КРИПТОГРАФИЧЕСКИЙ БЕЛЫЙ ЯЩИК

Тошболтаев Д.Б.

Тошболтаев Дилёр Бахтиёр угли– ассистент, преподаватель,
кафедра математическое моделирование и криптоанализ,
Национальный университет Узбекистана им. Мирзо Улугбека,
г. Ташкент, Республика Узбекистан

Аннотация: *в контексте атаки белого ящика, то есть в настройке, где реализация криптографического алгоритма выполняется на ненадежной платформе, противник имеет полный доступ к реализации и ее среде выполнения. В 2002 году Chow et al. представила реализацию AES с белым ящиком, которая направлена на предотвращение извлечения ключей в контексте атаки белого ящика. Однако в 2004 году Billet et al. представила эффективную практическую атаку на реализацию AES с белым ящиком Chow и др. В ответ, в 2009 году, Xiao и Lai предложили новую реализацию AES с белым ящиком, которая, как утверждается, устойчива к атаке Билле и др. В этой статье представлен практический криптоанализ реализации AES белого ящика, предложенный Xiao et al. Алгоритм линейной эквивалентности, представленный Бирюковым и др., используется как строительный блок. Криптоанализ эффективно извлекает ключ AES из реализации AES белого ящика Xiao и др. С коэффициентом работы около* 2^{32}.

Ключевые слова: *криптография белого ящика, AES, управление цифровыми правами.*

1.1 Криптография белого ящика: пример использования

Криптография «белого ящика» направлена на создание программных реализаций криптографических алгоритмов таким образом, чтобы они обеспечивали достаточный уровень надежности против злоумышленника с белым ящиком. Часть «достаточный уровень надежности» относится к защите конфиденциальности секретного криптографического ключа, который также является основной целью криптографии белого ящика. В конечном счете, злоумышленник в модели белого ящика не должен иметь никакого преимущества перед злоумышленником в модели черного ящика в отношении извлечения секретного криптографического ключа, то есть либо иметь полный доступ и полный контроль над реализацией криптографического программного обеспечения, либо иметь единственный доступ к поведению ввода / вывода реализации не должен иметь никакого значения. Реализации, полученные с помощью шифрования с использованием белого ящика, называются реализациями белого ящика.

1.2 Управление цифровыми правами

Из-за цифровой революции, начавшейся в 1990-х годах, копирование и (незаконное) распространение цифрового контента никогда не было таким простым. Поэтому контент-провайдеры нуждались в новых технологиях для защиты своих цифровых активов и контроля доступа и распространения их защищенного авторским правом контента. Такие схемы защиты контента называются Digital Rights Management или DRM. Как и ожидалось, DRM можно найти во многих популярных онлайн-цифровых мультимедиа (таких как видео, музыка, электронные книги, приложения и т. Д.) В настоящее время. Например, обратитесь к онлайн-магазинам Apple iTunes и iBooks, используя систему Apple FairPlay DRM. Хотя Apple выпустила музыку DRM бесплатно в 2009 году [1], видео и электронные книги, приобретенные через iTunes и iBooks Store, по-прежнему используют систему Apple FairPlay DRM. Помимо Apple, есть много других компаний, использующих технологию DRM, а также Microsoft, использующую Windows Media DRM для проигрывателя Windows Media [2].

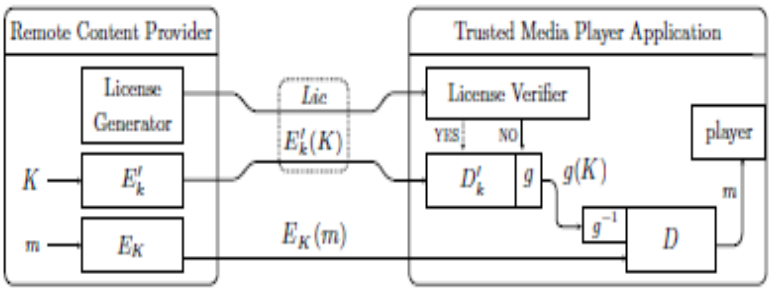

Рис. 1.1: Использование криптографии с белым ящиком: упрощенная модель DRM

Криптография обычно формирует один из основных строительных блоков для обеспечения защиты системы DRM. Упрощенная модель DRM показана на рисунке 1.1, которая служит лишь примером для наброска среды, которая может извлечь выгоду из криптографии с белым ящиком и не предназначена

для представления архитектуры DRM реального мира. Эта упрощенная модель DRM состоит из двух сторон: поставщика удаленного контента и доверенного медиаплеера (например, iTunes), выполненного на ненадежной платформе конечного пользователя (например, ПК). Здесь предполагается, что доверенный медиаплеер является исключительно программным приложением.

