Семинарское занятие № 1. Криптоанализ: современное состояние и перспективы развития.

Цель занятия: обзор современных методов криптоанализа.

План занятия:
Введение
1 Современные методы криптоанализа
Заключение
Контрольные вопросы

Ключевые слова: [выбрать самостоятельно].

Содержание занятия**:**

Введение

Любая тайна, порожденная человеческим сознанием, им же может быть и раскрыта.

/Шерлок Холмс/

Одним из главных аспектов аудита безопасности информационных систем является оценка надежности используемых криптографических алгоритмов. На семинарских занятиях мы проведем обзор современных методов криптоанализа. Наряду с классическими методами, такими как метод полного перебора и метод Полларда, описываются атаки на симметричные и асимметричные криптосистемы: линейный и разностный анализ блочных шифров, субэкспоненциальные алгоритмы факторизации и дискретного логарифмирования и т. д. Особое внимание уделяется новому виду криптоанализа – атакам по побочным каналам.

1 Современные методы криптоанализа

Великий сыщик и великий писатель ошибались: их утверждения, вынесенные в эпиграф, были в середине 40х гг. прошлого века опровергнуты великим ученым и основоположником современной криптографии Клодом Шенноном. Он показал [1], что если на любой исходный текст наложить (т.е. сложить по модулю с текстом) ключ длины не меньшей, чем само сообщение, то такой шифр будет нераскрываемым: потенциальному злоумышленнику потребуется перебрать все возможные ключи и каждым из них попробовать расшифровать сообщение. Однако использование такого способа шифрования, получившего название «одноразовых блокнотов», в большинстве случаев оказывается слишком дорогим и неоправданным. Это связано с тем, что нет смысла бороться за устойчивость системы защиты информации к взлому ниже некоторой «фоновой» вероятности, т.е. вероятности события, которое мы не в состоянии предотвратить [2]. Например, если вероятность выхода компании из бизнеса равна 2^{-30} (менее чем один из миллиона), то есть ли смысл для защиты информации, которая может нанести компании ущерб, сопоставимый с кризисом рынка, использовать алгоритм, вероятность вскрытия которого за приемлемое время составляет 2^{-200}?

Выбор необходимой степени защиты информации и средств ее обеспечения является важной задачей и должен учитывать ряд параметров: уровень секретности информации; ее стоимость; время, в течение которого она должна оставаться в тайне и т.д. Проблема защиты информационных ресурсов в настоящее время приобретает все более важное

[1] Шеннон К.Э. Работы по теории информации и кибернетике // М.: И.Л., 1963.
[2] Баричев С. Основной вопрос криптографии // Chief Inforamtion Officer - руководитель информационной службы. #5 (37), 2005, с. 93-95.

значение. Так, по данным отчета CSI/FBI Computer Crime and Security Survey 2005 [3], средний ущерб каждой компании, в которой в минувшем году была зафиксирована утечка конфиденциальных данных, составил 355,5 тыс. долларов (причем по сравнению с 2004 годом эта цифра возросла почти вдвое). По некоторым оценкам, экономические потери от злонамеренных атак на банковские системы по всему миру составляют ежегодно около 130 млрд. долларов.

Как известно [4], далеко не все присутствующие на рынке криптографические средства обеспечивают обещанный уровень защиты. Важность этой проблемы подчеркивается и в работе [5]. Системы и средства защиты информации (СЗИ) характеризуются тем, что для них не существует простых и однозначных тестов, позволяющих убедиться в надежной защите информации. Например, для проверки работоспособности системы связи достаточно провести ее испытания. Однако успешное завершение этих испытаний не позволяет сделать вывод о том, что встроенная в нее подсистема защиты информации тоже работоспособна. Задача определения эффективности СЗИ при использовании криптографических методов защиты зачастую более трудоемкая, чем разработка СЗИ, требует наличия специальных знаний и более высокой квалификации, чем задача разработки. Часто анализ нового шифра является новой научной, а не инженерной задачей.

Эти обстоятельства приводят к тому, что на рынке появляются средства криптографической защиты информации, про которые никто не может сказать ничего определенного. При этом нередко разработчики держат криптоалгоритм (как показывает практика, часто легко взламываемый) в секрете. Однако задача точного определения используемого криптоалгоритма не может быть гарантированно сложной хотя бы потому, что он известен разработчикам. Кроме того, если нарушитель нашел способ преодоления защиты, то не в его интересах об этом заявлять. В результате пользователи таких СЗИ попадают в зависимость как минимум от разработчика. Поэтому обществу должно быть выгодно открытое обсуждение безопасности СЗИ массового применения, а сокрытие разработчиками криптоалгоритма должно быть недопустимым [6].

Современная криптография – соревнование методов шифрования и криптоанализа. Криптоанализом (от греческого kryptós – «скрытый» и analýein – «ослаблять» или «избавлять») называют науку восстановления (дешифрования) открытого текста без доступа к ключу. Фундаментальное допущение криптоанализа, впервые сформулированное Кирхгоффом [7], состоит в том, что секретность сообщения всецело зависит от ключа, т.е. весь механизм шифрования, кроме значения ключа, известен противнику. Как бы то ни было, секретность алгоритма не является большим препятствием: например, для определения типа программно реализованного криптографического алгоритма требуется лишь несколько дней инженерного анализа исполняемого кода.

Криптоанализ ставит своей задачей в разных условиях получить дополнительные сведения о ключе шифрования, чтобы значительно уменьшить диапазон вероятных ключей. Результаты криптоанализа могут варьироваться по степени практической применимости. Так, криптограф Ларс Кнудсен [8] предлагает следующую классификацию успешных

---

[3] Gordon L.A., Loeb M.P., Lucyshyn W., Richardson R. CSI/FBI Computer Crime and Security Survey 2005 // Computer Security Institute Publications, 2005.

