УДК 004.056

КЛЕПТОГРАФИЯ: МЕТОДЫ СИНТЕЗА И АНАЛИЗА КАНАЛОВ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ

А.И. ТРУБЕЙ, М.Е. ШЕЛЕСТ
Учреждение БГУ «НИИ прикладных проблем математики и информатики»
г. Минск, Республика Беларусь

Введение. Окружающая нас информационная среда включает разнообразные программно-аппаратные средства для решения задач информационной безопасности, в том числе программно и аппаратно реализованные криптографические алгоритмы, которые для пользователей зачастую представляются как черные ящики. Конкретную структуру алгоритма сложно отследить даже в программных продуктах при отсутствии текстов исходных программ. И даже в тех случаях, когда спецификация становится доступной для пользователя, последний весьма редко проверяет соответствие имеющегося в его распоряжении продукта официальной документации. Таким образом, пользователи зачастую получают лишь иллюзию защиты. Используя алгоритм, все детали работы которого известны только его разработчику, пользователь располагает единственной гарантией стойкости – утверждением самого разработчика о надежности алгоритма. В то же время разработчики готовых продуктов объективно имеют возможность встроить лазейки в реализуемые криптографические алгоритмы по своей ли инициативе, по чьему-либо заказу или по указанию «сверху» [1].

Любое государство пытается контролировать, по крайней мере, свой сегмент киберпространства. Это возможно разными способами. Например, существует видимая коллаборация с государственными структурами (в первую очередь спецслужб США, Китая и России) крупных фирм-производителей микроэлектроники, вычислительной и телекоммуникационной техники с целью сбора информации о пользователях и доступе к их информации. В СМИ неоднократно появлялись данные о сотрудничестве со спецслужбами известных производителей средств телекоммуникаций (Cisco, Huaway), шифраторов (Crypto AG, Omnisec, Mils Electronic), программного обеспечения (Microsoft), социальных сетей (Facebook, Вконтакте, Одноклассники), антивирусных систем (Касперский, Radware, McAfee), поставщиков услуг электронной почты и сетевых Интернет-гигантов (Google, Yahoo, AT&T, CenturyLink, Verizon). Такое сотрудничество включает разработку и встраивание необходимых «бэкдоров» с последующей передачей спецслужбам тайных сведений о уязвимостях в аппаратном и программном обеспечении, в том числе и о действующих ключах шифрования [2].

1. Клептография и ее связь с криптографией и стеганографией. Вопросами разработки и встраивания закладок в системы защиты информации занимается клептография. Клептография изучает методы синтеза и анализа каналов скрытой передачи данных (embedded trapdoor, subliminal channel), которые позволяют лицу, внедрившего такой канал, получать чувствительную информацию относительно криптосистемы, ключей шифрования или организовывать извлечение защищаемых данных из информационных систем. Клептография стала системно развиваться в 70-х годах прошлого столетия с формированием рынка электронных шифраторов, а затем и открытого программного обеспечения, включая операционные системы. Методы клептографии в последнее время также успешно осваиваются и применяются хакерами.

Клептография, как направление информационной безопасности, тесно связана с криптографией и стеганографией (см. рисунок 1). Связь клептографии с криптографией обусловлена тем, что объектом ее исследований является клептографическая закладка (механизм), которая является частью криптосистемы. Методы криптоанализа часто используются для выявления закладок, то есть являются и инструментами клептоанализа. Клептография близка также к стеганографии. Общей отправной точкой как клептографии, так и стеганографии можно считать работы Г.Саймонса, в которых сформулированы и исследованы «проблема узника» («the prisoner’s problem») и скрытые каналы передачи («subliminal channels») [3, 4].