Теперь поставщик удаленного контента доставляет защищенный авторским правом медиа-контент m авторизованным конечным пользователям в зашифрованном виде, состоящий из следующих трех элементов:

1. зашифрованный мультимедийный контент $E_k(m)$, где E_k (•) обозначает известный алгоритм E с использованием алгоритма с симметричным ключом, используя ключ секретного контента K;

2. ключ зашифрованного содержимого $E_k^{'}(K)$, где $E_k^{'}(.)$ обозначает (возможно, другой) известный алгоритм $E^{'}$ шифрования с симметричным ключом, используя секретный ключ k секретного конечного пользователя. Соответствующие алгоритмы дешифрования E и E_0 обозначаются соответственно D и D_0;

3. Лицензия лицензии DRM, содержащая ограничения (условия), в соответствии с которыми конечный пользователь может получить доступ к цифровому контенту. Такая лицензия DRM может, например, указывать ограниченный временной интервал (например, для проката фильмов) или максимальное количество копий, которые могут быть сделаны.

Как правило, пункты 2 и 3 отправляются одновременно только по запросу (то есть при покупке) конечного пользователя, тогда как элемент 1 доступен для загрузки. После получения вышеуказанных трех элементов медиаплеер выполняет следующие задачи. Во-первых, он проверяет через лицензию DRM, разрешено ли конечному пользователю получить доступ к медиа-контенту или нет. После положительного подтверждения («ДА») медиаплеер сначала расшифровывает ключ K контента, используя личный ключ k конечного пользователя, и немедленно применяет обратимое кодирование g к K, а затем расшифровывает медиаконтент с использованием K после первого применения инверсного кодирование $g-1$ до g

Очевидно, что в настройке DRM (рис.1.1) злоумышленник (т. Е. Вредоносный пользователь или вредоносная программа, выполняемая на устройстве конечного пользователя) выходит из традиционной модели черного ящика и соответствует белой коробке модель; он владеет и контролирует платформу, на которой выполняется приложение медиаплеера. У злоумышленника есть стимул обойти ограничения, установленные лицензией DRM. Будучи в состоянии сделать это, прокат фильмов становится как бы приобретением фильма. Он может достичь своей цели, успешно выполнив одно из следующих трех действий:

1. извлечь один из обоих ключей дешифрования, то есть либо ключ K контента, либо конечный пользовательский ключ k;

2. подделывать код верификатора лицензии таким образом, чтобы он всегда выводил «YES»;

3. перехватить медиа-контент m.

Контрмеры против вышеупомянутых попыток обхода системы DRM приведены ниже:

1. убедитесь, что используемые криптографические ключи никогда не обнаруживаются в коде, реализующем приложение медиаплеера (статическом или динамическом) или в памяти устройства, на котором выполняется приложение;

2. сделать код верификатора лицензий устойчивым, так что обратное проектирование становится сложной задачей, и любая попытка изменить код приводит к нарушению функциональности медиаплеера;

3. Отпечатайте отпечаток медиаконтента, который однозначно идентифицирует конечного пользователя таким образом, что предатель (т.е. Вредоносный конечный пользователь, незаконно распространяющий свой медиа-контент) может быть прослежен.

Что касается первой контрмеры, это может быть достигнуто путем построения реализации белых расширений обоих алгоритмов дешифрования для предотвращения извлечения ключа дешифрования. Обратите внимание, что между обеими алгоритмами дешифрования ключ K содержимого содержит только в кодированной форме, то есть $g(K)$.

Список литературы

1. *Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A., Vadhan S.P. and Yang K.* On the (im)possibility of obfuscating programs. In J. Kilian, editor, CRYPTO, Volume 2139 of Lecture Notes in Computer Science. Pages 1–18. Springer, 2001.
2. *Barkan E. and Biham E.* The book of Rijndaels. IACR Cryptology ePrint Archive, 2002:158, 2002.