Możliwości wykorzystania watermarkingu do zabezpieczenia telefonii IP

WOJCIECH MAZURCZYK
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: W.Mazurczyk@elka.pw.edu.pl
http://security.tele.pw.edu.pl

Streszczenie

W artykule przedstawiono sposoby zastosowania metod wykorzystujących oznaczanie głosu cyfrowym znakiem wodnym (*watermarking*) do zabezpieczania telefonii IP. Na wstępie przedstawiono obecne problemy bezpieczeństwa dla systemów telefonii IP oraz ich źródła. Zdefiniowano kryterium określające, jakie usługi ochrony informacji i komunikacji w sieci musi spełnić system telefonii IP, aby można go uznać za bezpieczny. Następnie przedstawiono, jakimi parametrami powinien charakteryzować się cyfrowy znak wodny, aby mógł być wykorzystany do zabezpieczania telefonii IP.

Zaproponowano możliwe scenariusze wykorzystania metod oznaczania cyfrowym znakiem wodnym do zapewnienia usług uwierzytelnienia oraz integralności dla głosu oraz wymiany wiadomości sygnalizacyjnych. Wykorzystanie przedstawionych tutaj rozwiązań ma szansę stać się realną alternatywą dla klasycznych mechanizmów zdefiniowanych w obecnych standardach.

1. Wprowadzenie

Telefonia IP obecnie, w znaczącym stopniu, wpływa na kształt rynku telekomunikacyjnego na świecie. Większość liczących się operatorów telekomunikacyjnych migruje z transportem głosu z sieci z komutacją łączy do sieci z komutacją pakietów – najczęściej wykorzystujących protokół IP. Ostatnio mamy również do czynienia z fenomenem takich rozwiązań software'owych jak np. Skype. W dość krótkim czasie i przy stosunkowo małych nakładach finansowych zdobył on dość pokaźną liczbę abonentów i już niedługo może stanowić poważną konkurencję dla dużych firm telekomunikacyjnych.

Mimo rosnącej popularności usług, które niesie za sobą telefonia IP, propozycji kolejnych rozwiązań, standardów i protokołów cały czas sprawą zaniedbaną i pozostawioną w cieniu, jest kwestia jej **bezpieczeństwa**. Mamy do czynienia z nieco podobną sytuacją, jaką można zaobserwować w przypadku technologii *wireless*. Pomimo tego, iż powszechnie znane są luki w architekturze bezpieczeństwa rozwiązań bezprzewodowych – produktów i klientów na rynku przybywa coraz więcej. W przypadku telefonii IP jest natomiast tak, że dla wielu rozwiązań zdefiniowano poprawną architekturę bezpieczeństwa dla tej usługi, ale się jej nie implementuje.

Można, więc zadać pytanie: dlaczego tak rzadko stosuje się odpowiednie, często już zdefiniowane w standardach mechanizmy zabezpieczeń dla telefonii IP? Odpowiedź wynika bezpośrednio z jednej z jej głównych cech – **wrażliwości na opóźnienia**. Małe (mniejsze niż 150ms) sumaryczne opóźnienia na całej drodze komunikacyjnej są gwarantem poprawnej jakości pakietowej usługi głosowej. Natomiast zachowanie tej wartości już nawet bez zaimplementowania mechanizmów zabezpieczeń jest trudne do osiągnięcia, co opisano na przykładzie usługi VoIP w [1]. Dodatkowo występują jeszcze opóźnienia wprowadzane poprzez małą kompatybilność Firewalli oraz urządzeń wykorzystujących technikę NAT z systemami przenoszącymi głos w czasie rzeczywistym. Efektem tego jest brak lub bardzo mała ilość dostępnego czasu na realizację usług ochrony informacji.

Do zabezpieczania wykorzystuje się obecnie również inne rozwiązania: np. VPN (*Virtual Private Networks*), czy ALG (*Aplication Level Gateway*).Tu jednak możemy natknąć się na problemy ze skalowalnością, a dane rozwiązanie musi być bezwzględnie dopasowane do sieci, w której je stosujemy. Jednym słowem da się zabezpieczyć telefonię IP, ale nie ma ogólnej recepty na jej bezpieczeństwo.

