Тема 2.1. Принципы криптографической защиты информации

Network security.

Протокол передачи данных — набор соглашений интерфейса логического уровня, которые определяют обмен данными между различными программами.

Слои интернет протоколов:

- на физическом уровне определяются физические (механические, электрические, оптические) характеристики линий связи;
- на канальном уровне определяются правила использования физического уровня узлами сети;
- сетевой уровень отвечает за адресацию и доставку сообщений;
- транспортный уровень контролирует очередность прохождения компонентов сообщения;
- задача сеансового уровня — координация связи между двумя прикладными программами, работающими на разных рабочих станциях;
- уровень представления служит для преобразования данных из внутреннего формата компьютера в формат передачи;
- прикладной уровень является пограничным между прикладной программой и другими уровнями — обеспечивает удобный интерфейс связи сетевых программ пользователя.

Другая модель — стек протоколов TCP/IP — содержит 4 уровня:

- канальный уровень (link layer), Ethernet, PPP, PPTP, L2TP
- сетевой уровень (Internet layer), Ipv4, IPv6
- транспортный уровень (transport layer), TCP, UDP
- прикладной уровень (application layer). FTP, SMTP, HTTP, HTTPS, Telnet

Сетевая безопасность относится ко всем слоям, поскольку на каждом из них могут совершаться атаки и возникать ошибки.

Угрозы сетевой безопасности (не все связаны с криптографией):

- Наблюдатель — перехватывает сообщения — читает содержимое сообщений.
- Нарушитель — пораженный хост — вмешивается в содержимое сообщений.
- Самозванец — Удаленная социальная инженерия — обман с целью получения информации
- Вымогатель — botnet — разрушает сетевые сервисы. (DdoS)

Таким образом портокол безопасности в 802.11 (WEP И WPA) безопасны для наблюдателя?

Не совсем. Какие еще угрозы безопасности возможны для wi-fi?

- Взломать защиту протокола — Легко для WEP и очень сложно для WPA
- Угадать пароль — Часто возможно

- Получить пароль с устройства — может быть возможно.
- Вторжение в дом и доступ к устройству AP — Сложно.

Реальность: многие сетевые протоколы (TCP, IP, DNS) были разработаны прежде чем Интернет стал популярным. Это был маленький мир, где все друг другу доверяли, поэтому протоколы не были направлены на безопасность.

Wireless Security

В отличие от Ethernet wi-fi отправляет сообщения всем устройствам в радиусе.

Главные угрозы для беспроводной сети:

- Возможность получать все сообщения
- Неавторизированный доступ к сети

Безопасность основана на пароле.

Стандарты: 802.11 (1999) использует WEP. 802.11i (2004) использует WPA. С 2006 г. поддержка WPA2 — обязательное условие для всех сертифицированных Wi-Fi устройств.

HTTP — TCP — IP — 802.11

Web Security

Основной протокол безопасности в web — HTTPS (HTTP over SSL/TLS). Пртокол SSL основан на сертификатах безопасности.

SSL (англ. secure sockets layer — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. В настоящее время известно, что протокол не является безопасным. SSL должен быть исключен из работы в пользу TLS. TLS и SSL используют асимметричную криптографию для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Основные шаги процедуры создания защищённого сеанса связи:

- клиент подключается к серверу, поддерживающему TLS, и запрашивает защищённое соединение;
- клиент предоставляет список поддерживаемых алгоритмов шифрования и хеш-функций;
- сервер выбирает из списка, предоставленного клиентом, наиболее надёжные алгоритмы среди тех, которые поддерживаются сервером, и сообщает о своём выборе клиенту;
- сервер отправляет клиенту цифровой сертификат для собственной аутентификации. Обычно цифровой сертификат содержит имя сервера, имя удостоверяющего центра сертификации и открытый ключ сервера;
- клиент может связаться с сервером доверенного центра сертификации и подтвердить аутентичность переданного сертификата до начала передачи данных;

- для генерации сеансового ключа для защищённого соединения клиент шифрует случайно сгенерированную цифровую последовательность открытым ключом сервера и посылает результат на сервер. Учитывая специфику алгоритма асимметричного шифрования, используемого для установления соединения, только сервер может расшифровать полученную последовательность, используя свой закрытый ключ.

