8. Тимофеев, А.М. Энтропия потерь однофотонного асинхронного волоконно-оптического канала связи с приемником на основе счетчика фотонов с продлевающимся мертвым временем / А.М. Тимофеев // Актуальные проблемы науки XXI века. – 2018. – вып. 7. – С. 5–10.

УДК 004.056

МЕТОДЫ ПОСТРОЕНИЯ КРИПТОСИСТЕМ БЕЗ КЛЕПТОМЕХАНИЗМОВ И ВЫЯВЛЕНИЯ КЛЕПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ

А.И.ТРУБЕЙ, И.Б.БЕРЕЖНОЙ
Учреждение БГУ «НИИ прикладных проблем математики и информатики»
г. Минск, 220030, Республика Беларусь

Введение

Клептография (англ. Kleptography) – раздел криптовирологии, который исследует безопасные и скрытые коммуникации через криптосистемы и криптографические протоколы и асимметричные бэкдоры в криптографических алгоритмах (генерации ключей, цифровой подписи, обмене ключами, генераторах псевдослучайных чисел, алгоритмах шифрования) с целью совершения клептографической атаки. Еще в 1960-х ЦРУ, АНБ и немецкая БНД тайно получили контроль над всеми аспектами деятельности широко известной швейцарской фирмы Crypto AG, производившей шифраппаратуру в коммерческих целях: согласование набора персонала и клиентской базы, влияние на разработку аппаратно-программных средств, а также непосредственное вмешательство в устройства с использованием бэкдоров. Первейшей целью деятельности Crypto AG на протяжении десятилетий стала возможность ЦРУ читать переписку иностранных государств [1].

Действия спецслужб США затронули более 120 стран, в том числе Иран, Аргентину, Ватикан и Саудовскую Аравию. Как отметили в статье швейцарской медиакомпании SRF, «взломанные швейцарские устройства шифрования играли существенную роль, например, в рамках переговоров в Кэмп-Дэвиде в 1979 году, на переговорах об американских заложниках в Иране в 1981 году и во время американского вторжения в Панаму в 1989 году». Кроме того, декодированные телеграммы аргентинского военно-морского флота, передаваемые британцам немцами и американцами, внесли решающий вклад в победу Великобритании в войне 1982 года за Фолклендские острова.

К информационным потокам, которыми оперирует реализация одной из сторон криптосистемы, относятся источники случайности, канал приема данных от других сторон, каналы передачи данных другим сторонам, а также скрытые каналы утечек секрета, если рассматривать в контексте. клептографических модификаций. Для простоты будем считать, что есть только источник случайности (входной канал) и каналы передачи другим сторонам и разработчику (выходные каналы). Под такое упрощение подпадает, например, асимметричный криптопротокол на этапе генерации сессионной пары асимметричных ключей.

1. Мониторинг трафика и контроль целостности собственной реализации

К имеющимся сейчас методам обнаружением лазейки относятся мониторинг трафика и контроль целостности собственной реализации. Недостатками этих методов являются:

1.1 Мониторинг трафика не способен отследить SETUP (одно из требований к SETUP – невозможность наблюдателя отличить модификацию его от оригинала).

1.2 Контроль целостности затруднен тем, что в модели SETUP злоумышленник уже имеет доступ к реализации для модификации, следовательно, он также будет иметь возможность обойти контроль (например, перегенерировать подпись и заменить ключи проверки).

1.3 Если даже абонент имеет возможность контролировать целостность, он не способен проконтролировать целостность реализации своего оппонента.

Ключевым принципом работы системы с доказанной отсутствием клептографических лазеек является то, что ни один из абонентов системы не использует в протоколах внутренние источники случайности, а все псевдослучайные последовательности генерируются на базе публичных уникальных значений (счетчиков) с механизмами доказательства оригинальности (отсутствия модификаций). Это позволяет обеспечить выполнение достаточных условий об отсутствии канала незаметной утечки секрета.