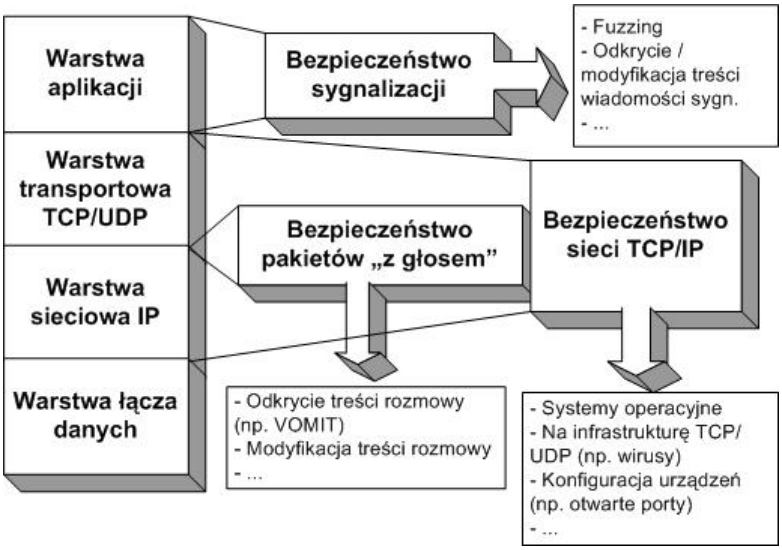
Sytuacja taka zmusza do rozpoczęcia poszukiwań nowych, skuteczniejszych i bardziej elastycznych rozwiązań zapewnienia bezpieczeństwa systemom telefonii IP.

2. Od czego zależy bezpieczeństwo telefonii IP?

Różnorodność źródeł oraz rodzajów potencjalnych zagrożeń bezpieczeństwa dla systemów telefonii IP jest o wiele większa niż w przypadku jej klasycznego odpowiednika. Przyczynia się do tego paradoksalnie ten sam fakt, który stanowi również o popularności tego typu rozwiązań: bardzo dynamiczny rozwój sieci IP, a w szczególności Internetu. Zapewnienie bezpieczeństwa systemom telefonii IP jest sprawą złożoną, a problemy z tym związane można podzielić na trzy grupy zagadnień:

- Bezpieczeństwo wiadomości sygnalizacyjnych protokołu sygnalizacyjnego, na którym bazuje telefonia IP,
- Bezpieczeństwo pakietów „z głosem" (np. dla VoIP są to pakiety RTP),
- Bezpieczeństwo środowiska i sieci z protokołem IP.

Z przedstawionych powyżej grup zagadnieniem niesłusznie zapominanym i pozostawianym na uboczu jest bezpieczeństwo protokołów sygnalizacyjnych. Nie przypadkowo protokoły te nazywa się „sercem" telefonii IP, gdyż to właśnie od nich zależy architektura systemu oraz nawiązywanie/sterowanie połączeniami. Brak odpowiedniej dbałości o bezpieczeństwo protokołu sygnalizacyjnego, na którym bazuje dane rozwiązanie pakietowej usługi głosowej może mieć trudne do przewidzenia skutki, czego dowiodły wyniki opublikowane w [8] i [9].
Powyższy podział zagadnień bezpieczeństwa telefonii IP został przedstawiony na rysunku 1 z uwzględnieniem modelu odniesienia TCP/IP oraz przykładowych ataków i słabości.



Rys. 1. Bezpieczeństwo systemów telefonii IP w odniesieniu do modelu TCP/IP

Esencję bezpieczeństwa systemów telefonii IP określa kryterium przedstawione w [2]. Będące modyfikacją kryterium z normy ISO 7498-2 i uwzględniające cechy charakterystyczne systemów telefonii IP stwierdza, iż warunkiem koniecznym i wystarczającym do uznania protokołu sygnalizacyjnego za bezpieczny jest zapewnienie usług ochrony informacji i komunikacji w sieci: **poufności** oraz **uwierzytelnienia**.
Zdefiniowane w [2] kryterium stosowane było dotychczas jedynie do oceny bezpieczeństwa protokołów sygnalizacyjnych VoIP. Będzie ono również poprawne, jeśli jego zastosowanie rozszerzymy na zagadnienia dotyczące bezpieczeństwa pakietów przenoszących głos oraz protokołów sygnalizacyjnych innych niż VoIP. Stąd możemy sformułować bardziej ogólne kryterium: **bezpieczeństwo systemu telefonii IP** zależy od poprawności zapewnienia następujących usług ochrony informacji i komunikacji w sieci:

