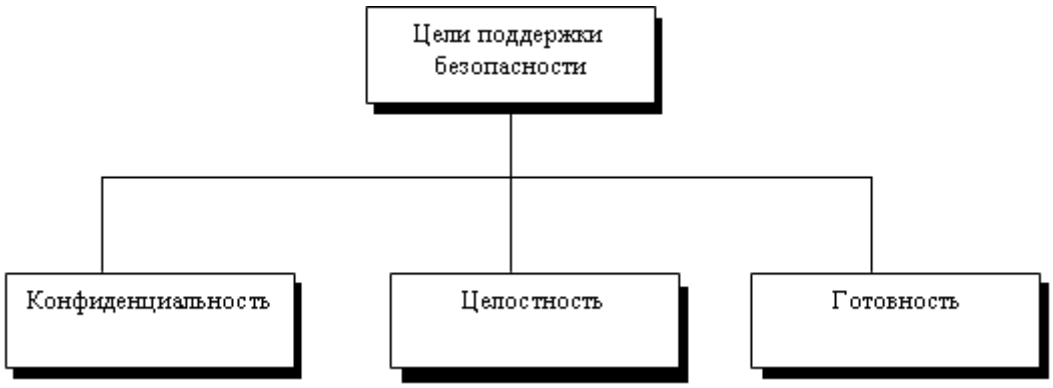


Рис. 1.1. Систематизация целей поддержки безопасности

Конфиденциальность

Конфиденциальность — вероятно, самый общий аспект информационной безопасности. Мы должны защитить нашу конфиденциальную информацию. Организация должна принять меры против тех злонамеренных действий, которые могут нарушить конфиденциальность информации. В военных организациях сохранение секретности важной информации – главная забота руководства. В промышленности сохранение тайны некоторой информации от конкурентов является одним из основных факторов работы организации. В банковском деле должна сохраняться секретность учетных записей клиентов.

Как мы увидим позже в этой лекции, конфиденциальность нужна не только при хранении информации, она также необходима при ее передаче. Когда мы передаем часть информации, которая должна будет

храниться в удаленном компьютере, или когда мы отыскиваем информацию, которая находится в удаленном компьютере, мы должны гарантировать ее секретность в течение передачи.

Целостность

Потребители изменяют информацию постоянно. В банке, когда клиент вносит или снимает деньги, баланс на его счету должен быть изменен. **Целостность** означает, что изменения должны быть сделаны только разрешенными объектами и с помощью разрешенных механизмов. *Нарушение целостности* — не обязательно результат злонамеренного действия; сбой в системе, такой, например, как всплеск или прерывание мощности в *первичной сети* электропитания, может привести к нежелательным изменениям некоторой информации.

Готовность

Третий компонент информационной безопасности — **готовность**. Информация, созданная и сохраненная организацией, должна быть доступна разрешенным объектам. Информация бесполезна, если она не доступна. Информация должна постоянно изменяться, и поэтому тоже должна быть доступна для разрешенных объектов. Неготовность информации столь же вредна для организации, как отсутствие конфиденциальности или целостности. Вообразите, что случилось бы с банком, если клиенты не могли бы обратиться к своим счетам для снятия или вклада денег.

1.2. Атаки

Нашим трем целям информационной безопасности — конфиденциальности, целостности и готовности — могут угрожать **атаки с целью нарушения** *безопасности информации*. Хотя в литературе встречаются различные подходы к систематизации атак, мы сначала разделим их на три группы, связанные с целями нарушения информационной безопасности. Позже мы будем делить их на две широких категории, основанные на эффективности их воздействия на систему. Рисунок 1.2 показывает первую систематизацию.

