УДК 004.056(043.2)

В.А. Марченко

Інститут кібернетики ім. В.М. Глушкова НАНУ, Київ

ПОБУДОВА СИСТЕМ ОБМІНУ МУЛЬТИМЕДІЙНОЮ ІНФОРМАЦІЄЮ З НЕРОЗКРИВНИМ ШИФРУВАННЯМ ТИПУ «END-TO-END»

В статті описуються деякі підходи побудови систем захисту інформації на базі нерозкривних алгоритмів шифрування для потокових мультимедійних систем. Наведено особливості створення систем захисту типу «end-to-end» для потокових систем обміну мультимедійною інформацією. Описано розроблений апаратно-програмний комплекс захисту на базі ПЦОС - процесорів та приведено особливості його реалізації. Дано рекомендації стосовно особливостей організації ключового обміну та застосування нерозкривних алгоритмів в мультимедійних системах.

Ключові слова: *криптографія, нерозкривні шифри, непряме шифрування, rtsp, rtp, потокова трансляція.*

Вступ

Сучасні системи обміну мультимедійною інформацією представляють собою велике різноманіття різних програмних, апаратних і програмно-апаратних комплексів. В основному вони виконують ряд задач, таких як:

- трансляція аудіо-відео потоку через мережу;
- організація телефонії та відео-телефонії;
- організація зв'язку для різноманітних віддалених конференцій.

Для виконання подібних задач було розроблено стек мережевих протоколів [1] (рис. 1).

В цьому стеці виділено 3 функціональні задачі:

1. Організація управління(сигналізація) послугою.
2. Забезпечення необхідної якості (QoS).
3. Реалізація передачі мультимедіа (Транспорт).

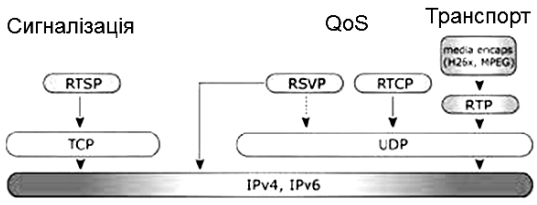

Рис. 1. Стек протоколів
для організації мультимедіа-потоку

Однією з базових особливостей стеку є його інтеграція з популярним стеком телекомунікаційних протоколів TCP\IP[2]. Таким чином, йому властиві всі переваги та недоліки вказаного стеку. Зокрема це

гетерогенність мережевої інфраструктури між користувачами та особливості маршрутизації трафіку в загальнодоступних мережах.

Постановка задачі. Для організації захисту даних в системах на базі цих протоколів слід мати на увазі, що протоколи, які відносяться до різних функціональних задач, можуть оброблюватися в різних підсистемах постачальника. Так типовою є практика при реалізації мультимедіа трансляції або телефонії трафік сигналізації маршрутизується таким чином, щоб він проходив через керуючі сервери постачальника послуги. Це дозволяє забезпечити виконання ряду задач[3]:

- управління та тарифікація послуги;
- адресна книга(для інтернет-телефонії),
- авторизація та аутентифікація користувачів;
- управління послугами QoS.

При цьому сам мультимедійний потік проходить найкоротшим шляхом між користувачами та зазвичай не оброблюється постачальником послуги.

Вказана можливість дозволяє для подібних систем інтегрувати захист з використанням принципу «End-To-End» шифрування. Цей принцип передбачає організацію наскрізного шифрування трафіку між кінцевими користувачами послуги [4].

Виклад основного матеріалу

Шифрування протоколів управління вимагає організацію відповідної інфраструктури на стороні постачальника послуги. При цьому для обробки цього трафіку до відповідних криптографічних параметрів повинен мати доступ окрім кінцевих користувачів і провайдер послуг, що суперечить вказаному принципу організації захисту.

Більш перспективним з точки зору ефективної реалізації вказаного принципу є шифрування тільки самого потоку даних на базі відповідних транспортних протоколів. В яких, по-суті, і знаходиться інформація, яку потрібно захистити від сторонніх користувачів, в тому числі і постачальника послуг.

Одним з найбільш популярних протоколів транспортного рівня для організації передачі мультимедійного потоку є протокол RTP. В основні цього протоколу лежить протокол UDP, що є ймовірнісним протоколом без гарантування передачі даних. Таким чином, задачі організації передачі даних та контроль втрачених пакетів лежать повністю на розробниках систем зв'язку. Сучасні аудіо та відео кодеки, що застосовуються в потокових мультимедійних системах, передбачають можливість втрати пакетів під час передачі без значних втрат в якості аудіо або відео ряду. Ця особливість значно спрощує розробку систем шифрування для потокових систем, але в той же час, висуває ряд вимог до криптосистем, що застосовуються при шифруванні потоків даних:

- потоковий режим роботи;
- незалежність отриманих шифрограм від попереднього тексту, що зашифровано.

