Agnieszka CHODOREK, Robert CHODOREK

Standard SRTP

Streszczenie

W artykule omówiony został protokół RTP do transmisji informacji multimedialnej w czasie rzeczywistym oraz jego profil RTP/SAVP, szerzej znany pod nazwą SRTP (Secure RTP), stanowiący rozszerzenie znanego profilu RTP/AVP o kwestie związane z bezpieczeństwem transmisji. SRTP pozwala na uwierzytelnianie pakietu RTP oraz szyfrowanie danych użytkownika (danych medialnych) przenoszonych w pakiecie RTP.

WSTĘP

Protokół transportowy RTP (ang. *Real-time Transport Protocol*) został zaprojektowany do pracy w systemach czasu rzeczywistego. Został on zestandaryzowany w styczniu 1996 dokumentem RFC 1889 [1], który lipcu 2003 roku został zastąpiony dokumentem RFC 3550 [2]. Integralną częścią dokumentacji protokołu RTP jest specyfikacja protokołu RTCP (ang. *Real-time Transport Control Protocol*) - protokołu kontrolno-sterującego, pracującego na potrzeby protokołu RTP. Zarówno RTP, jak i RTCP, są protokołami multikastowymi [1][2][3], co oznacza, że w swym podstawowym trybie pracy realizują transmisję punkt-wielopunkt, a transmisja punkt-punkt (ang. *unicast*) traktowana jest przez te protokoły jako szczególny przypadek transmisji multikastowej.

Protokół RTP został opracowany do zastosowań półprofesjonalnych i profesjonalnych. Jest on jednym z dwóch sztandarowych protokołów architektury MMUSIC, zaprojektowanej jako architektura multikastowej wideokonferencji. A która, dzięki swojej elastyczności i udanym rozwiązaniom, znalazła zastosowanie niemal wszędzie tam, gdzie mamy do czynienia z transmisją multimediów przez sieć teleinformatyczną z zachowaniem warunków czasu rzeczywistego - poczynając od VoIP (ang. *Voice over Internet Protocol*, *Voice over IP*), na IPTV (ang. *IP Television*) kończąc.

Obecnie, ze względu na rozwój systemów webowych, należy się spodziewać, że architektura MMUSIC ustąpi miejsca architekturze WebRTC, która w znacznej mierze została już zestandaryzowana, a standaryzacji pozostałych, specyficznych dla niej rozwiązań protokołowych, należy się spodziewać w niedalekiej przyszłości. Jednak i ta architektura używa protokołu RTP do transmisji informacji multimedialnej (tu: pomiędzy przeglądarkami WWW).

Jedną z ważniejszych kwestii w zastosowaniach profesjonalnych, zwłaszcza biznesowych, jest kwestia poufności oraz wiarygodności przesyłanych informacji. Profil bezpieczeństwa dla protokołu RTP, szerzej znany pod nazwą SRTP (ang. *Secure Real-time Transport Protocol*, *Secure RTP*) wychodzi naprzeciw temu zapotrzebowaniu. SRTP dostarcza narzędzi protokołowych niezbędnych do realizacji szyfrowania i uwierzytelniania pomiędzy urządzeniami końcowymi (nadajnikiem i odbiornikiem lub odbiornikami). SRTP nie definiuje własnej metody szyfrowania, zapewnia natomiast wsparcie dla szyfrowania danych RTP zgodnie ze standardem AES (ang. *Advanced Encryption Standard*).

W artykule zostanie zaprezentowany protokół RTP ze wskazaniem na te jego elementy, które wspierają metody kryptograficzne lub przeciwdziałają metodom kryptoanalitycznym. Zostanie również omówiony profil SRTP protokołu RTP, pozwalający na szyfrowanie danych użytkownika oraz uwierzytelnianie pakietów RTP, a także jego rozszerzenie, pozwalające na szyfrowanie również rozszerzeń nagłówków pakietów protokołu RTP.