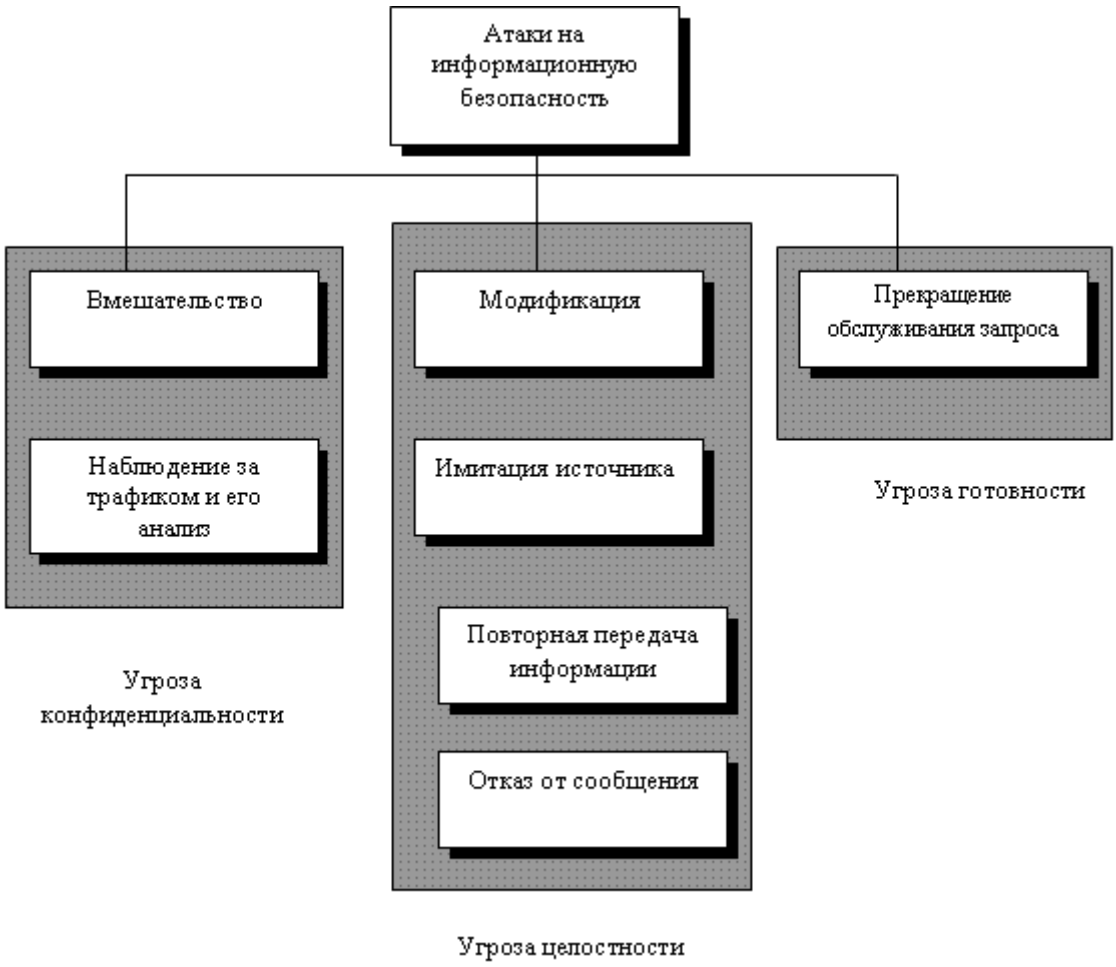


Рис. 1.2. Систематизация атак и соотношение их с целями поддержки информационной безопасности

Атаки, угрожающие конфиденциальности

Вообще, имеется два типа атак, которые угрожают конфиденциальности информации: **вмешательство и наблюдение за трафиком и его анализ**.

Вмешательство

Вмешательство относится к неправомочному доступу или *перехвату данных*. Например, файл, передаваемый через Интернет, может содержать конфиденциальную информацию. Объект, не имеющий полномочий, может прервать передачу и использовать передаваемую информацию для собственной выгоды. Чтобы предотвратить вмешательство, данные могут быть представлены так, что перехвативший не сможет понять их. Для этого применимы методы шифрования, приводимые в этом курсе.

Наблюдение за трафиком и его анализ

Хотя *шифрование данных* может сделать их непонятными для злоумышленника, он, анализируя сетевой трафик, может получить некоторую другую информацию. Например, он может найти электронный адрес (адрес электронной почты) передатчика или приемника. Он может также собрать пары запросов и ответов, что поможет ему понять активность действий наблюдаемой организации.