- **Poufności** – dającej ochronę przed atakami pasywnymi oraz zabezpieczającej wiadomości sygnalizacyjne [oraz pakiety „z głosem"]*, wymieniane pomiędzy komunikującymi się jednostkami, przed ich nieuprawnionym uzyskaniem przez strony do tego nieupoważnione;
- **Uwierzytelnienia (zawierającego usługę integralności)** – gwarantującego ochronę przed atakami aktywnymi oraz kontrolę tożsamości stron, wiadomości sygnalizacyjnych [oraz pakietów „z głosem"*] wymienianych pomiędzy nimi.

* oznaczono części tekstu dodane w porównaniu z kryterium zdefiniowanym w [2]; sformułowanie „pakiety z głosem" użyte zostało celowo, aby uwzględnić te systemy telefonii IP, które nie wykorzystują protokołu RTP.

Dodatkowo możemy również rozróżnić w ramach usługi uwierzytelnienia: **uwierzytelnienie pełne** (uwierzytelnienie + integralność) oraz **niepełne** (tylko usługa uwierzytelnienia).

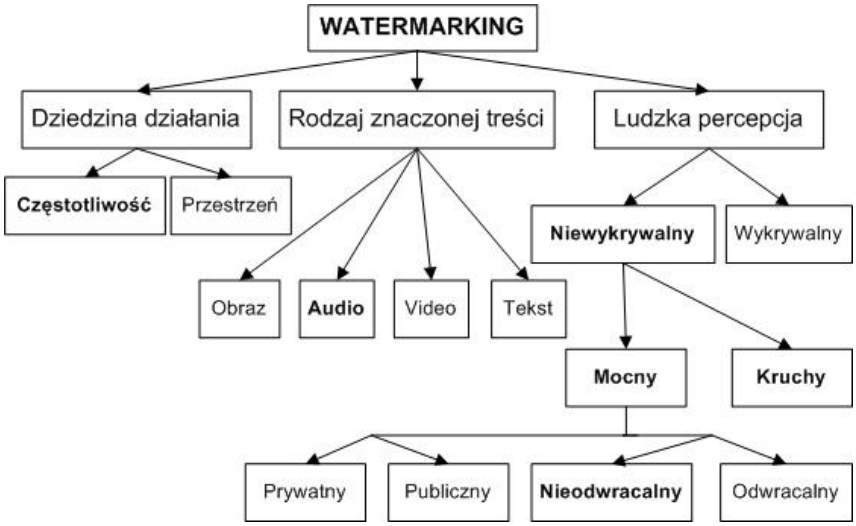
Tak jak wspomniano wcześniej, obecne mechanizmy zabezpieczeń dla telefonii IP definiują często poprawną architekturę bezpieczeństwa zarówno dla sygnalizacji, jak i głosu. Należy jednak wziąć pod uwagę następujące argumenty:

- Stosuje się je rzadko lub wcale (szczególnie w odniesieniu do sygnalizacji),
- Stworzono osobne sposoby zabezpieczania wiadomości sygnalizacyjnych oraz głosu, co powoduje dublowanie się opóźnień i zwiększanie wymagań na moc obliczeniową urządzeń na drodze komunikacyjnej.

W następnej części artykułu rozważymy, czy zastosowanie metod wykorzystujących *watermarking* pozwoli na rozwiązanie powyższych problemów przy jednoczesnym spełnieniu zdefiniowanego powyżej kryterium.