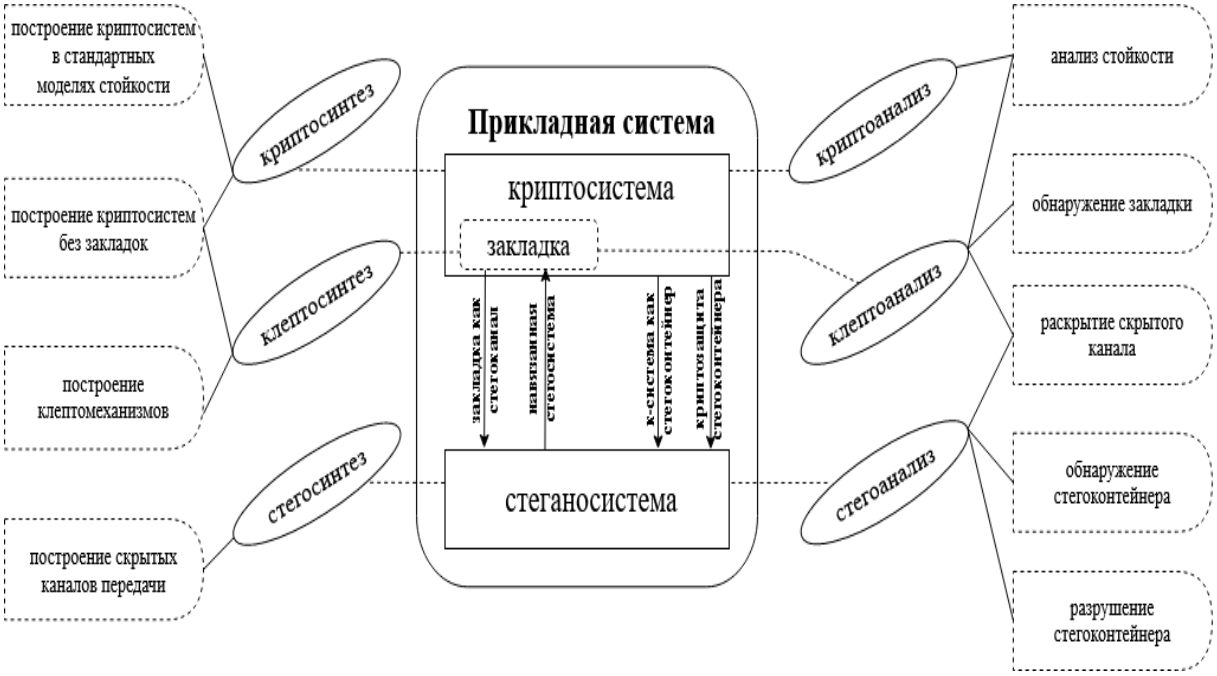

Рис. 1. Связь криптографии, стеганографии и клептографии

Криптоалгоритм с лазейкой (Backdoor, Trapdoor) – это алгоритм, который содержит некоторую скрытую структуру (лазейку), обеспечивающую существование скрытого канала передачи информации; знание этой структуры позволяет получать конфиденциальную информацию (например, о секретном ключе). Без знания лазейки алгоритм кажется надежным. Функционирование клептографических и стеганографических механизмов в некоторых аспектах схожи или пересекаются:

1.1. Клептомеханизм, который выполняет передачу секрета, может рассматриваться как стеганографический канал.

1.2. Скрытно встроенный стеганографический механизм может использоваться разработчиком для клептографических атак передачи секрета.

1.3. Клептографический механизм и стегосистема могут сосуществовать независимо. Например, в одной из модификаций SETUP, кроме схемы передачи ключа, существуют также стегоканалы, которые базируются на временных задержках отправления, вероятностном контроле определенных бит открытых случайных параметров, имитации сбоев и пр.

2. Основные направления развития клептографии. На данный момент, основным направлением практической клептографии является синтез криптосистем и криптопримитивов с соответствующими закладками. Криптосистемой с клептозакладкой будем называть такую криптосистему, у которой:

2.1. Структура системы сгенерирована с использованием «секрета разработчика».

2.2 «Секрет разработчика» практически невозможно получить путем анализа криптосистемы или такой анализ вообще невозможен.

2.3. Криптографические свойства системы существенно снижаются в случае знания «секрета разработчика».

То есть, в клептографической модели криптосистемы добавляется роль «разработчика», цель которого состоит в модифицировании (построении) криптосистемы таким образом, чтобы она содержала закладку, которая бы позволяла в процессе работы системы незаметно передавать определенную секретную информацию разработчику или упрощала ему задачу понижения криптографических свойств системы.

Построение канала утечки путем модификации реализации стандартного протокола – одна из наиболее изученных клептографических проблем [5]. Первой попыткой формализации клептографического механизма является модель SETUP (Secretly Embedded Trapdoor with Universal Protection), предложенная Яном и Юнгом, которая позволяет организовать скрытую передачу секретного ключа криптосистем на базе RSA и задачи дискретного логарифма [6].

Учитывая широкое использование криптографической защиты в информационно-телекоммуникационных системах, особую остроту приобретают вопросы защиты самих криптосистем на всех уровнях их жизненного цикла: этапе проектирования, реализации, развертывания и использования. Актуальными в этом аспекте являются вопросы:

– возможности построения криптосистем, устойчивых к различным типам клептографических атак;

– разработки критериев наличия/отсутствия клептографических закладок;

– синтеза криптографических систем и криптопримитивов с закладками с целью расширения множества шаблонов проектирования закладок для исследования методов их выявления и противодействия им.

Клептографические механизмы разнятся по сценарию построения, способу защиты канала разработчика, уровню абстракции и тому подобное. Известные работы, касающиеся проблем клептографии, фокусируются на отдельных алгоритмах с потенциальной закладкой или построением конкретных протоколов с каналами незаметной утечки секрета, поэтому разнообразие методов в определенной мере размывает общую картину направления. Классификация клептографических механизмов приведена в таблице 1.