1. PROTOKÓŁ RTP

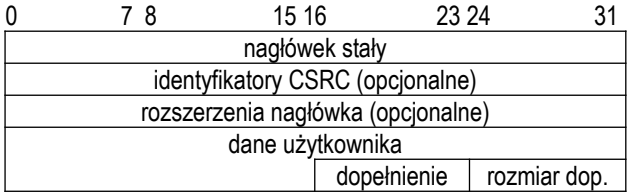
Protokół RTP jest protokołem transportowym przeznaczonym do transmisji informacji (domyślnie: informacji multimedialnej) w czasie rzeczywistym.

1.1. Charakterystyka protokołu RTP

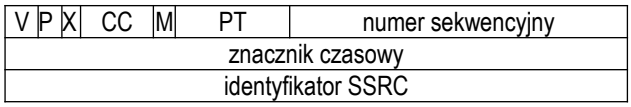
Protokół RTP został opracowany w ramach grupy roboczej *Audio-Video Transport IETF* (ang. *Internet Engineering Task Force* - organizacja zajmująca się standaryzacją Internetu). Protokół ten współpracuje bezpośrednio z protokołem UDP (ang. *User Datagram Protocol*) [3] warstwy transportowej, tworząc stos protokołowy RTP/UDP/IP. Protokoły RTP i RTCP, współpracujące w ramach jednej sesji RTP, typowo wykorzystują dwa kolejne adresy portów UDP - RTP parzysty, a RTCP następny w kolejności (nieparzysty). Takie rozwiązanie pozwala zaimplementować RTP w aplikacjach nadawczych i odbiorczych, a komunikacja protokołu RTP z protokołem UDP odbywa się z wykorzystaniem standardowego interfejsu gniazd (ang. *sockets*). W efekcie, protokół UDP zajmuje dolną podwarstwę warstwy transportowej. Protokół RTP, zajmujący górną podwarstwę warstwy transportowej, korzysta z jego ochrony pakietów za pomocą sumy kontrolnej oraz z multipleksacji połączeń transportowych. Datagramy UDP przenoszące pakiety RTP, które zostaną odrzucone przez UDP jako uszkodzone, będą uznane przez RTP za utracone.

Podobnie protokół RTCP tworzy stos protokołowy RTCP/UDP/IP. Ponieważ jednak protokół RTCP jest protokołem sesyjnym (warstwy sesji modelu odniesienia OSI, ang. *Open Systems Interconnection Reference Model*), protokół UDP w tym przypadku zajmuje całość warstwy transportowej.

a)



b)



Rys. 1. *Format pakietu RTP (oprac. na podst. [1][2]): a) format pakietu, b) format nagłówka stałego*

1.2. Pola wersji i znaczników

Pakiet RTP składa się z nagłówka stałego, dwóch części opcjonalnych nagłówka (identyfikatorów CSRC i rozszerzeń nagłówka) oraz danych użytkownika, które mogą być dopełnione do granicy (najczęściej 32-bitowego) słowa (rys. 1a). Nagłówek stały rozpoczyna dwubitowe pole wersja, którego pierwszy bit jest ustawiony (wersja druga protokołu RTP). Wersja protokołu nie uległa zmianie podczas zmiany specyfikacji RTP z [1] na [2]. Trzeci i czwarty bit nagłówka to bity znaczników. Trzeci bit zawiera znacznik dopełnienia P (ang. *padding*). Jeśli znacznik P jest ustawiony, pole danych zawiera bajty dopełnienia, zakończone bajtem zawierającym rozmiar dopełnienia (rys. 1). Rozmiar dopełnienia liczony jest jako liczba bajtów dopełnienia plus 1 (rozmiar pola rozmiar dopełnienia doliczane

jest do rozmiaru dopełnienia). Dopełnienie jest wymagane m.in. przez szyfry blokowe (operujące na blokach danych). Czwarty bit nagłówka stałego to znacznik rozszerzeń X (ang. *extension*). Jeśli jest ustawiony, nagłówek zawiera przynajmniej jedno rozszerzenie nagłówka. Ostatnie cztery bity pierwszego bajtu nagłówka zawiera pole CC (ang. *CSRC count*), przenoszące liczbę identyfikatorów CSRC zawartych w części opcjonalnej nagłówka. Drugi bajt nagłówka stałego pakietu protokołu RTP zaczyna się jednobitowym znacznikiem M (ang. *marker*), którego znaczenie jest zależne od profilu. Intencją projektodawców było dostarczenie markera, którym można byłoby wskazywać istotne zjawiska występujące w strumieniu multimedialnym.