2. Основные принципы создания криптосистемы с защитой от SETUP

К данным принципам относятся:

2.1 Каждый участник системы идентифицируется собственной парой асимметричных ключей.

2.2 Если конкретному участнику необходимо сгенерировать случайную последовательность, он генерирует ее исключительно на основе своего ключа- идентификатора и уникальных открытых значений (счетчиков), генерируемых оговоренным и одинаковым для всех способом (к примеру, простой инкремент.

2.3 В случае генерации такой последовательности, участник должен доказать другим сторонам протокола честность генерации.

То есть, в случае, когда протокол предусматривает использование источника случайности, участник может сгенерировать псевдослучайную последовательность на основе публичного счетчика, с использованием собственного секретного ключа, без использование собственных источников случайности, с невозможностью прогнозирования другими сторонами и возможностью доведения аутентичности данных. Для такой задачи могут быть применены схемы цифровой подписи без рандомизации, например, алгоритм цифровой подписи BLS, строящегося на конечных абелевых группах с определенными билинейными отображениями (например, криптографически стойкие эллиптические кривые с определенными функциями Вейля или Тейта, или алгоритм цифровой подписи RSA без рандомизации).

Подход к генерации псевдослучайной последовательности с публичного счетчика, кроме защиты от клептографических атак, имеет еще одно полезное свойство: он позволяет получить качественный генератор псевдослучайных последовательностей в случае отсутствия собственного источника случайности. Это актуально для виртуальных машин (доступ ко многим аппаратным ресурсам ограничен), систем IoT («интернета вещей»), систем на базе контроллеров без аппаратной поддержки источников случайности, толстых клиентов, когда большая часть логики веб ресурса переводится на мощности клиента, причем как правило средства обработки такой логики имеют ограниченный доступ к системным ресурсам.

3. Основные подходы к клептографическому анализу

Наряду с методами построения клептомеханизмов с доказанной отсутствием клептографических механизмов в криптосистемах важное значение также имеют методы выявления механизмов в существующих стандартах и реализациях.

Существует два принципиально разных подхода к клептографическому анализу:

3.1 Поиск собственного канала утечки через обнаружение модификаций реализации, использования классических методов криптоанализа примитивов и протоколов, анализ поведения абонентов и тому подобное. То есть считается, что криптосистема содержит клептографический механизм, если этот механизм фактически найден.

Преимущества первого подхода – подход является конструктивным, позволяет применить конкретные методы устранения канала утечки, возможна частичная автоматизация процесса обнаружения (например, контроль целостности при загрузке ПО, антивирусные средства и т.п.). Недостатками является наличие ошибки 2-го рода, то есть реально существующий клептомеханизм не обнаруживается в силу малой вычислительной мощности аналитика или ограниченности информации о потенциальной лазейке. Более того, если рассматривать устойчивость клептомеханизма к выявлению как задачу практической неразличимости, принципиально единственная возможность обнаружения – это переход к расширенной модели аналитика, что закладывается в дизайн лазейки. В случае высокого порога предусмотренных мощностей аналитика, это сделать практически невозможно.

3.2 Демонстрация отсутствия способов доказательства отсутствия канала утечки. То есть априори считается, что криптосистема содержит встроенный клептографический механизм, а задача анализа сводится к обоснованию невозможности такого построения. К данному методу, например, относится метод оценки клептографического потенциала, который не демонстрирует пути построения закладки, но показывает, что гипотетически такая возможность существует.

Преимуществами второго подхода является широкое покрытие алгоритмов с возможными каналами утечки и более простые (относительно первого подхода) методы оценки потенциальных каналов. Однако недостатками является наличие ошибки 1-го рода, что допускает наличие больших классов криптосистем, которые определяются как потенциально содержащие клептографические механизмы, хотя на самом деле они отсутствуют. Фактически, согласно этому подходу, криптосистемами без лазейки считаются только те, для которых формально доказано наличие достаточных условий отсутствия канала утечки секрета.