Нами було створено апаратно-програмний комплекс шифрування на базі ПЦОС процесорів. В якості алгоритму шифрування, який реалізований в середині апаратної складової, було використано алгоритм непрямого шифрування [5], що відноситься до класу нерозкривних шифрів [6]. Ці алгоритми зазвичай представляють собою потокові алгоритми, таким чином, вони повністю задовольняють першу вимогу. Ключовий потік, що використовується для шифрування даних, генерується незалежно від даних, що шифруються в конкретний момент часу. При цьому у разі зникнення якогось пакету цілком допустимими є пропущення відповідного об'єму ключового потоку з переходом на відповідну позицію згідно з наступного отриманого пакету. Ці особливості, в свою чергу, задовольняють другу вимогу до алгоритмів шифрування.

В розробленому комплексі було реалізовано описаний підхід захисту даних, що передаються по транспортному протоколу RTP. На рис. 2 показано структуру організації системи захисту.

В основі комплексу лежить спеціалізоване програмне забезпечення (Проксі-сервер). Воно складається з двох частин:

- обробник мультимедіа потоку;
- програмний комплекс взаємодії з пристроєм шифрування.

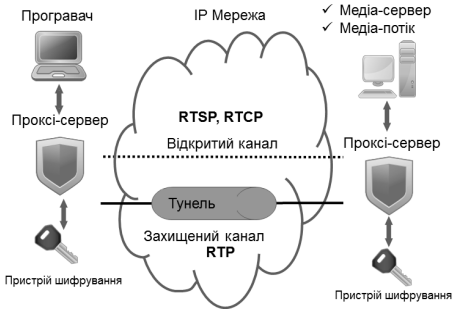

Рис. 2. Структура організації системи захисту

Система захисту працює наступним чином. Після запуску проксі-серверу клієнт отримує медіа-потік з джерела, яким може виступати заданий медіа сервер або інший медіа потік. При цьому у якості протоколу для зв'язку використовується управляючий протокол RTSP. Це простий керуючий протокол текстового формату, що дозволяє керувати запуском, зупинкою медіа потоку та передає ряд параметрів для налаштування підключення та відтворення медіапотоку на клієнтській стороні. Для конфігурування параметрів налаштування зазвичай використовується спеціалізований протокол SDP. В цьому протоколі при встановленні з'єднання відбувається передача з серверу на клієнт текстового масиву налаштувань зокрема:

- адреса та порт вихідного мережевого інтерфейсу;
- тип та параметри мультимедіа потоку.

Після успішного встановлення зв'язку запускається внутрішній RTSP-сервер, який підключає отримані потоки з клієнта та переходить в режим готовності та очікування з'єднань від інших клієнтів. При цьому джерелом мультимедіа потоків вже буде сам проксі-сервер. Тобто під час встановлення з'єднань з вбудованим RTSP-сервером буде передаватись масив налаштувань SDP, в якому в якості вихідного адресу та порту буде виступати адрес і порт комп'ютера з встановленим проксі-сервером, а налаштування медіапотоку передаються без змін. Таким чином, дозволяючи одночасно оброблювати декілька медіапотоків з різних джерел навіть з інших проксі-серверів. Слід зазначити, що згідно специфікацій в рамках організованого з'єднання RTSP кожен вид трафіку (аудіо, відео, текст) передається по окремому мережевому з'єднанню. Тобто якщо йде передача стандартного мультимедіа потоку, що складається з відео ряду та аудіо потоку, то в рамках сесії організовується два з'єднання з одним ідентифікатором сесії, але з різними вихідними мережевими портами.

Ключовою проблемою організації шифрування сесії є проблема узгодження ключів шифрування або параметрів генерації ключового потоку. В стандартних рішеннях на базі симетричних алгоритмів для цих задач використовуються відомі схеми, наприклад різні модифікації алгоритму Дифі-Хелмана [7]. Але цей підхід абсолютно неможливий в системах з використанням нерозкривних алгоритмів, так як в такому випадку повністю нівелюються переваги застосування подібних алгоритмів шифрування. Тому задачі узгодження ключів шифрування (параметрів генерації ключового потоку) слід приділяти особливу увагу. Додатковим обмеженням на процес синхронізації ключової інформації для потокових мультимедійних систем є обмеженість в часі. Зокрема всі параметри для налаштування систем шифрування повинні передаватися в рамках встановленої RTSP сесії. Тобто необхідні параметри повинні передаватись в SDP описі потоку в розділі необов'язкових параметрів. Отже процедура узгодження повинна відбутися в один етап запиту-відповіді. В іншому випадку буде порушено алгоритм встановлення RTSP сесії та організація RTP каналу зв'язку. Одним з можливих варіантів вирішення цієї проблеми є використання вбудованих можливостей засобів шифрування. Зокрема в розробленому пристрої передбачено реалізації синхронізованого сховища ключової інформації для організації захищених сеансів зв'язку між пристроями. Питання конкретних алгоритмів організації ключового обміну виходять за рамки статі та не будуть розглядатися.