1.3. Kodowanie formatu danych

Siedem bitów, które pozostało z drugiego bajtu po ulokowaniu tam znacznika M, zostało przeznaczone na pole PT (ang. *payload type*, dosł. typ ładunku) zawierające oznaczenie kodowe formatu danych przenoszonych w pakiecie. Pozwala to aplikacji odbiorczej na szybkie dobranie kodeka pozwalającego na zdekodowanie przesyłanych danych. Zalecane oznaczenia kodowe dla danych audio/wideo zawarte zostały w specyfikacji profilu RTP/AVP (z ang. *Audio/Video Profile*) [4] z lipca 2003 roku. Przykładowo, kod 0 użyty został do oznaczenia kodowania głosu zgodnie ze standardem G.711, tj. kodowanie PCM (ang. *Pulse-Code Modulation*) z kompresją dynamiki z 12 bitów na 8 zgodnie z regułą μ stosowaną w USA i Japonii i częstotliwością próbkowania 8 kHz. Dokument [4] zawiera również kody dla kodeków wideo. Przykładowo, kod 31 oznacza kodowanie H.261 (czyli kompresję wideo stosowaną w sieci ISDN), a kod 34 kodowanie H.263 (kompresja wideo stosowana w systemach wideokonferencji H.323). Dokumenty serii H są wydawane przez ITU (ang. *International Telecommunication Union*).

W sierpniu 2013 roku dokument [4] został uaktualniony - usunięto z niego obowiązek korzystania z formatu audio DVI4, w praktyce niewykorzystywanego [5]. W kwietniu 2010 roku do standardu RTP dodano możliwość multipleksacji RTP i RTCP na pojedynczym porcie UDP [6], co upraszcza korzystanie z NAT (ang. *Network Address Translation*).

1.4. Numeracja sekwencyjna pakietów

Protokół RTP nie implementuje korekcji błędów, ale błędy transmisji są zliczane i raportowane przez odbiornik(i) do nadajnika z wykorzystaniem protokołu RTCP. Detekcja błędów w protokole RTP odbywa się w odbiorniku na podstawie przerw w numeracji sekwencyjnej pakietów. Pakiety RTP są numerowane w kolejności ich nadawania, przy czym zalecane jest, aby (w celu, m.in., utrudnienia kryptoanalizy) numer sekwencyjny pierwszego pakietu był przydzielany losowo. Numery sekwencyjne pozwalają uporządkować pakiety, które (np. ze względu na zadziałanie mechanizmu równoważenia obciążeń) zostały odebrane w kolejności innej niż kolejność ich nadawania. Numer sekwencyjny pakietu RTP jest przenoszony w polu numer sekwencyjny nagłówka stałego tego pakietu (rys. 1b). Pakiety RTCP nie posiadają własnej numeracji sekwencyjnej. Ponieważ profil RTP/SAVP wymaga takiej numeracji, została ona wprowadzona dokumentem [7] na potrzeby tego profilu i obowiązuje jedynie wewnątrz tego profilu oraz wewnątrz jego profili pochodnych.