4. Базовая схема построения криптосистем без клептомеханизмов

Поскольку главной целью исследований является повышение уровня защищенности криптосистемы за счет уменьшения клептографических рисков, покажем место отдельных направлений клептографических исследований (клептоанализ, клептосинтез и построение криптосистем с доказанным отсутствием клептомеханизмов) в процессе повышения безопасности криптосистемы.

Построение криптосистем сегодня тесно связано с процессом разработки программных и программно-аппаратных комплексов, реализующих данные криптосистемы. Одной из проблем построения является то, что в связи с высокими темпами внедрений технических решений широко распространены «гибкие» подходы к разработке. Это значит, что на практике сложно внедрить строгий процесс контроля безопасности решений (в том числе и в клептографическом контексте) на каждом этапе жизненного цикла продукта. Фактически

программное проектирование, аудит защищенности продукта и осуществление мероприятий по уменьшению клептографических рисков являются параллельными и непрерывными процессами. В свою очередь, процесс повышения уровня информационной защищенности (в клептографическом контексте) также может состоять из параллельных процессов, что удобно укладывается в концепцию микросервисной архитектуры. На рисунке 1 приведен процесс уменьшения клептографических рисков криптосистемы.

В приведенном процессе (схеме) уменьшения клептографических рисков криптосистемы выходными артефактами является база известных клептографических механизмов, база известных криптографических примитивов и протоколов и собственно целевая криптосистема. Основа схемы – непрерывное взаимодействие параллельных процессов (блоков), каждый из которых отвечает за свою подзадачу.

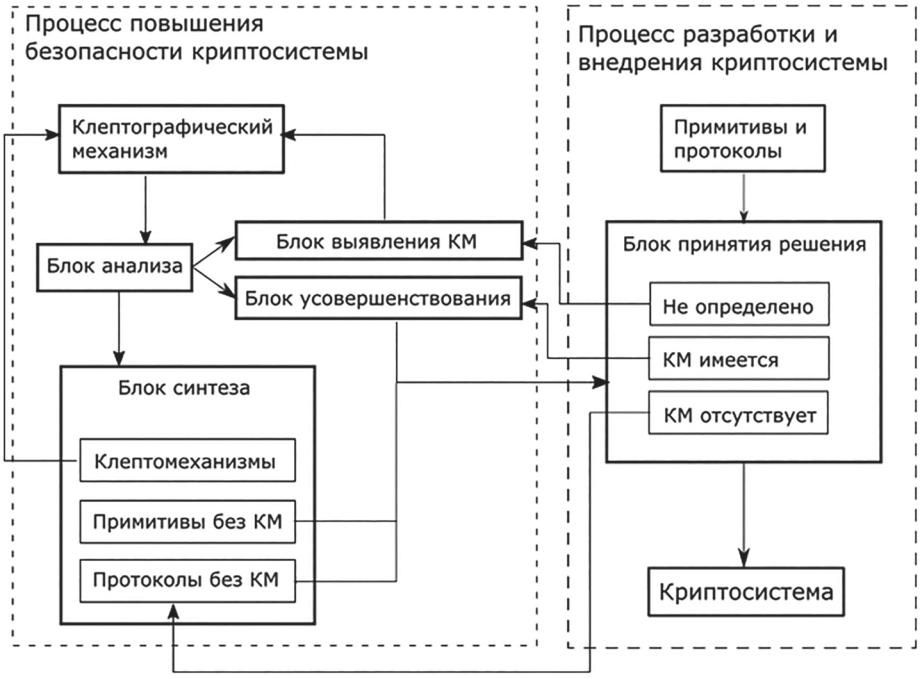

Рисунок 1. Процесс уменьшения клептографических рисков криптосистемы

4.1 Основные блоки в архитектуре схемы:

4.1.1 Блок анализа – анализ клептографических механизмов, классификация, построение формальной модели. На входе блока – известные клептографические механизмы, на выходе – формальная модель.