Проблемой всех практических клептографических механизмов является то, что даже при нахождении закладки или канала утечки невозможно практически доказать «умышленность» ее построения, поскольку они также могут свидетельствовать лишь о недостаточности имеющихся методов или квалификации аналитиков. Поэтому под криптопримитивом с встроенным клептографическим механизмом мы понимаем такую схему, где только потенциально может быть намеренно организован канал утечки.

Таблица 1

Классификация клептографических механизмов

Тип классификации	Тип клептомеханизма	Примеры
По степени закрытости реализации	Закрытые стандартизованные реализации	Программные библиотеки, схемотехнические описания, спецификации алгоритмов
	Закрытые реализации	Проприетарные программные продукты с обфускацией программного обеспечения и потоков данных
	Аппаратные реализации	Криптографические микроконтроллеры, аппаратные криптомодули
По результатам анализа	Недеструктивные (с возможностью дальнейшего использования)	Анализ программных компонентов, маскирующихся аппаратных компонентов, логический анализ спецификаций и т. д.
	Деструктивные (без возможности дальнейшего использования)	Анализ криптографических контролеров, встроенной EEPROM-памяти и т. д.
По уровню построения	Модификация готовых криптосистем	Добавления канала утечки в реализацию системы, например, атака BEAST протокола TLS1.0 и ниже
	Построение новых криптоалгоритмов со встроенными закладками	Примеры вероятно таких алгоритмов: DES, DualEC, DRGB
По способу внедрения	Открытое распространение клептографических модификаций реализации алгоритмов	Например, в виде программных компонентов
	Распространения проприетарных закрытых криптосистем в виде аппаратных модулей	
	Лоббирование стандартизации клептографических криптосистем, навязывание их использования через правовые механизмы, корпоративные политики или маркетинговые кампании	

3. Краткий обзор современных клептографических механизмов. Приведем несколько примеров, которые, по всей вероятности, содержат клептографические механизмы:

3.1. Алгоритм шифрования DES. Алгоритм симметричного шифрования DES был предложен в 1974 году фирмой IBM, базируется на сети Фейстеля, размер открытого текста и сообщения составляет 64 бит, размер ключа – 56 бит. В оригинальную схему АНБ США был внесен ряд изменений (уменьшение длины ключа с 64 до 56 бит, «помощь» сотрудников АНБ в генерации *S*-блоков), что снизило устойчивость алгоритма к атакам перебора и дифференциальных анализа. Это наводило на подозрения, что такие изменения были внесены преднамеренно для того, чтобы спецслужбы США, имевшие достаточные вычислительные возможности, могли проводить дешифрование сообщений без знания секретных ключей. В частности, есть подозрения, что они владели методами дифференциального криптоанализа до его публикации Бихамом [7].

3.2 Система аппаратного шифрования Skipjack и стандарт EES. Стандарт EES (Escrowed Encryption Standard) аппаратного шифрования разработан АНБ США в рамках проекта Capstone для систем защищенной правительственной связи с закладкой. Стандарт включает в себя блочный алгоритм симметричного шифрования Skipjack и архитектуру LEAF (Law Enforcement Access Field – поле доступа для правоохранительных органов). Для имплементации стандарта использовался защищенный чип Clipper. Предполагалось, что стойкость шифратора будет базироваться на секретном алгоритме шифрования Skipjack, а процесс инициализации ключей будет производиться непосредственно разработчиком чипа. Архитектура LEAF позволяет использовать два ключа расшифрования: один – для пользователя, а другой – для правоохранительных органов. Поэтому разработчики могут расшифровывать перехваченное сообщение, в то время как обычные пользователи могут это делать только с помощью собственных секретных ключей, которые зашиты аппаратно.

3.3. Канал утечки в системах на основе криптографии на эллиптических кривых. Известны как минимум два принципиальных подхода к построению лазейки на базе криптографии на эллиптических кривых:

- генерация криптографически слабой эллиптической кривой, построение и публикация изоморфной к ней (изоморфизм является секретным параметром разработчика);
- использование стойкой эллиптической кривой такого вида, что отсутствие проверки того, что точка находится на кривой приводит к переводу операций над классом кривых, в котором разработчик может за приемлемое время решать задачу дискретного логарифмирования.

Идея первого подхода заключается в том, что разработчик сначала выбирает эллиптических кривую E_s, задачу дискретного логарифмирования которой можно свести к задаче дискретного логарифмирования в поле F_2^N, используя определенную функцию спаривания Вейля так, что последняя практически решается разработчиком. Далее, разработчик строит изоморфную кривую E_{pb}, используя секретное преобразование $\varphi : E_s \to E_{pb}$ методом, описанным в [8]. Затем кривая E_{pb} публикуется (например, как часть стандарта) и используется жертвой. В таком случае задача дискретного логарифмирования, например, поиск $x : xG = P$ по известным *G* и *P*, сложная для пользователя системы, однако разработчик может ее свести к задаче на кривой $E_s : P \to \varphi^{-1}(P), G \to \varphi^{-1}(G)$, что сведением к задаче дискретного логарифмирования над полем остатков по методу, описанному в [9] позволяет разработчику решить задачу ECDLP за приемлемое время.