Для організації процесу шифрування отримані вбудованим клієнтом RTP пакети ретранслюються на відповідний порт, переданий в конфігураційних параметрах заданого потоку. При цьому виокремлюється тіло пакету, проводиться його криптографічне перетворення та знову інкапсулюється в той самий пакет. Так як в рамках мультимедійного потоку тіло пакету оброблюється на рівні узгодженого аудіо або відео-кодеку, що виключає його перевірку під час передачі по телекомунікаційним лініям зв'язку. Це, в свою чергу, породжує ряд проблем, таких як неможливість в рамках лише мережевої взаємодії визначити проблеми, що утворилися під час проведення процесу криптографічних перетворень та максимально швидко їх виправити.

RTSP-сервер ретранслює отриманий медіапотік іншим пристроям та програмним додаткам. Таким чином, нема необхідності вносити будь-які зміни до сторонніх програмних комплексів або апаратних засобів, що у свою чергу дозволяє прозоро інтегрувати подібну систему в існуючі комплекси.

Висновки

Створення систем захисту типу «End-To-End» є досить популярною задачею в сучасних системах обміну інформацією. Використання нерозкривних шифрів для організації процесу шифрування потоків даних є новою науково-технічною задачею для подібних систем. Розробка та дослідження апаратно-програмного комплексу захисту показала наявність ряду проблем, вирішення яких вимагає розробку нових методів та алгоритмів організації ключового обміну як в рамках мультимедійної сесії, так і між взаємодіючими ключами. При цьому використання саме нерозкривних алгоритмів шифрування дозволяє кардинально змінити рівень захищеності систем обміну навіть для звичайних користувачів.

Список літератури

1. Network Protocols Handbook. – Javvin Technologies, 2005. – 360 p.

2. Comer Douglas. Internetworking with TCP/IP Volume One. – Addison-Wesley, 2013. – 744 p.

3. Wallingford Theodore. Switching to VoIP / Wallingford Theodore. – O'Reilly Media, 2009. – 504 p.

4. Saltzer J.H. End-to-end arguments in system design / J.H. Saltzer , D.P. Reed , D.D. Clark // ACM Transactions on Computer Systems (TOCS). – Nov. 1984. – V.2, n.4. – P. 277-288.

5. Марченко В. Краткая математическая модель метода косвенного шифрования с фиксированными ключами / В. Марченко // Системи обробки інформації. – Х.: ХУ ПС, 2012. – Вип. 4(102). – Т. 1. – С. 128-132.

6. Зубов А. Совершенные шифры / А. Зубов. – М.: Гелиос АРВ, 2003. – 160 с.

7. Diffie W. New Directions in Cryptography / W. Diffie, M.E. Hellman // IEEE Transactions on Information Theory. – Nov. 1976. – Vol. IT-22. – P. 644-654.

Надійшла до редколегії 11.08.2014

Рецензент: д-р техн. наук, проф. Н.І. Алішов, Інститут кібернетики ім. В.М. Глушкова НАН України, Київ.

ПОСТРОЕНИЕ СИСТЕМ ОБМЕНА МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ С НЕРАСКРЫВАЕМЫМ ШИФРОВАНИЕМ ТИПА «END-TO-END»

В.А. Марченко

В статье описываются некоторые подходы построения систем защиты информации на базе нераскрываемых алгоритмов шифрования для потоковых мультимедийных систем. Приведены особенности создания систем защиты типа «end-to-end» для потоковых систем обмена мультимедийной информацией. Описан разработанный аппаратно-программный комплекс защиты на базе ПЦОС - процессоров и приведены особенности его реализации. Даны рекомендации относительно особенностей организации ключевого обмена и применения нераскрываемых шифров в мультимедийных системах.

Ключевые слова: *криптография, нераскрываемые шифры, косвенное шифрование, rtsp, rtp, потоковая трансляция.*

THE CONSTRUCTION OF SYSTEMS FOR SHARING MULTIMEDIA CONTENT WITH UNBREAKABLE ENCRYPTION TYPE «END-TO-END»

V.A. Marchenko

This article describes some of the approaches of building security systems based on unbreakable encryption algorithms for streaming multi-media systems. Peculiarities of creating systems of protection type «end-to-end» for streaming multimedia information exchange systems. The developed hardware-software system protection based on DSP - processors and are the features of its implementation. Recommendations regarding the characteristics of the organization and implementation of key exchange unbreakable ciphers in multimedia systems.

Keywords: *Cryptography, unbreakable ciphers, encryption indirect, rtsp, rtp, streaming.*