3. Nowe możliwości: watermarking

Ogromna popularność sieci Internet, jak również rozwój handlu elektronicznego i elektronicznych kanałów dystrybucji treści spowodowały powstanie nowych wyzwań związanych z ochroną wartości intelektualnej. Coraz trudniej jest zabezpieczyć nośnik przeciwko skopiowaniu, a coraz łatwiejsze i tańsze staje się jego powielenie. Istotne jest zaproponowanie metod i technik gwarantowania praw autorskich dla informacji. Jedną z propozycji rozwiązania powyższych problemów jest **watermarking** (oznaczanie cyfrowymi znakami wodnymi), którego podstawową zasadą działania jest wbudowywanie dodatkowych informacji do zabezpieczanych danych. Obecnie szerokie zastosowanie tych metod ograniczają wymagania istnienia centrów autoryzacyjnych certyfikatów oraz serwerów centralnych do zapewnienia unikalności znaku wodnego. Są to wymagania większości protokołów wykorzystujących oznaczanie cyfrowymi znakami wodnymi. Innymi warunkami, jakie muszą spełniać tego typu rozwiązania to m.in. istnienie rozłącznych kluczy dla każdej transakcji lub ujawnienie swojego klucza prywatnego w przypadku konieczności udowodnienia swojego autorstwa.
Podział metod wykorzystujących *watermarking* w zależności od różnych czynników tj. dziedziny działania, rodzaju znaczonej treści oraz ludzkiej percepcji w odniesieniu do znaku wodnego przedstawia rysunek 2:



Rys. 2. Podział watermarkingu ze względu na dziedzinę działania, rodzaj znaczonej treści oraz ludzką percepcję

Jak widać z powyższego rysunku pod pojęciem *watermarkingu* kryje się wiele różnych technik oraz metod - jest to bardzo popularny temat rozważań naukowców ostatniej dekady. Mimo tej różnorodności ideę oznaczania cyfrowym znakiem wodnym można sprowadzić do dwóch podstawowych algorytmów:

- **Wbudowującego** cyfrowy znak wodny w oznaczane dane (*ang. Embedding Algorithm*),
- **Ekstrakcji** cyfrowego znaku wodnego z oznaczanych danych (*ang. Extraction Algoritm*).

W dalszej części artykułu będziemy rozważać możliwość zastosowania *watermarkingu* dla zabezpieczania telefonii IP.

4. Cechy znaku wodnego i usługi ochrony przez niego realizowane

W naszych rozważaniach ograniczymy się jedynie do tych aspektów *watermarkingu*, które wyróżniono pogrubieniem na rysunku 2, czyli dziedzina działania: częstotliwość oraz rodzaj znaczonej treści: audio. Zawężenie to wynika z naszych poszukiwań możliwego wykorzystania do oznaczania cyfrowymi znakami wodnymi do zabezpieczania usługi czasu rzeczywistego, jaką jest telefonia IP.
Przedstawmy, więc cechy, którymi powinien charakteryzować się cyfrowy znak wodny tak, aby można go wykorzystać dla systemów telefonii IP, uwzględniając zbiór parametrów zdefiniowanych w [4]:

- **Żywotność** znaku wodnego opisuje, czy może on zostać wykryty również po przeprowadzeniu pewnych operacji (nie ataków!) na oznaczanych danych. Chodzi tu np. o zmianę kodowania w trakcie transmisji sygnału, czy konwersję AD/DA,
- **Bezpieczeństwo** opisuje, czy wbudowana informacja jest odporna na celowe ataki, aby mimo prób jej usunięcia lub osłabienia mogła być wiarygodnie wykryta,
- **Niewykrywalność** (przezroczystość) – wbudowanie znaku wodnego nie może powodować zmian w jakości głosu w trakcie komunikacji, czyli dla percepcji człowieka musi być przezroczyste,
- **Złożoność** – parametr ten mówi nam o złożoności obliczeniowej procesu wbudowania\ekstrakcji znaku wodnego, co nie jest bez znaczenia szczególnie dla systemów czasu rzeczywistego, jakimi są systemy

telefonii IP (dąży się, aby wykorzystywany algorytm był jak najprostszy). Złożoność determinuje, iż wymaganym przez nas rodzajem watermarkingu będzie tzw. *blind watermarking.* W związku z tym nie potrzeba będzie oryginalnych danych do stwierdzenia, czy znak wodny został wpisany, czy nie,

- **Pojemność** – charakteryzuje ilość informacji (liczbę bitów), którą możemy wpisać,
- **Weryfikacja** – dla tej cechy mamy do wyboru weryfikację prywatną lub publiczną. Jest to sposób opisu wbudowywania/detekcji znaku wodnego odnoszący się do kryptografii – prywatny oznacza detekcję z kluczem prywatnym, natomiast publiczny – odpowiednik PKI dla watermarkingu.