Атаки, угрожающие целостности

Целостности данных можно угрожать несколькими видами атак, такими как **модификация, имитация источника, повторная передача информации и отказ от сообщения**.

Модификация

После прерывания или доступа к информации атакующий изменяет информацию с определенной выгодой для себя. Например, клиент передает сообщение банку, чтобы провести некоторую операцию. Атакующий прерывает сообщение и изменяет тип операции, чтобы принести этим пользу себе. Обратите внимание, что иногда атакующий просто удаляет или задерживает сообщение, чтобы навредить системе или извлечь выгоду из самого факта задержки операции.

Имитация источника

Имитация источника (*spoofing*) заключается в том, что атакующий имитирует кого-то, кто имеет право на производимые действия. Например, атакующий захватывает банковскую кредитную карточку и *PIN*-код клиента банка. Он может действовать как настоящий клиент. Иногда атакующий имитирует приемник. Например, пользователь хочет войти в контакт с банком, но ему предоставляется другой сайт, который имитирует, что это – банк, и атакующий получает необходимую ему информацию от пользователя.

Повторная передача информации

Другой вид атаки — повторная передача информации (*атака воспроизведения*). Атакующий получает копию сообщения, передаваемого пользователем, и передает эту копию с целью дезорганизации процесса или попыток повторить его. Например, человек передает запрос банку, чтобы оплатить работу своему сотруднику. Атакующий перехватывает сообщение и передает его снова, чтобы получить оплату этой работы от этого банка еще раз (повторно).

Отказ от сообщения

Этот тип атак отличается от других, потому что это действие может быть выполнено одной из двух сторон связи: передатчиком или приемником. Передатчик сообщения может отказаться и отрицать факт передачи сообщения. Другой вариант — когда приемник сообщения отрицает, что он получил сообщение. Пример отказа от сообщения передатчика: клиент банка передал запрос банку на перевод некоторой суммы денег третьему лицу, но впоследствии отрицает, что он сделал такой запрос. Пример опровержения сообщения приемником: человек, который покупает изделие у изготовителя и платит за это с помощью электроники, но изготовитель позже отрицает, что получил оплату, и просит оплатить покупку.

Атаки, угрожающие готовности

Рассмотрим только одну атаку, угрожающую готовности: **отказ в обслуживании**.

Отказ в обслуживании

Отказ в обслуживании (*Denial* of Service — DoS) — очень общее название атаки. Она может замедлить или полностью прервать обслуживание системы. Атакующий может использовать несколько стратегий, чтобы достигнуть этого. Атакующий может передать так много фиктивных запросов серверу, что это приведет к сбою сервера из-за высокой нагрузки. Атакующий может также прервать и удалить ответ сервера клиенту, порождая у клиента впечатление, что сервер не отвечает. Атакующий может прервать запросы от клиентов, порождая у клиента уверенность, что сервер не отвечает. Атакующий может прерывать запросы клиентов, заставляя клиентов передать запросы много раз и перезагружать систему.

Пассивные и активные атаки

Давайте теперь разделим атаки на две группы: **пассивные** и **активные**. Таблица 1.1 показывает соотношения между этим делением и предыдущей классификацией.

Пассивные нападения

При пассивном нападении *цель атакующего* состоит в том, чтобы только получить информацию. Это означает, что нападение не изменяет данные и не повреждает систему. Система продолжает нормально работать. Однако атака может нанести вред передатчику или приемнику сообщения. Атаки, которые

угрожают конфиденциальности — вмешательство и наблюдение за трафиком плюс его анализ, — являются пассивными. *Раскрытие информации* может вредить передатчику или приемнику сообщения, но систему не затрагивает. По этой причине трудно обнаружить этот тип нападения, пока передатчик или приемник не узнают об утечке конфиденциальной информации. Пассивные нападения, однако, могут быть предотвращены *шифрованием данных*.