Клептомеханизм второго подхода продемонстрирован на примере схемы цифровой подписи на базе эллиптических кривых ECKCDSA [10]. Идея заключается в том, что в алгоритм генерации цифровой подписи жертвы вводится ошибка (секретный параметр разработчика), что позволяет ему, перехватив определенное количество подписей жертвы, получить ее секретный ключ.

3.4. Каналы утечки секрета в протоколах. Одним из известных примеров таких механизмов является метод SETUP, который позволяет организовать завладение секретным ключом путем преднамеренной модификации реализации криптосистемы на основе задачи

факторизации больших чисел или задачи дискретного логарифмирования в конечных полях. В настоящее время этот метод является теоретическим (общеизвестных фактов его применения не известно), однако вполне реальный для использования на практике. Другой тип атаки – BEAST (CVE-2011-3389) на протокол SSL до версии TLS 1.0, который использует комбинации уязвимостей XSS (Cross Site Scripting) веб сервиса и Session Fixation в реализации CBC режима шифрования протокола SSL. Злоумышленник может принудить жертву выполнить браузерный код таким образом, что в полученной зашифрованной последовательности нарушается уникальность стартового вектора (CBC режим шифра) для каждого открытого сообщения, позволяя нападающему дешифровать секретную часть сообщения. В действительности, маловероятно, чтобы данная атака была спланированным клептографическим механизмом, однако она имеет определенные признаки такого: вследствие вмешательства в систему жертвы образуется канал скрытной утечки секрета.

Заключение

1. Обозначена актуальность нового направления в защите информации – клептографии и ее связь с криптографией и стеганографией.

2. Введено неформальное понятие клептографического механизма как расширение криптосистемы, которое дает дополнительные возможности разработчику.

3. Приведена общая классификация клептографических механизмов.

4. Продемонстрированы некоторые известные криптопримитивы с встроенным клептографическим механизмом.

Список литературы

1. Жуков, А. Криптография и клептография: скрытые каналы и лазейки в криптоалгоритмах / А. Жуков, А. Маркелова // Information Security. – 2019 – № 1 – С. 36–41.

2. Шелест, М. Е. Клептография vs криптография & стеганография / М. Е. Шелест, Б. А. Коваленко, А. И. Трубей // Теоретическая и прикладная криптография : мат-лы междунар. науч. конф., Минск, 20–21 октября 2020 г. Минск, 2021. – С. 106–113.

3. Simmons, G. J. The Prisoners' Problem and the Subliminal Channel [Электронный ресурс] / G. J. Simmons // Advances in Cryptology: Proceedings of Crypto. – Режим доступа : https://doi.org/10.1007/978-1-4684-4730-95.

4. Simmons, G. J. The Subliminal Channel and Digital Signatures [Электронный ресурс] / G. J. Simmons // Advances in Cryptology. – Berlin, Heidelberg: Springer Berlin Heidelberg, 1985:364–378.

5. Kovalenko, B. Kleptography trapdoor free cryptographic protocols [Electronic resource] / B. Kovalenko, A. Kudin // Cryptology ePrint Archive, Report 2018/989. – Режим доступа : https://eprint.iacr.org/2018/989.

6. Young, A. The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone? / A. Young, , M. Yung // Advances in Cryptology – CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings / editor N. Koblitz. – Berlin, Heidelberg : Springer Berlin Heidelberg, 1996. – P. 89–103.

7. Biham, E. Differential cryptanalysis of DES-like cryptosystems / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – № 4. –P. 3–72.

8. Galbraith, S. D. Extending the GHS Weil Descent Attack. в: Advances in Cryptology / S. D. Galbraith, F. Hess, N. P. Smart // EUROCRYPT 2002 / editor L. R. Knudsen. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. – P. 29–44.

9. Menezes, A. Cryptographic Implications of Hess' Generalized GHS Attack [Electronic resource] / A. Menezes, E. Teske // Cryptology ePrint Archive, Report 2004/235. – Режим доступа : https: // eprint. iacr.org/2004/235. 2004.

10. Bernstein, D. J. How to Manipulate Curve Standards: A White Paper for the Black Hat / D. J. Bernstein, T. Chou, C. Chuengsatiansup // Proceedings of the Second International Conference on Security Standardisation Research. SSR 2015. – Japan : SpringerVerlag, 2015. – P. 109–139.