Optymalizacja wybranych parametrów wpływa na wartość innych. Niezbędny jest na każdym kroku wyważony kompromis w zależności od tego, na jakich cechach najbardziej nam zależy.
Na początku wskażemy, jakie usługi ochrony informacji i komunikacji w sieci gwarantuje nam zastosowanie techniki *watermarkingu*, a następnie określimy, jakie parametry są najważniejsze z punktu widzenia ich przydatności dla telefonii IP. Po analizie dostępnych klas oznaczania cyfrowymi znakami wodnymi zawartych w [4] należy stwierdzić, że możliwe do osiągnięcia są dwie usługi: **uwierzytelnienie** i **integralność**, czyli uwzględniając nazewnictwo wprowadzone podczas definiowania kryterium, **uwierzytelnienie pełne**. Najprostszy sposób, w jaki można osiągnąć zapewnienie tej usługi ochrony polega na włączeniu określonych danych charakterystycznych dla nawiązującego połączenie oraz charakteryzujących samą przenoszoną treść.
Jeśli wskazane usługi ochrony informacji i komunikacji w sieci odniesiemy do zdefiniowanego wcześniej kryterium to widzimy, że wykorzystując *watermarking* **nie jest** możliwe zapewnienie usługi poufności. Wynika to przede wszystkim z charakteru samego *watermarkingu* jako techniki steganograficznej – „zanurzonej w zawartości". Chodzi tu przecież o stworzenie dodatkowego kanału informacji, aby możliwe było przeniesienie określonych informacji w kanale odkrytym bez wiedzy lub możliwości ich ujawnienia przez potencjalnego intruza. Czy brak możliwości zapewnienia usługi poufności dyskredytuje oznaczanie cyfrowym znakiem wodnym, jako technikę dla zabezpieczenia telefonii IP? Na pewno nie, co postaramy się udowodnić w dalszej części tego artykułu. Brak jednak możliwości realizacji tej usługi wprowadza pewne ograniczenia, co do możliwego spektrum wykorzystania *watermarkingu*.

Skoro wiemy już, jakie usługi ochrony informacji i komunikacji jesteśmy w stanie zapewnić dzięki wykorzystaniu *watermarkingu* to przejdźmy do postawienia wymagań na parametry znaku wodnego przedstawione wcześniej. Za [5] znak wodny powinien charakteryzować się: wysoką żywotnością (aby zagwarantować integralność można wykorzystać tzw. *content-fragile watermarking*) i bezpieczeństwem. Dodatkowo, jak napisano wcześniej, powinien wykorzystywać on metody tzw. *blind watermarkingu* oraz prywatnej weryfikacji (jest ona bardziej zalecana w [5] dla realizacji usługi uwierzytelnienia niż publiczna).

5. Watermarking w telefonii IP – możliwe scenariusze

Z opisanych dotychczas faktów wynika, że istnieje potrzeba znalezienia nowych rozwiązań służących zabezpieczaniu sygnalizacji i głosu w telefonii IP. Obecne rozwiązania zabezpieczenia głosu (np. protokół SRTP dla VoIP) stosuje się raczej z powodzeniem, o ile pozwala na to przepływność sieci (chociaż posiadają pewne wady dla komunikacji w czasie rzeczywistym co opisano w [6]). Natomiast bezpieczeństwo wymiany wiadomości sygnalizacyjnych pozostawia wiele do życzenia.
W związku z tym zastanówmy się jak można wykorzystać *watermarking* do poprawy bezpieczeństwa telefonii IP. Możliwe są następujące scenariusze takiego zastosowania oznaczania cyfrowymi znakami wodnymi:

a. **Do zabezpieczenia pakietów „z głosem"** - dotychczas opracowano wiele metod oznaczania audio cyfrowymi znakami wodnymi, część z nich można by zastosować dla telefonii IP – jedna z metod dla usług czasu rzeczywistego została zaproponowana w [6],
b. **Do zabezpieczania wiadomości protokołu sygnalizacyjnego**, na którym bazuje telefonia IP,
c. **Do zabezpieczania** zarówno **głosu**, jak i **sygnalizacji**.