Таблица 1.1. Классификация пассивных и активных атак

Атаки	Пассивные / Активные	Угроза
Вмешательство	Пассивные	Конфиденциальности
Наблюдение за трафиком и его анализ		
Модификация	Активные	Целостности
Имитация источника		
Повторная передача информации		
Отказ от сообщения		
Отказ в обслуживании	Активные	Готовности

Активные атаки

Активные атаки изменяют данные или повреждают систему. Атаки, которые угрожают целостности или готовности, — активные. *Активные атаки* обычно легче обнаруживаются, чем предотвращаются, потому что атакующий может начинать их разнообразными методами.

1.3. Услуги и механизмы

Международный Союз Электросвязи, Секция Стандартов по телекоммуникации (ITU-T) (см. *приложение* B) разработал стандарты некоторых служб безопасности и некоторые *механизмы* для осуществления этих услуг. Службы информационной безопасности и *механизмы* близко связаны, потому что механизм или комбинация механизмов применяются, чтобы обеспечить обслуживание. Механизм может использоваться в одной или нескольких услугах. Ниже эти *механизмы* кратко обсуждаются, чтобы понять их общую идею. Далее они будут рассмотрены более подробно.

Услуги информационной безопасности

ITU-T (X.800) определил пять услуг, связанных с целями информационной безопасности и атаками, типы которых мы определили в предыдущих секциях. Рисунок 1.3 показывает классификацию пяти общих услуг.

Рис. 1.3. Услуги информационной безопасности

Чтобы предотвратить атаки на информационную безопасность, о которых мы говорили, надо просто иметь одну или больше показанных выше услуг для одного или большего количества целей информационной безопасности.

Конфиденциальность данных

Конфиденциальность данных разработана, чтобы защитить данные от попытки их раскрытия. Эта широкая услуга, определенная в рекомендации *ITU*-T X.800. Она может охватывать конфиденциальность

целого сообщения или его части, а также защищает от наблюдения за трафиком и его анализа — собственно, она разработана для предотвращения вмешательства и наблюдения за трафиком.

Целостность данных

Целостность данных разработана для защиты данных от модификации, вставки, удаления и повторной передачи информации противником. Она может защищать целое сообщение или часть сообщения.

Установление подлинности (аутентификация)

Эта услуга обеспечивает **установление подлинности (аутентификацию)** оператора на другом конце линии. При соединении, ориентированном на подключение, она обеспечивает установление подлинности передатчика или приемника в течение установления соединения (*установление подлинности объектов* равного уровня). При соединении без установления подключения она подтверждает подлинность источника данных (установление подлинности происхождения данных).

Исключение отказа от сообщений

Услуга **исключение отказа от сообщений** защищает от отказа от сообщения передатчиком или приемником данных. При исключении отказа от сообщения передатчиком приемник данных может потом доказать происхождение сообщения, используя опознавательный код (идентификатор) передатчика. При исключении отказа от сообщений приемником передатчик, используя подтверждение доставки, может потом доказать, что данные доставлены предназначенному получателю.

Управление доступом

Управление доступом обеспечивает защиту против неправомочного доступа к данным. *Доступ* в этом определении — термин очень широкий и может включать чтение, запись, изменение данных, запуск выполнения программы и так далее.

Механизмы безопасности

Для обеспечения услуг информационной безопасности *ITU*-T (X.800) рекомендует некоторые **механизмы безопасности**, определенные в предыдущей секции. Рисунок 1.4 дает классификацию этих механизмов.

Рис. 1.4. Механизмы информационной безопасности

Шифрование

Шифрование. Засекречивая или рассекречивая данные, можно обеспечить конфиденциальность. Шифрование также дополняет другие механизмы, которые обеспечивают другие услуги. Сегодня для шифрования используются два метода: криптография и стеганография — тайнопись (*steganography*). Мы коротко обсудим их в дальнейшем.

Целостность данных

Механизм **целостности данных** добавляет в конце данных короткий контрольный признак (check value), который создается *определенным процессом* отдельно от данных. Приемник получает данные и контрольный признак. На основании полученных данных он создает новый контрольный признак и сравнивает только что созданный с полученным. Если эти два контрольных признака совпадают, *целостность данных* была сохранена.