1.5. Znacznik czasowy

Porządkującą rolę, jaką dla pakietów RTP pełni numer sekwencyjny, dla danych przenoszonych w tym pakiecie pełni znacznik czasowy (ang. *timestamp*). Znacznik czasowy odpowiada chwilom utworzenia pierwszego bajtu danych - pierwszego bajtu próbki głosu lub pierwszego bajtu klatki obrazu wideo (ramki wideo). Pozwala on na uporządkowanie danych w kolejności ich generowania, na odtwarzanie danych zgodnie z tempem ich generowania oraz na pomiar fluktuacji opóźnienia pakietów (ang. *jitter*) wynikającej ze zmiennych warunków transmisji. Wartość znacznika czasowego przenoszona jest w polu znacznik czasowy nagłówka stałego (rys. 1b), a jego wartość początkowa (dla pierwszej próbki danych w strumieniu mediów) powinna być przydzielana losowo. Znaczniki czasowe pozwalają na synchronizację danych w obrębie pojedynczego strumienia, nie pozwalają natomiast na synchronizację strumieni danych między sobą. W tym celu wykorzystywane są zegary odniesienia (ang. *wallclock*), będące źródłem sygnału czasowego. Sygnał ten (czas odniesienia, podawany w formacie NTP, ang. *Network Time Protocol*) wraz z odpowiadającymi mu wartościami znacznika czasowego przenoszony jest w raportach nadajnika RTP, rozsyłanych za pomocą protokołu RTCP.

1.6. Identyfikatory źródeł

Źródło strumienia danych RTP należących do tej samej przestrzeni czasowej (danej znacznikiem czasowym) i numeracyjnej (danej numerem sekwencyjnym) nosi nazwę źródła synchronizującego (ang. *synchronization source*, SSRC, tłumaczone również jako "źródło synchronizacji"). Źródło synchronizujące posiada swój identyfikator, który jest przekazywany nagłówku stałym pakietu RTP, w polu identyfikator SSRC (rys. 1b). Identyfikator SSRC musi być unikalny w skali sesji RTP. Ze źródłem synchronizującym nie jest związany ani format danych (w tym: metoda kodowania i kompresji), ani jego parametry, co oznacza, że mogą się one zmieniać w trakcie transmisji. W szczególności, źródłem synchronizującym może być urządzenie typu mikser, które łączy (miksuje) sygnały (najczęściej audio, rzadziej wideo) nadawane jako osobne strumienie danych w jeden, wspólny sygnał. Mikser nadaje ten sygnał jako własny strumień danych, z własnym identyfikatorem SSRC, a obecność w nim strumieni składowych jest zaznaczana poprzez umieszczenie ich identyfikatorów SSRC w kolejnych polach opcjonalnych identyfikator CSRC (ang. *contributing source*, źródło współbieżne) nagłówka (rys. 1a). Liczba pól przenoszących identyfikatory CSRC jest ograniczona rozmiarem pola CC nagłówka stałego (4 bity, co daje maksimum 15 identyfikatorów CSRC), jednak liczba źródeł realnie współuczestniczących w tworzeniu przekazu oznakowanego danym identyfikatorem SSRC może być większa.

2. PROFIL SRTP

Innym znanym profilem SRTP, oprócz profilu RTP/AVP, jest profil RTP/SAVP (ang. *Secure Audio/Video Profile*), zapewniający ochronę kryptograficzną danych przenoszonych wewnątrz pakietów RTP oraz uwierzytelnianie pakietów.

2.1. Profil RTP/SAVP

Profil RTP/SAVP jest rozszerzeniem profilu RTP/AVP. Został on zdefiniowany w marcu 2004 roku dokumentem RFC 3711 [7]. Ze względu na tytuł dokumentu ("*The Secure Real-time Transport Protocol (SRTP)*") SRTP bywa niekiedy uważany za odrębny protokół, a nie profil. SRTP zapewnia poufność, wiarygodność nadawcy oraz integralność pakietu i strumienia (to ostatnie dzięki uwierzytelnieniu numeracji sekwencyjnej) danych medialnych. Poufność raportowanych danych, wiarygodność oraz integralność pakietu i strumienia dotyczy też SRTP.