[4] Schneier B. Snake Oil, Crypto-Gram // February, 1999. Available via http://www.counterpane.com/Crypto-Gram.html

[5] Ростовцев А.Г., Михайлова Н.В. Методы криптоанализа классических шифров // 1998. Опубликовано: http://crypto.hotbox.ru/download/cryptoan.zip

[6] Ростовцев А.Г., Михайлова Н.В. Методы криптоанализа классических шифров // 1998. Опубликовано: http://crypto.hotbox.ru/download/cryptoan.zip

[7] Kerckhoffs A. La cryptographie militaire // Journal des sciences militaires, vol. IX. P. 5-38, Jan. 1883, (P. 161-191, Feb. 1883).

[8] Knudsen L.R. Block Ciphers - Analysis, Design, Applicatons // Ph.D. dissertation, Aarhus Unversity, Nov 1994.

исходов криптоанализа блочных шифров в зависимости от объема и качества секретной информации, которую удалось получить:

- ✓ *Полный взлом – криптоаналитик извлекает секретный ключ.*
- ✓ *Глобальная дедукция – криптоаналитик разрабатывает функциональный эквивалент исследуемого алгоритма, позволяющий зашифровывать и расшифровывать информацию без знания ключа.*
- ✓ *Частичная дедукция – криптоаналитику удается расшифровать или зашифровать некоторые сообщения.*
- ✓ *Информационная дедукция – криптоаналитик получает некоторую информацию об открытом тексте или ключе.*

Однако взлом шифра совсем не обязательно подразумевает обнаружение способа, применимого на практике для восстановления открытого текста по перехваченному зашифрованному сообщению. В научной криптологии другие правила [[9]]. Шифр считается взломанным, если в системе обнаружено слабое место, которое может быть использовано для более эффективного взлома, чем метод полного перебора ключей (‘brute-force approach’). Допустим, для дешифрования текста методом полного перебора требуется перебрать 2^{128} возможных ключей; тогда изобретение способа, требующего для дешифрования 2^{110} операций по подбору ключа, будет считаться взломом. Такие способы могут требовать нереалистично больших объемов подобранного открытого текста или памяти ЭВМ. Под взломом понимается лишь подтверждение наличия уязвимости криптоалгоритма, свидетельствующее о том, что свойства надежности шифра не соответствуют заявленным характеристикам. Как правило, криптоанализ начинается с попыток взлома упрощенной модификации алгоритма, после чего результаты распространяются на полноценную версию: прежде чем браться за взлом, например, 16-раундовой версии DES, естественно для начала попытаться взломать шифр с меньшим количеством раундов, чем указано в его спецификации (например, 8-раундовую версию шифра).

Попытка криптоанализа называется атакой. Прежде чем классифицировать атаки, введем ряд обозначений: открытый текст будем обозначать буквой x, шифртекст – буквой y (в качестве x может выступать любая последовательность битов: текстовый файл, оцифрованный звук, точечный рисунок и т.д.). Пусть для зашифрования и расшифрования используются ключи k и k' соответственно (в симметричной криптографии k = k'); обозначим функцию зашифрования E_k, расшифрования – $D_{k'}$. Тогда выполняются соотношения $E_k(x) = y$, $D_{k'}(y) = x$.

Известны четыре основных типа криптоаналитических атак. В каждом случае предполагается (согласно фундаментальному допущению Кирхгоффа), что криптоаналитик знает используемый алгоритм шифрования.

- ✓ *Атака на основе только шифртекста. Криптоаналитик располагает шифртекстами $y_1, \ldots, y_m$, полученными из неизвестных открытых текстов $x_1, \ldots, x_m$ различных сообщений. Требуется найти хотя бы один из x_i, $i = 1, \ldots, m$ (или соответствующий ключ $к_i$), исходя из достаточного числа m криптограмм, или убедиться в своей неспособности сделать это. В качестве частных случаев возможно совпадение ключей: $k_1 = \ldots = k_m$ или совпадение открытых текстов: $x_1 = \ldots = x_m$.*
- ✓ *Атака на основе открытого текста. Криптоаналитик располагает парами $(x_1, y_1), \ldots, (x_m, y_m)$ открытых и соответствующим им зашифрованных текстов. Требуется определить ключ k_i для хотя бы одной из пар. В частном случае, когда $k_1 = \ldots = k_m = k$, требуется определить ключ k или, убедившись в своей неспособности сделать это, определить открытый текст x_{m+1} еще одной криптограммы y_{m+1}, зашифрованной на том же ключе.*

[9] Schneier B. A self-study course in block-cipher cryptanalysis // Cryptologia, v.24, n.1, Jan 2000. P. 18-34.

- ✓ *Атака на основе подобранного открытого текста отличается от предыдущей лишь тем, что криптоаналитик имеет возможность выбора открытых текстов $x_1, \ldots, x_m$. Цель атаки та же, что и предыдущей. Подобная атака возможна, например, в случае, когда криптоаналитик имеет доступ к шифратору передающей стороны.*
- ✓ *Атака на основе адаптивно подобранного открытого текста. Это частный случай вышеописанной атаки с использованием подобранного открытого текста. Криптоаналитик может не только выбирать используемых шифруемый текст, но также уточнять свой последующий выбор на основе полученных ранее результатов шифрования.*

Заключение

В последнее время много публикаций посвящяется «экзотическим» методам криптоанализа, основанным на использовании нейронных сетей, генетических алгоритмов и квантовых компьютеров: несмотря на то, что в настоящее время эти методы не привели к сколько-нибудь серьезным прорывам во взломе шифров, нельзя исключать, что со временем их значение в криптологии может возрасти.

Контрольные вопросы

Смотри руководство по организации самостоятельной работы студентов.