Цифровая подпись

Цифровая подпись — средство, которым отправитель может с помощью электроники подписать данные, а приемник может с помощью компьютера проверить подпись. Отправитель использует процесс, который может указать, что эта подпись имеет частный ключ, выбранный из общедоступных ключей, которые были объявлены публично для общего пользования. Приемник использует общедоступный ключ отправителя, чтобы доказать, что сообщение действительно подписано отправителем, который утверждает, что послал сообщение.

Обмен сообщениями для опознавания

При **обмене сообщениями для опознавания** два объекта обмениваются некоторыми сообщениями, чтобы доказать, что эти объекты известны друг другу. Например, одно юридическое лицо может доказать, что оно знает тайный признак, который только оно может знать (скажем, последнее место встречи с партнером).

Заполнение трафика

Заполнение трафика означает возможность вставлять в трафик данных некоторые фиктивные данные, чтобы сорвать попытки злоумышленников использовать его для анализа.

Управление маршрутизацией

Управление маршрутизацией означает выбор и непрерывное изменение различных доступных маршрутов между отправителем и приемником для того, чтобы препятствовать противнику в перехвате информации на определенном маршруте.

Доверенность

Доверенность означает выбор третьей стороны, с целью доверить ей контроль обменом между двумя объектами. Это может быть сделано, например, для того, чтобы предотвратить отказ от сообщения. Приемник может вовлечь третью сторону, которой можно доверить хранение запросов отправителя, и тем самым предотвратить последующее отрицание отправителем факта передачи сообщения.

Контроль доступа

Контроль доступа использует методы доказательства, что пользователь имеет право доступа к данным или ресурсам, принадлежащим системе. Примеры такого доказательства — пароли и *PIN*-коды.

Соотношение между услугами и механизмами

Таблица 1.2 показывает соотношение между услугами и механизмами информационной безопасности. Таблица приводит три механизма (шифрование, *цифровая подпись* и *обмен сообщениями* для опознавания), которые могут использоваться для того, чтобы обеспечить удостоверение подлинности. Таблица также показывает, что шифрование может использоваться при трех услугах (конфиденциальности данных, *целостности данных* и аутентификации).

Таблица 1.2. Соотношение между услугами безопасности и механизмами обеспечения безопасности

Услуга безопасности	Механизм обеспечения безопасности
Конфиденциальность данных	Шифрование и *управление маршрутизацией*
Целостность данных	Шифрование, *цифровая подпись*, контрольные признаки *целостности данных*

Проверка полномочий	Шифрование, *цифровая подпись*, установление правомочности изменений
Исключение отказа от сообщений	*Цифровая подпись*, *целостность данных* и *доверенность*
Управление доступом	Механизм управления доступом

1.4. Методы

Механизмы, которые мы рассмотрели в предыдущих секциях, — это только теоретические рецепты. Для реализации информационной безопасности требуется небольшое число методов. Два из них наиболее распространены: один общий (*криптография*) и один специфический (стеганография).

Криптография

Некоторые механизмы информационной безопасности, перечисленные в предыдущей секции, могут быть реализованы с помощью криптографии. **Криптография**, слово с греческим происхождением, означает "тайна написанного". Однако мы используем этот термин, чтобы обозначить науку и искусство преобразования сообщений, которые делают их безопасными и придают иммунитет к атакам. Хотя в прошлом криптография заключалась только в шифровании и *дешифровании* сообщений с применением секретных ключей, сегодня она определяется как совокупность трех различных механизмов: шифрование *симметричными ключами*, шифрование асимметричными ключами и хэширование. Ниже кратко рассмотрим эти три механизма.