4.1.2 Блок синтеза – построение криптосистем с клептомеханизмами и с доказанным отсутствием закладок. Синтезированные клептомеханизмы используются для расширения пространства известных клептомеханизмов для дальнейшего анализа. На входе блока – формальные модели закладок и систем без них, на выходе – криптосистемы с закладками и криптосистемы с доказанным их отсутствием.

4.1.3 Блок обнаружения клептомеханизма – выявление клептомеханизма и клептоанализ, целью которого является расширение базы известных клептомеханизмов. На входе блока – криптосистема, определенная как содержащая закладку, на выходе – запись в базу клептомеханизмов.

4.1.4 Блок усовершенствования криптосистемы – модификация криптосистемы с закладкой или без так, чтобы модифицированная система была свободной от клептомеханизма. На входе блока – криптосистема, определенная как та, что содержит закладку, на выходе – модифицированная криптосистема без закладки.

4.1.5 Блок принятия решений – определяет содержит ли данная криптосистема лазейки. Блок принятия решений – это ключевой элемент клептографических взаимодействий мероприятий с реальным процессом разработки. Фактически здесь происходит принятие рисков, связанных с клептографическими атаками. Например, если блок определяет заданный криптопримитив как не содержащий лазейки, это означает только то, что в данном случае использование предполагается, что криптопримитив не содержит лазейки, а соответствующие риски приняты.

Приведенная схема является одним из простых возможных процессов улучшения функционирующей системы с относительно небольшими экономическими затратами, сравнительно с внедрением полного цикла разработки безопасного программного обеспечение, и может применяться ко многим практическим процессам разработки.

Заключение

В статье приведен обзор существующих методов выявления клептографических механизмов и их недостатков. Проведен анализ принципов создания криптографической системы с защитой от SETUP и существующих подходов к клептографическому анализу. Приведена базовая схема построения криптосистем без клептомеханизмов.

Список литературы

1. Endres F., Vögele N. Weltweite Spionage-Operation mit Schweizer Firma aufgedeckt. SRF, 2020 https:// www.srf.ch/news/schweiz/geheimdienstaffaere-cryptoleaks-weltweite-spionage-operation-mit-schweizer-firma-aufgedeckt.
2. Жуков, А., Маркелова, А. Криптография и клептография: скрытые каналы и лазейки в криптоалгоритмах / Information Security / Информационная безопасность – 2019 – № 1 – С. 36–41.
3. Шелест М.Е., Коваленко Б.А., Трубей А.И. Клептография vs криптография & стеганография // Теоретическая и прикладная криптография: Материалы международной научной конференции, Минск, 20–21 октября 2020 г. – С 106–113.
4. Simmons GJ. The Prisoners' Problem and the Subliminal Channel. в: Advances in Cryptology: Proceedings of Crypto 83. за ред. Chaum, D. Boston, MA: Springer US, 1984:51—67. doi: 10.1007/978-1-4684-4730-9_5. url: https://doi.org/10.1007/978-1-4684-4730-9_5.
5. Simmons GJ. The Subliminal Channel and Digital Signatures. в: Advances in Cryptology. за ред. Beth, T., Cot, N., Ingemarsson, I. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985:364—378.
6. 6. Kovalenko B., Kudin A., «Kleptography trapdoor free cryptographic protocols», Cryptology ePrint Archive, Report 2018/989, https://eprint.iacr.org/2018/989.
7. Young, A., Yung, M. The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone? в: Advances in Cryptology — CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings. за ред. Koblitz, N. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996:89—103.
8. Bernstein, DJ., Chou, T., Chuengsatiansup, C та ін. How to Manipulate Curve Standards: A White Paper for the Black Hat Http://Bada55.Cr.Yp.To. в: Proceedings of the Second International Conference on Security Standardisation Research - Volume 9497. SSR 2015. Tokyo, Japan: SpringerVerlag, 2015:109—139. doi: 10.1007/978-3-319-27152-1_6. url: https: //doi.org/10.1007/978-3-319-27152-1_6.