На этом заканчивается процедура подтверждения связи. Между клиентом и сервером установлено безопасное соединение, данные, передаваемые по нему, шифруются и расшифровываются с использованием ключа шифрования до тех пор, пока соединение не будет завершено.

В текущей версии протокола доступны следующие алгоритмы:

- Для обмена ключами и проверки их подлинности применяются комбинации алгоритмов: RSA (асимметричный шифр), Diffie-Hellman (безопасный обмен ключами), DSA (алгоритм цифровой подписи), ECDSA;
- Для симметричного шифрования: RC4, IDEA, Triple DES, SEED, Camellia или AES;
- Для хеш-функций: MD5, SHA, SHA-256/384.

Алгоритмы могут дополняться в зависимости от версии протокола. До последней версии протокола TLS 1.2 были доступны также следующие алгоритмы симметричного шифрования, но они были убраны как небезопасные: RC2, IDEA, DES.

Симметричные алгоритмы

Симметричная криптосистема - способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Симметричный шифр — это пара «эффективных» алгоритмов (E, D) на множествах (K, M, C), где E: KxM → C, D: KxC → M такие, что для любых m из M и k из K : D(k, E(k, m)) = m.

Одноразовый шифр-блокнот (Шифр Вернама) — 1917 г.

M = C = K = {0, 1}^n. Ключ — это строка битов такой же длины, как и исходное сообщение.

Здесь c = E(k, m) = k XOR m, a m = D(k, c) = k XOR c. D(k, E(k, m)) = D(k, k XOR m) = k XOR (k XOR m) = (k XOR k) XOR m = 0 XOR m = m.

Вопрос: Если у нас есть m и c, можем ли мы узнать k? Да, k = m XOR c.

Одна из основных идей теории безопасности (Schannon 1949) — если у вас есть зашифрованное сообщение, оно не должно предоставлять какую-либо информацию об исходном сообщении.

Определение. Шифр (E, D) на множествах (K, M, C) имеет абсолютную стойкость, если для любых двух сообщений m1, m2 одинаковой длины и для любого c из C: Pr[E(k, m1) = c] = Pr[E(k, m2) = c] для любого k из K. Т.е. см предыдущий абзац.

Лемма. ОШБ имеет абсолютную стойкость

Вопрос. Пусть у нас есть m, c. Сколько различных ключей соответствует данным m, c?

Теорема. Для абсолютной стойкости |K| >= |M|.

Для потокового шифра можно сделать так: заменить случайный ключ на псевдослучайный ключ, т. е. G: {0, 1}^s → {0, 1}^n, где s « n.

Отсюда:

1. Нужно новое определение безопасности.
2. Безопасность будет зависить от PRG.

Загадка Цикады

Всё началось 4 января 2012 года, когда посетители всем известного 4chan обнаружили пост с картинкой, представлявшей собой белый печатный текст на чёрном фоне.

Текст гласил: «Привет. Мы ищем лиц с высоким интеллектом. Для этого мы разработали тест. В этом изображении есть скрытое сообщение. Найдите его, и оно покажет вам, как найти нас. С нетерпением ожидаем тех немногих, которым удастся пройти весь путь. Удачи. 3301».

Посетители этого анонимного имиджборда, на котором обычно выкладываются хулиганские и полупорнографические картинки, принялись активно обсуждать необычное изображение, и многие пришли к выводу, что, возможно, так АНБ ищет потенциальных сотрудников. Действительно, способ не нов: спецслужбы отслеживают хакерские мероприятия и форумы с целью привлечь на госслужбу талантливую молодёжь. А во время Второй мировой войны британские спецслужбы отыскивали перспективных сотрудников при помощи кроссвордов в газете Daily Telegraph. Так или иначе, картинка привлекла внимание, её перепостили на других форумах — и энтузиасты взялись за расшифровку.

Кто-то из комментаторов предложил открыть изображение в простом текстовом редакторе WordPad, и в полученном тексте обнаружилось единственное осмысленное сообщение: «TIBERIVS CLAVDIVS CAESAR says «lxxt>33m2mqkyv2gsq3q=w]O2ntk»», то есть «Тиберий Клавдий Цезарь говорит “lxxt>33m2mqkyv2gsq3q=w]O2ntk”». Благодаря очевидной подсказке расшифровать код оказалось несложно: это был так называемый код Цезаря, или шифр сдвига, в котором каждый отдельный символ в тексте заменяется символом, находящемся в алфавите на некоторое постоянное число позиций левее или правее. Для знающих, что Тиберий Клавдий был четвёртым римским императором, было логичным предположить, что сработает смещение текста на четыре буквы назад, — результатом которого и стал адрес сайта в интернете.