Шифрование симметричными ключами

Шифрование симметричными ключами иногда называют шифрованием с секретным ключом или криптографией с секретным ключом. Например, объект, назовем его Алиса, может передать сообщение другому объекту, который называется Боб, по опасному каналу, для того, чтобы ее противник, который называется Ева, не смог понять содержание сообщения, просто подслушав его по каналу. Алиса зашифровала сообщение, используя алгоритм шифрования; Боб расшифровывает сообщение, используя алгоритм расшифровки. В шифровании *симметричными ключами* применяется единственный **ключ засекречивания** и для шифрования, и для расшифровки. Шифрование/дешифрование можно представить как электронный замок. При шифровании симметричным ключом Алиса помещает сообщение в блок и закрывает блок, используя совместный ключ засекречивания; Боб отпирает замок другим экземпляром того же ключа и извлекает сообщение.

Шифрование асимметричными ключами

При шифровании асимметричными ключами (иногда называемом шифрованием с открытыми ключами или криптографией с открытыми ключами) мы имеем ту же самую ситуацию, что и при шифровании *симметричными ключами*, но с небольшой разницей. Во-первых, мы имеем два ключа вместо одного: из них один **открытый ключ (public key)**, другой — индивидуальный или **секретный (private key)**. Для того чтобы передать защищенное сообщение Бобу, Алиса сначала зашифровала сообщение, используя открытый ключ Боба. Чтобы расшифровывать сообщение, Боб использует свой собственный секретный ключ.

Хэширование

При **хэшировании** из сообщения переменной длины может быть создан *дайджест* фиксированной длины, обычно намного меньшего размера, чем исходное сообщение. Сообщение и *дайджест* нужно передать Бобу. *Дайджест* используется, чтобы обеспечить проверку *целостности данных*, которая обсуждалась раньше.

Стеганография

Хотя эта книга базируется на криптографии как методике реализации *механизмов безопасности*, но все же кратко рассмотрим другую методику, которая в прошлом использовалась для засекречивания связи. В настоящее время она — стеганография — снова восстанавливается. Это слово происходит от греческого названия и означает "закрытую запись", в отличие от криптографии, означающей "секретную запись". Криптография скрывает содержание сообщение путем шифрования. Стеганография скрывает само сообщение непосредственно, закрывая его чем-нибудь.

Исторические примеры использования

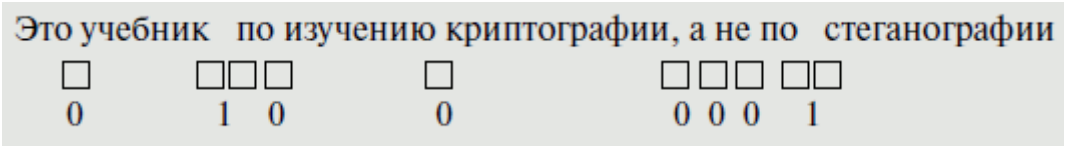
История полна фактов и мифов об использовании стеганографии. В Китае военные сообщения писались на кусках тончайшего шелка и закатывались в маленький шар, который глотал посыльный. В Риме и Греции сообщения вырезались на кусочках древесины, которые потом опускались в воск, чтобы закрыть запись. Также использовались невидимые чернила (такие как луковый сок или соли аммиака) для записи секретного сообщения между строками безобидного текста или в конце бумаги; секретное сообщение выступало, когда эта бумага нагревалась или обрабатывалась каким-то веществом.

Недавно были изобретены другие методы. В некоторые безобидные письма могли бы быть записаны сообщения поверх письма карандашом, след которого видим только тогда, когда текст помещен под яркий источник света под углом. Нулевые шифры использовались, чтобы скрыть секретное сообщение в безвредном сообщении. Например, секретное сообщение можно составить, если первая или вторая буква в каждом слове бесполезна, а только закрывает истинное сообщение. Микроточки также применялись для этой цели. Секретные сообщения были сфотографированы и уменьшены до размера точки и вставлялись в простые сообщения или периодически вставлялись в конце предложения.

Современное использование

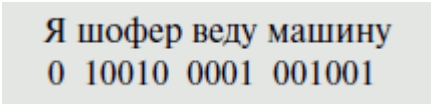
Сегодня любая форма данных, такая как текст, изображение, аудио- или видеоинформация, может быть переведена в цифровую форму, и во время преобразования в цифровую форму или обработки можно в общие данные вставить секретную двоичную информацию. Такая скрытая информация не обязательно используется для сохранения тайны. Она может также использоваться как пометка, чтобы защитить авторское право, предотвратить вмешательство или внести дополнительную информацию, комментирующую текст для некоего получателя.