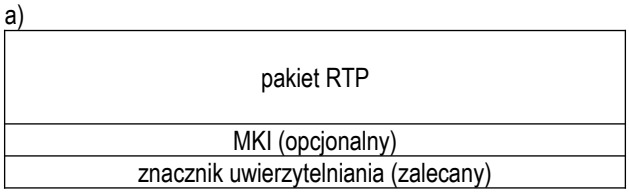
Dokument [7] stanowi, że SRTP jest strukturalnie ulokowany pomiędzy protokołami RTP i UDP. RFC 3711 przybliża również działanie protokołu jako dodatkowej enkapsulacji pakietów RTP w pakiety SRTP. Należy jednak mieć świadomość, że opis ten nie dotyczy pełnego protokołu, a jedynie profilu, który jest "najbardziej zewnętrzną" usługą RTP, ulokowaną (jeśli weźmiemy pod uwagę architekturę protokołu) najbliżej styku międzyprotokołowego RTP/

UDP. Taka lokalizacja jest typowa dla komponentów ochrony (w tym komponentu płaszczyzny bezpieczeństwa), pozwala bowiem chronić gotowy już pakiet wraz z danymi. Podobnie ulokowany jest komponent ochrony, np. w protokole UDP - pakiety UDP (nagłówek wraz z danymi) są chronione sumą kontrolną, której wyznaczanie jest dokonywane już po utworzeniu całego, gotowego pakietu.

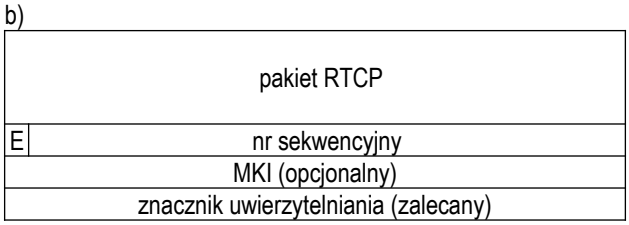
2.2. Rozszerzenia pakietów

Pakiety RTP i RTCP nie przenoszą danych kryptograficznych. Niezbędne zatem stało się uzupełnienie pakietów tych protokołów o pola związane z bezpieczeństwem i ochroną danych. Zostały one dodane jako zakończenia pakietów, (inaczej, niż typowe rozszerzenia, umiejscowione pomiędzy identyfikatorami źródeł a danymi użytkownika). Upodabnia to wizualnie format pakietu RTP do formatu ramek warstwy łącza danych (np. Ethernet), gdzie dane komponentu ochrony (suma kontrolna) umieszczane są nie w nagłówku lecz w zakończeniu. Pozwala to nie modyfikować danych nagłówka po zakończeniu działania komponentu ochrony.

a)



b)



Rys. 2. *Format pakietów RTP i RTCP z rozszerzeniami wprowadzonymi przez profil RTP/SAVP: a) RTP, b) RTCP*

SRTP rozszerza pakiet RTP (rys. 1a) o dwa pola o konfigurowalnej długości, stanowiące zakończenie pakietu (rys. 2a). Pole MKI (ang. *Master Key Identifier*) jest polem opcjonalnym, przenoszącym klucz główny, na podstawie którego będą tworzone klucze kryptograficzne sesji, wykorzystywane do ochrony konkretnego pakietu. Klucz główny jest kluczem losowym, prywatnym. Pole znacznik uwierzytelniania jest polem zalecanym, używanym do przenoszenia informacji uwierzytelniającej. SRTP uwierzytelnia pakiet wraz z danymi użytkownika. Jeśli dane użytkownika są szyfrowane, szyfrowanie powinno się odbyć przed uwierzytelnianiem.

SRTP rozszerza pakiet RTCP o cztery pola (rys. 2b), z czego dwa, MKI oraz znacznik uwierzytelnienia) są polami o konfigurowalnej długości, a ich znaczenie jest identyczne, jak analogicznych pól rozszerzających pakiet RTP. Jednobitowe pole E jest polem znacznika zaszyfrowania (ang. *encrypted*). Jeżeli bit E jest ustawiony, zawartość pakietu jest zaszyfrowana, a jeżeli jest wyzerowany, zawartość pakietu jest jawna. Pole nr sekwencyjny jest 31-bitowym licznikiem pakietów RTCP, zerowanym przed wysłaniem pierwszego bajtu danych użytkownika oraz po każdej zmianie klucza kryptograficznego. Po każdym wysłaniu pakietu RTCP wartość licznika jest zwiększana o 1.