Dodatkowo możliwe jest wykorzystanie zabezpieczeń wynikających: jedynie z zastosowania metod *watermarkingu*, bądź połączenia działania części istniejących mechanizmów zabezpieczeń z metodami *watermarkingu*, o ile wprowadzone w ten sposób opóźnienia nie były by zbyt duże.
Po określeniu możliwych scenariuszy przejdźmy do ich charakterystyki.

5.1. Zabezpieczanie audio

Zaproponowane w punkcie **a** rozwiązanie nie jest niczym nowym. Powstało już kilka algorytmów do zabezpieczania komunikacji głosowej w czasie rzeczywistym (np. w [6], [13]). Usługa uwierzytelnienia zapewniana jest poprzez wbudowanie informacji charakteryzujących dzwoniącego (*Authentication Watermark*), natomiast integralność poprzez wpisanie informacji opisujących cechy przesyłanej treści (*Integrity Watermark*). Po wykonaniu algorytmu ekstrakcji i weryfikacji uzyskanych w ten sposób informacji z odebranymi danymi

następuje decyzja o kontynuacji/przerwaniu połączenia. Zaletą tego rodzaju rozwiązań jest zabezpieczanie całości konwersacji, a nie tylko pojedynczych pakietów z głosem. Przykładowe badania opóźnień wprowadzanych poprzez wbudowanie/ekstrakcję cyfrowego znaku wodnego przedstawiono w [6]. Według opublikowanych tam danych, dla kodera GSM 610, czas potrzebny do wykonania czynności związanych z *watermarkingiem* był 100 razy mniejszy od czasu obliczeniowego potrzebnego do kodowania/dekodowania ramki. Takie wyniki świadczą o słuszności poszukania rozwiązań wykorzystujących oznaczanie cyfrowym znakiem wodnym nie tylko do zabezpieczania głosu.

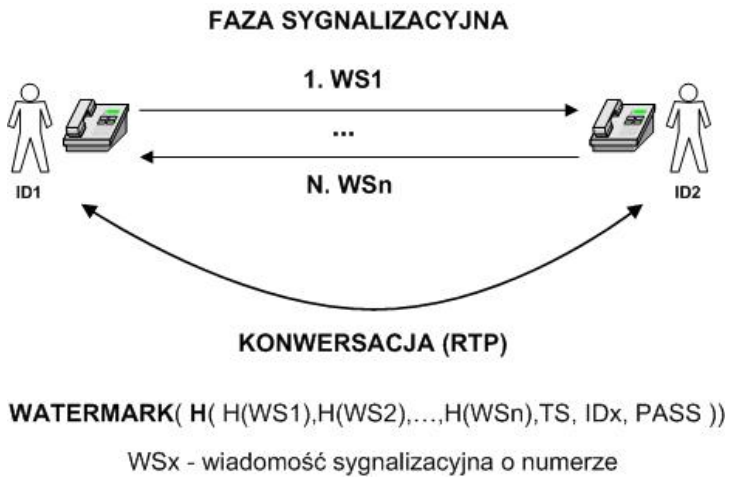
5.2. Zabezpieczanie sygnalizacji

Rozwiązanie **b** jest zupełnie nową propozycją. Aby przejść do charakterystyki tego rozwiązania należy najpierw powiedzieć, że w telefonii IP, na połączenie składają się dwie fazy: pierwsza sygnalizacyjna oraz druga, podczas, której następuje konwersacja.