Скрывающие тексты. Для незаметной передачи секретных данных может быть задействован обычный текст. Есть несколько путей. Один из них — вставка двоичных символов. Например, мы можем использовать пробел между словами. Чтобы представить двоичную цифру `0`, используется одиночный пробел — и два пробела, чтобы представить двоичную цифру `1`. Представленное ниже короткое сообщение скрывает двоичное `8`-битовое представление буквы `A (01000001)` в коде ASCII.



В сообщении, которое приведено выше, два пробела содержатся между словами `"учебник"` и `"по"` и между `"по"` и `"стеганография"`. Конечно, усложненное программное обеспечение может вставить пробелы, которые различаются минимально, чтобы скрыть код от непосредственного визуального распознавания.

Другой, более эффективный метод использует словарь слов, организованных согласно их грамматическим значениям (частям речи). Мы можем, например, иметь словарь, содержащий `2` местоимения, `16` глаголов, `32` существительных. За каждым представителем этого словаря закреплен код. Предположим, что первый бит двоичных данных может быть представлен местоимением, каждое из которых имеет код (например, `Я` — это `0`, а "мы" — это `1`). Следующие пять битов могут быть представлены существительным (подлежащим в предложении). В нашем примере можно обозначить код `10010` словом `"шофер"`. Следующие четыре бита могут быть представлены глаголом, (в примере — словом `"веду"`, которое представляет код `0001`), и последние пять бит — другим существительным (дополнение). В нашем примере `"машину"` — означает код `001001`. Тогда можно договориться использовать скрывающий текст, который всегда применяет предложения *местоимение — существительное — глагол — существительное*. Секретные двоичные данные могут быть разделены на куски на `16` битов. Например, секретное сообщение `"Hi"`, которое в ASCII отображается `0 10010 0001 001001`, могло быть засекречено следующим предложением:



Это — очень тривиальный пример. Реальный подход использует более усложненный алгоритм и большее разнообразие применяемых слов для одного и того же кода.

Методы скрытия, использующие изображения. Данные могут быть скрыты другим цветным изображением. Переведенные в цифровую форму изображения состоят из пикселей (элемент картинки), в котором обычно каждый пиксель использует `24` бита (три байта). Каждый байт представляет один из первичных цветов (красный, зеленый или синий). Мы можем поэтому иметь 2^8 различных оттенков каждого цвета. В методе, названном *LSB* (Last Significant Bit), самый младший бит каждого байта установлен на нуль. От этого изображение становится немного светлее в некоторых областях, но это обычно не замечается. Теперь мы можем скрыть двоичные данные в изображении, сохраняя или изменяя самый младший бит. Если наша двоичная цифра — `0`, мы сохраняем бит; если это — `1`, мы изменяем бит на `1`. Этим способом мы можем скрыть символ (восемь битов ASCII) в трех пикселях. Последний бит последнего пикселя не учитывается. Например, следующие три пикселя могут представить латинскую букву `M` (`4D16` или, в двоичной системе, `0100 1101`):

01010010	10111100	01010100
01011111	10111101	01100101
01111110	01001011	00010100

Другие методы скрытия. Возможны также другие методы скрытия. Секретное сообщение, например, может быть закрыто аудио- (звук и музыка) и видеоинформацией. И аудио, и видео сегодня подвергаются сжатию. Секретные данные могут быть внесены в информацию в процессе или перед сжатием. Теперь мы прекращаем обсуждение этих методов и рекомендуем интересующимся более специализированную литературу по стеганографии.

1.5. Рекомендованное чтение

Для более детального ознакомления с предметами, о которых шла речь в этой главе, начинающим можно рекомендовать нижеследующие книги и сайты. Символы, заключенные в скобки, рассматриваются как ссылки к списку литературы в конце книги.

Книги

Несколько книг рассматривают *цели безопасности*, нападения и механизмы. Мы рекомендуем [Bis05] и [Sta06].