2.3. Kontekst kryptograficzny

Zmienne stanu ochrony kryptograficznej noszą nazwę kontekstu kryptograficznego (ang. *cryptographic context*). Kontekst kryptograficzny jest jednoznacznie identyfikowany przez trójkę `(s,a,p)`, gdzie `s` jest identyfikatorem SSRC źródła, `a` jest adresem IP odbiornika(ów), zaś `p` jest numerem portu. W skład kontekstu kryptograficznego wchodzą zmienne zależne i niezależne od użytej metody kryptograficznej. Te pierwsze to, przykładowo, rozmiar bloku szyfru blokowego czy klucze sesyjne. Do tych drugich należą, między innymi, licznik przepełnień ROC (ang. *rollover counter*) pola numeracji sekwencyjnej, identyfikatory algorytmów szyfrowania i uwierzytelniania, znacznik MKI (wskazujący, czy pole MKI znajduje się w pakiecie) i rozmiar pola MKI, klucz(e) główny(e), czas życia klucza głównego. Kontekst kryptograficzny SRTCP zasadniczo zbliżony jest do opisanego wyżej kontekstu SRTP. Wyjątek stanowi brak licznika przepełnień ROC, zastąpionego przez własny, 31-bitowy licznik numeracji sekwencyjnej (rys. 2b). Do kontekstów kryptograficznych obu protokołów należą też listy powtórek (ang. *replay list*), przechowywane w odbiorniku, zawierające identyfikatory ostatnio otrzymanych uwierzytelnionych pakietów, chroniące przed atakiem z wykorzystaniem fałszywego źródła wysyłającego powtórzone (przechwycone w sieci) pakiety. Każdy z protokołów ma swoją własną listę powtórek.

2.4. Schemat działania ochronnego

Przetwarzanie zgodne z SRTP rozpoczyna się zawsze od określenia bieżącego kontekstu kryptograficznego dla danej trójki `(s,a,p)` oraz wyznaczenia rzeczywistego numeru sekwencyjnego (na podstawie bieżącego numeru sekwencyjnego i licznika ROC). W dalszej kolejności wyznacza się klucz główny (np. na postawie MKI) oraz główny ciąg zaburzający (ang. *master salt*), a następnie klucz sesyjny i sesyjny ciąg zaburzający. Mając to wszystko, w nadajniku dokonuje się szyfrowania danych i(lub) uwierzytelnienia całego pakietu, zgodnie z metodami podanymi w kontekście. Nadajnik zakończy pakiet RTP polem MKI (jeśli znacznik MKI jest ustawiony) oraz znacznikiem uwierzytelniania. Odbiornik odczytuje informacje z zakończenia i usuwa zakończenie, po czym dokonuje najpierw sprawdzenia obecności pakietu na liście powtórek. Jeśli pakiet znajduje się na liście, jest on odrzucany, a zdarzenie obecności na liście powinno zostać zanotowane. W następnej kolejności dokonuje się uwierzytelnienia pakietu RTP. Jeśli operacja nie powiodła się, pakiet a wystąpienie niepowodzenie uwierzytelnienia powinno zostać zanotowane. Jeśli uwierzytelnienie powiodło się, następuje deszyfracja danych przenoszonych w pakiecie. Ostatnim krokiem dokonywanym przez oba systemy końcowe jest uaktualnienie licznika ROC (o ile zachodzi taka potrzeba).

