Технологии стеганографии в ситемах инфокоммуникаций

Лектор: к.т.н., доц. Небаева Ксения Андреевна
E-mail: oklaba@mail.ru

Лекция 1. Вводная.

СТЕГАНОГРАФИЯ (В широком смысле).
Англоязычный термин"Скрытие информации" (Information hiding (IH)).

Определение. IH - это семейство методов, при помощи которых некоторое дополнительное сведение погружается в основное
(покрывающее сообщение (ПС)) при сохранении хорошего качества ПС.

Две основные части IH:
1. Собственно стеганография (стеганография).
2. Цифровые "водяные знаки" (ЦВЗ).

Задачи стеганографии:
Погрузить дополнительное сообщение в ПС так, чтобы сам факт его присутствия в нем нельзя было бы обнаружить нелегитимным пользователям.

Задача ЦВЗ:
Погрузить дополнительные сведения (обычно идентификационный код автора) в ПС так, чтобы его нельзя было бы удалить, не ухудшив существенно качество ПС.
(Факт такого вложения может и обнаруживаться нелегитимными пользователями.)

Типичные ПС:
- неподвижное изображение
- подвижное изображение (видео)
- аудио файлы
- речь
- печатный смысловой текст
- графические представления текста и схем
- интернет - протоколы
- программы для компьютеров.

Вкладываемая информация:
- изображение
- текстовые сообщения и данные
- речевые сообщения.

Замечание. Как правило, все вкладываемые сообщения предварительно шифруются с использованием ключей шифрования.

Принцип Кирхгоффа для IH:
Предполагается, что нелегитимным пользователям известно о IH-системе все, кроме стегоключа.
Нелегитимный пользователь, который пытается нарушить выполнение задачи IH, называется атакующим (или злоумышленником), а его действия атакой на стегосистему.

Часть I. Стегосистемы.

Отличие стеганографии (СГ) от криптографии (КР):
КР делает невозможным понимание содержание сообщения, сохраняя при этом возможность обнаружить факт ее использования (шумоподобные сигналы).
СГ утаивает сам факт погружения дополнительной информации в "невинное" сообщение.

Цели использования СГ:
1. Альтернатива криптографии при ее запрещении или ограничении уровня стойкости.
2. Скрытие пользователей нуждающихся в хранении и передаче секретной информации.
3. Передача секретной информации через транзитных пользователей.
4. Передача секретных сигналов и команд определенным пользователям сети интернет.
5. Отслеживание распространителей информации.

Различные постановки задач и методы их решения

- Некоторые возможные подходы к сокрытию передаваемой информации
- 1) Попытаться скрыть сам факт передачи и, в частности,
- скрыть канал связи,
- скрыть отправителя,
- скрыть получателя,
- скрыть способ передачи,
- скрыть способ представления информации в виде сообщений.
- 2) Попытаться в открытом канале связи создать трудности для перехвата передаваемых сообщений,
- 3) Попытаться в открытом канале связи, доступном для перехвата, спрятать скрытые данные в передаваемых открытых сообщениях так, чтобы они не могли быть обнаружены без специальных средств, например, химических, оптических и т.п.
- 4) Попытаться в открытом канале связи, доступном для перехвата, спрятать скрытое сообщение в протоколе, т.е. в порядке выбора и последовательности передачи открытых сообщений.
- 5) В открытом канале связи, доступном для перехвата и обнаружения наличия скрытых сообщений, попытаться затруднить возможность противника по обнаружению скрытых данных в передаваемых со общениях, в частности, путем использования особенностей человеческого восприятия.
- 6) В открытом канале связи, доступном для перехвата и обнаружения противником наличия скрытых сообщений, попытаться затруднить возможность противника по ознакомлению с содержанием скрытых данных в передаваемых сообщениях, например, путем использования:
- кодов,
- шифрования сообщений.
- 7) В открытом канале связи, доступном для перехвата, обнаружения наличия и ознакомления с содержанием крытой информации, попытаться затруднить возможность противника по пониманию смысла передаваемых сообщениях путем использования таких методов, как:
- дезинформация,
- многозначное толкование.

Основные атаки на СГ:
- обнаружение стегосигналов
- нахождение объема секретного вложения
- чтение стегосообщения
- удаление стегосигнала без значительного ухудшения качества ПС и даже при необнаружении СГ.

Пример: Случайное изменение положений стрелок в партии наручных часов, прибывшей на американскую таможню во время 2-ой Мировой Войны.

Возможные преобразования стегосигналов:
- естественные преобразования (фильтрация, сжатие, масштабирование. передача по каналам с шумом);
- преднамеренные (атаки).

Критерии эффективности СГ:
- вероятность пропуска стегосигнала
- вероятность ложного обнаружения стегосигнала
- вероятность ошибки бита при извлечении легитимными пользователями вложенного сообщения
- качество ПС после вложения (отношение сигнал/шум или более сложные, в том числе экспертные, оценки)
- скорость вложения (число бит вложенного сообщения на один отсчет ПС).

Определение. СГ называется *робастной*, если секретное сообщение устойчиво выделяется при всех естественных или преднамеренных преобразованиях СГ, которые не искажают существенно ПС.

Основная классификация СГ:
а) Для легитимных пользователей:
- с известным ПС на легитимном декодере (*информированный декодер*)
- с неизвестным ПС на легальном декодере (*"слепой" декодер*)
- с использованием ПС в легальном кодере (*информированный кодер*).
б) Для "атакующих":
- с известной стеганограммой (выполняется всегда)
- с известным сообщением
- с выбранным сообщением
- с известным (или выбранным ПС) - для каналов с шумом.

Основная концепция в разработке СГ:
Найти "шумовые компоненты" (области) в ПС и заменить их на зашифрованное (т.е. шумоподобное) секретное сообщение.

Основная проблема при разработке СГ:
Статистика таких сложных ПС как звук, изображение и смысловой текст известна не полностью и весьма сложна. Поэтому существует опасность, что атакующий знает ее лучше, чем разработчик СГ.

Краткий исторический обзор СГ (примеры использования).

1. История с бритьем раба (обрить, сделать на голове татуировку секретного сообщения, отрастить волосы и направить через территорию противника к своим, а там снова обрить и прочитать сообщение).
2. Египетские надписи, содержащие скрытую информацию (для посвященных).
3. Индийская Кама-сутра, где под номером 45 значится секретное письмо.
4. Скрытый смысл в Библии.
" ... И сказал им вам дано знать тайны Царства Божия, а тем внешним все бывает в притчах. Так что они своими глазами смотрят, и не видят, своими ушами слышат и не разумеют, да не обратятся и прощены будут им грехи". (Евангелие от Матфея)
5. Симпатические чернила.
6. Язык жестов (карточные шулера).
7. Расположение предметов (ошибка пастора Шлага, потерянное письмо в повести Э.По).

Основные особенности современной СГ:
Это *цифровая стеганография*, когда все ПС представляются в цифровой форме, а вложение и извлечение секретной информации производится на компьютерах.