Сайты

Больше информации о темах, обсужденных в этой главе, дают следующие сайты:

- http://www.faqs.org/rfcs/rfc2828.html
- http://www.cs.binghamton.edu/~steflik/cs455/rfc/x800.pdf

1.6. Итоги

- Для информационной безопасности были определены три главные цели: конфиденциальность, целостность и готовность.
- Конфиденциальности информации угрожают два типа атак: вмешательство — и наблюдение за трафиком и его анализ. Четыре типа атак могут угрожать целостности информации: модификация, имитация источника, повторная передача информации и отказ от сообщения. Атака "прекращение обслуживания запроса" угрожает готовности информации.
- Организации, которые занимаются передачей данных и созданием сетей, такие как *ITU*-T или Internet *Forum*, определили несколько служб безопасности, предназначенных для целей информационной безопасности и защиты от атак. В этой главе рассматривались пять общих служб безопасности: конфиденциальность данных, *целостность данных*, установление подлинности, исключение отказа от сообщений и управление доступом.
- *ITU*-T также рекомендует некоторые механизмы обеспечения безопасности. В главе рассмотрены восемь из этих механизмов: шифрование, *целостность данных*, *цифровая подпись*, установление правомочности изменений, заполнение трафика, *управление маршрутизацией*, *доверенность* и управление доступом.
- Есть два метода — криптография и стеганография, которые могут реализовать некоторые или все механизмы. Криптография или "тайное письмо" включает скремблирование сообщения или создание *дайджеста сообщения*. Стеганография, или "закрытая запись", означает, что сообщение скрывается и закрывается другой информацией.

1.7. Набор для практики

Обзорные вопросы

1. Определите три *цели безопасности*.
2. Укажите различие между пассивными и *активными атаками* на секретную информацию. Назовите некоторые *пассивные атаки*. Назовите некоторые *активные атаки*.
3. Перечислите и определите пять служб безопасности, рассмотренные в этой главе.
4. Определите восемь *механизмов безопасности*, рассмотренные в этой главе.
5. Укажите различие между шифрованием и стеганографией.

Упражнения

1. Какая служба(ы) безопасности гарантируется при использовании каждого из следующих методов пересылки по почте в почтовом отделении?
    - Обычная почта

- Обычная почта с подтверждением доставки
- Обычная почта с доставкой и подписью получателя
- Заказное письмо
- Почта с объявленной ценностью
- Зарегистрированная корреспонденция

2. Определить тип атаки на секретную информацию в каждом из следующих случаев:
   - Студент проникает в офис профессора, чтобы получить копию теста, который будет проведен на следующий день.
   - Студент дает чек на получение денег на `10$` , чтобы купить уже подержанную книгу. Потом он узнает, что чек был оплачен на `100$` .
   - Студент передает сотни запросов в день, используя фальшивый обратный адрес телефона другого студента.

3. Какие механизм(ы) безопасности реализованы в каждом из следующих случаев?
   - Университет требует идентификатор студента и пароль, чтобы позволить студенту получить доступ в школьный сервер.
   - Университетский сервер разъединяет студента, если он получил доступ в систему более чем два часа назад.
   - Профессор отказывается передать студентам их оценки электронной почтой, если они не соответствуют студенческой идентификации, заранее назначенной профессором.
   - Банк требует подписи клиента для изъятия клиентом денег.

4. Какая методика (криптография или стеганография) используется в каждом из следующих случаев для защиты конфиденциальности?
   - Студент пишет ответы на билеты на маленьком листочке бумаги, бумага свертывается и вставляется в шариковую ручку, а ручка передается другому студенту.
   - Чтобы передать сообщение, шпион заменяет каждый символ в сообщении символом, который был согласован заранее как замена другого символа.
   - Компания использует специальные чернила на своих чеках, чтобы предотвратить подделки.
   - Аспирантка использует водяные знаки, чтобы защитить свою работу, которая вывешена на ее сайте.

5. Какой механизм(ы) безопасности реализуется, когда человек подписывает форму при заполнении заявления на кредитную карту?