2.5. Ochrona kryptograficzna

Ani protokół RTP, ani jego profil RTP/SAVP, nie definiują swojej własnej metody ochrony kryptograficznej. Zarówno w przypadku szyfrowania, jak i uwierzytelniania, korzystają z typowych, uznanych metod ochrony. Do zapewnienia poufności danych wykorzystany został szyfr AES pracujący w trybie CTR (ang. *counter-mode*, *CTR mode, CM*). Szyfr ten zostanie omówiony w następnym podrozdziale. Warto zauważyć, że operacja szyfrowania/deszyfrowania realizowana jest zawsze, nawet jeśli pole danych ma nie być szyfrowane. W tym drugim wypadku, do szyfrowania wykorzystuje się tzw. szyfr zerowy (ang. *NULL cipher*) polegający na wykonaniu operacji XOR (różnica symetryczna) każdego bitu danych z ciągiem bitów o wartości zero. Do zapewnienia wiarygodności przesyłanych danych wykorzystywana jest metoda HMAC (ang. *Hashing Message Authentication Codes*), zestandaryzowana dokumentem RFC 2104 z lutego 1997 roku [8]. Jest ona rozwinięciem metody bazującej na tajnym kluczu MAC (ang. *message authentication code*) o kryptograficzne funkcje skrótu (ang. *hash function*; spotykane są również tłumaczenia: funkcja mieszająca lub funkcja haszująca). Standard SRTP wykorzystuje funkcję SHA-1 (ang. *Secure Hash Algorithm*, liczba 1 oznacza wersję algorytmu), tworzącą 160-bitowy skrót wiadomości.

Sam algorytm HMAC pozwala na korzystanie z dowolnych funkcji skrótu, w tym z kolejnej wersji rozwojowej algorytmu SHA, funkcji SHA-2 (tworzącej skrót 256- lub 512-bitowy).

2.6. Szyfr AES

Szyfr AES jest szyfrem blokowym operującym na blokach danych o rozmiarze 128 bitów, symetrycznym (do szyfrowania i deszyfrowania wykorzystywany jest ten sam klucz). Standard AES dopuszcza szyfrowanie kluczem 128, 192 i 256-bitowym, przy czym RFC 3711 [7] implementuje obowiązkowo jedynie klucz 128-bitowy (główny i sesyjny). Klucze o długości 192 i 256 bitów zostały wprowadzone do profilu RTP/AVP dopiero w marcu 2011 roku, dokumentem RFC 6188 [9]. Ciągi zaburzające (główny i sesyjny) mają długość 112 bitów. Samo szyfrowanie polega na wykonaniu operacji XOR na bitach znajdujących się w polu danych użytkownika i strumieniu klucza AES-CTR, generowanego na podstawie klucza sesyjnego i 128-bitowego wektora inicjującego (ang. *initialization vector, IV*). Wektor inicjujący tworzony jest na bazie sesyjnego ciągu zaburzającego, identyfikatora SSRC i rzeczywistego numeru sekwencyjnego pakietu RTP. Sposób działania szyfru AES w trybie CTR jest zbliżony do szyfrów strumieniowych.

2.7. Wymiana kluczy i szyfrowanie rozszerzeń nagłówka

Standard SRTP definiuje ramy zarządzania kluczami, ale nie definiuje bezpiecznego mechanizmu wymiany kluczy. RFC 3711 [7] wskazuje jedynie, że zarówno klucz główny, jak i pozostałe elementy kontekstu kryptograficznego są dostarczane do SRTP za pomocą zewnętrznego mechanizmu zarządzania kluczami. Klucze wymieniane pomiędzy nadajnikiem a odbiornikiem (lub odbiornikami) RTP często są szyfrowane z wykorzystaniem protokołu TLS (ang. *Transport Layer Security*). Można też wykorzystać [10] protokół DTLS DTLS (ang. *Datagram Transport Layer Security*).