Зашедшего по этому адресу встречало изображение утки с издевательской надписью: «УПС просто заманивает сюда. Похоже, вы не смогли догадаться, как извлечь сообщение». Ключ к загадке скрывался в английском тексте: слова «guess» и «out» приводили к названию стеганографической программы OutGuess, позволяющей выявлять данные, которые скрыты в обычных цифровых изображениях. Прогнав картинку через OutGuess, можно было получить последовательность цифр с пометкой «Это книжный код» и ссылку на одну из «досок» популярного сайта Reddit, где посетителя встречали код, который состоял из цифр, использовавшихся в древности индейцами майя, множество периодически добавляющихся

зашифрованных строчек и две картинки с надписями «Добро пожаловать» и «Проблемы?».

В каждой картинке было скрыто по сообщению, которые также можно было прочитать с помощью OutGuess. В первом говорилось, что с этого момента каждое послание будет иметь PGP-подпись, и приводилась эта подпись, а второе гласило: «Ключ был всегда перед вашими глазами. Это не поиски Священного Грааля. Перестаньте всё усложнять. Удачи. 3301».

Цифры майя были ключом к расшифровке строчек: здесь снова использовался код Цезаря, и в результате перед глазами представал отрывок из поэмы о короле Артуре, входящей в состав средневекового валлийского сборника повестей «Мабиногион». Применив к расшифрованным строчкам «книжный код», дававшийся ранее (первое число — номер строки, второе — порядковый номер буквы), можно было получить такой текст: «Call us at us tele phone numBer two one four three nine oh nine six oh eight», то есть «Позвоните нам по телефонному номеру 2143909608».

Трубку снимал автоответчик с таким сообщением: «Очень хорошо. Вы справились. Три простых числа связаны с оригинальным изображением final.jpg. 3301 одно из них. Вы должны найти другие два. Чтобы перейти на следующий уровень, перемножьте эти числа между собой и добавьте .com. Удачи. До свидания».

Размеры первоначального изображения составляли 509×503 пикселя, и оба этих числа простые. Перемножив их с 3301, можно было получить адрес 845145127.com, где посетителя встречало изображение цикады и счётчик с обратным отсчётом.

Очередное сообщение, скрытое в картинке, гласило: «Вы хорошо постарались, чтобы зайти так далеко. Терпение — это добродетель. Вернитесь сюда в 17:00 в понедельник 9 января 2012 года по всемирному времени».

После того как отсчёт прекратился, сайт обновился, и в изображении цикады было скрыто уже другое сообщение, содержащее 14 GPS-координат разных точек на земном шаре, включая Варшаву, Париж, Сиэтл, Сеул, Аризону, Калифорнию, Новый Орлеан, Майами, Гавайи и Сидней. Масштабы мероприятия поразили даже самых недоверчивых участников! И, более того, быстро нашлись энтузиасты, которые проверили все 14 точек.

По всем указанным адресам находились уличные фонарные столбы, к которым был прикреплён плакат с изображением цикады и QR-кодом. Различные варианты сообщений предлагали расшифровать очередной «книжный код», на сей раз в книге «Агриппа» Уильяма Гибсона, который в итоге приводил к адресу sq6wmgv2zcsrix6t.onion в сети TOR. Подавляющее большинство зашедших по этому адресу получали сообщение «Нам нужны лучшие, а не последователи», а несколько недель спустя на 4chan и Reddit появилось следующее: «Привет. Мы нашли тех, кого искали. Так наше путешествие длиной в месяц заканчивается. Пока».

С чем столкнулись те, кого искали организаторы этого «путешествия», достоверно неизвестно. Некоторым зашедшим по адресу сайта в сети TOR предложили зарегистрировать анонимный почтовый ящик Hotmail, на который было прислано очередное задание. Впрочем,

поскольку желающих поделиться своими успехами в Сети не нашлось, что было дальше, так и остаётся тайной.