Profil RTP/SAVP szyfruje jedynie dane użytkownika. Tym niemniej, w polach rozszerzeń nagłówka też bywają przenoszone są dane wrażliwe. Szyfrowanie rozszerzeń pakietu RTP, zgodne z RFC 6904 [11] pozwala na szyfrowanie wybranych pól rozszerzeń nagłówka (niektóre dane z nagłówków RTP mogą być wykorzystywane przez systemy pośredniczące). Wybór pól odbywa się z wykorzystaniem maski nagłówka, tj. szablonu nagłówka, w którym bajty pól podlegających ochronie kryptograficznej mają wszystkie bity ustawione (wszystkie bity przyjmują wartość 1, czyli wartość bajtu wynosi 255), zaś bajty pól przesyłanych w sposób jawny mają wszystkie bity wyzerowane (wartość pola wynosi 0). Maska jest wyznaczana osobno dla każdego pakietu zawierającego rozszerzenie nagłówka.

PODSUMOWANIE

Standard SRTP to profil protokołu RTP zapewniający szyfrowanie danych medialnych przenoszonych w pakietach RTP i raportów RTSP oraz uwierzytelnianie pakietów obu tych protokołów. SRTP zapobiega zarówno nieautoryzowanemu dostępowi do treści strumienia mediów i raportów o stanie transmisji, jak również zapobiega atakom na strumień mediów, polegającym na podmianie całości części strumienia i zastąpienie go nową treścią lub treścią uprzednio przechwyconą, należącą do tego samego strumienia. Użycie SRTP jest obecnie zalecane w zastosowaniach VoIP.

BIBLIOGRAFIA

1. Schulzrinne H., Casner S., Frederick R., Jacobson V., *RTP: A Transport Protocol for Real-Time Applications*. RFC 1889, IETF, 1996.
2. Schulzrinne H., Casner S., Frederick R., Jacobson V., *RTP: A Transport Protocol for Real-Time Applications*. RFC 3550, IETF, 2003.
3. Chodorek R. R., Pach A. R., *Transmisja multikastowa w sieciach IP*. Wydawnictwo FPT, Kraków 2003.
4. Schulzrinne H., Casner S., *RTP Profile for Audio and Video Conferences with Minimal Control*. RFC 3551, IETF, 2003.
5. Terriberry T., *Update to Remove DVI4 from the Recommended Codecs for the RTP Profile for Audio and Video Conferences with Minimal Control (RTP/AVP)*. RFC 7007, IETF, 2013.
6. Perkins C., Westerlund M., *Multiplexing RTP Data and Control Packets on a Single Port*. RFC 5761, IETF, 2010.
7. Baugher M., McGrew D., Naslund M., Carrara E., Norrman K., *The Secure Real-time Transport Protocol (SRTP)*. RFC 3711, IETF, 2004.
8. Krawczyk H., Bellare M., Canetti R., *HMAC: Keyed-Hashing for Message Authentication*. RFC 2104, IETF, 1997.
9. McGrew D., *The Use of AES-192 and AES-256 in Secure RTP*. RFC 6188, IETF, 2011.
10. Fischl J., Tschofenig H., Rescorla E., *Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)*. RFC 5763, IETF, 2010.
11. Lennox J., *Encryption of Header Extensions in the Secure Real-time Transport Protocol (SRTP)*. RFC 6904, IETF, 2013.

THE SRTP STANDARD

Abstract

In the paper, the Real-time Transport Protocol (RTP), intended for real-time transmission of multimedia information was described, as well as its RTP/SAVP profile, also known as the Secure RTP (SRTP), which extends the well-known Audio/Video Profile of the RTP with security. The SRTP allows for authentication of RTP packets and encryption of the payload of RTP's packet (de facto, encryption of media data).

Autorzy:
dr inż. **Agnieszka Chodorek** – Politechnika Świętokrzyska, Wydział Elektrotechniki, Automatyki i Informatyki, Katedra Systemów Informatycznych; 25-314 Kielce; al. Tysiąclecia Państwa Polskiego 7.
E-mail: a.chodorek@tu.kielce.pl
dr inż. **Robert Chodorek** – AGH Akademia Górniczo-Hutnicza, Wydział Informatyki, Elektroniki i Telekomunikacji, Katedra Telekomunikacji; 30-059 Kraków; Al. A. Mickiewicza 30.
E-mail: chodorek@agh.edu.pl