Ogólna idea proponowanego tu rozwiązania polega na tym, aby w przesłany głos (faza druga) wpisać pewne informacje, które jednoznacznie scharakteryzowałyby przeprowadzoną wcześniej fazę sygnalizacyjną (faza pierwsza). W przypadku niezgodności uzyskanych z ekstrakcji znaku wodnego informacji z oryginalną wymianą wiadomości sygnalizacyjnych połączenie jest natychmiast przerywane i oznaczane jako niepoprawne.

Jest to swoiste działanie wstecz – atak nie jest wykrywany w momencie jego popełnienia, tylko dopiero po nawiązaniu połączenia. Dodatkowo można zadbać, aby przekazywanie informacji o sygnalizacji następowało dopiero po losowo ustalonym (ale niezbyt długim) czasie po rozpoczęciu rozmowy.

Przykładową realizację takiego procesu pokazano na rysunku nr 3:



Rys. 3. Przykładowa realizacja zabezpieczania sygnalizacji przy wykorzystaniu watermarkingu

Przedstawiony przykładowy proces może przebiegać następująco:

1) Osoba, która w sieci ma ID1 chce skomunikować się z drugą osobą o ID2. W tym celu następuje faza wymiany wiadomości sygnalizacyjnych pomiędzy węzłami. Zaznaczmy w tym miejscu, że połączenie dla telefonii IP oznacza jedynie pewien określony stan sygnalizacji, a nie fizyczną alokację kanału tak, jak jest to w telefonii klasycznej. Z każdej wymienianej wiadomości (czy to wysłanej, czy to otrzymanej) wyliczany jest skrót z wykorzystaniem funkcji H. W ten sposób powstają kolejne skróty H(WS1), H(WS2), … , H(WSn). Do ich przechowania potrzebny będzie zarówno stronie inicjującej, jak i docelowej bufor o określonej pojemności.
2) Po zakończeniu fazy sygnalizacyjnej następuje właściwa z punktu widzenia użytkowników końcowych faza połączenia: konwersacja. Przed jej rozpoczęciem obliczany jest skrót z wykorzystaniem ponownie funkcji H, której argumentami są: wcześniejsze skróty wiadomości sygnalizacyjnych (realizacja usługi integralności) oraz parametry służące uwierzytelnieniu np. współdzielone hasło, identyfikator. Możliwe jest również umieszczenie np. znaku czasowego dla zabezpieczenia przeciw atakom metodą powtórzenia (*ang. replay attack*).
3) Tak uzyskany skrót jest informacją wpisywaną następnie w trakcie trwania połączenia i który po detekcji w węźle docelowym jest weryfikowany. Sprawdzenie poprawności polega na porównaniu wyliczonych wcześniej skrótów otrzymanych/wysłanych wiadomości sygnalizacyjnych znajdujących się w buforze z tymi, które zostały przesłane za pomocą cyfrowego znaku wodnego.
   Dodatkowo, aby ograniczyć szansę ingerencji atakującego (np. poprzez usunięcie początku transmisji) rozpoczęcie wpisywania znaku wodnego można rozpocząć po losowo wybranym czasie p. W takim

wypadku należałoby określić sposób, w jakim ta informacja byłaby przekazywana do odbiornika, aby zapewnić poprawną weryfikację.

Przy implementacji tego typu rozwiązania ważne jest przede wszystkim sprecyzowanie, jakie parametry dla sygnalizacji mają być wbudowane w komunikację głosową, tak, aby w jak najlepszy i najbardziej jednoznaczny sposób zapewnić usługę uwierzytelnienia pełnego wymiany sygnalizacyjnej.

Do zalet takiego rozwiązania należy zaliczyć przede wszystkim fakt, iż obliczenia wykorzystujące funkcję skrótu, dla strony nadającej, są rozłożone w czasie, więc obciążenie i wymaganie na moc obliczeniową nie jest zbyt wygórowane. W takiej sytuacji nie jest konieczne również zabezpieczanie sygnalizacji w sposób klasyczny, czyli poprzez wykorzystanie mechanizmów zabezpieczeń dedykowanych dla danego systemu telefonii IP. Dodatkowo rozwiązanie takie jest bardziej elastyczne i daje niezależność od systemu telefonii IP zastosowanego w sieci – zabezpieczana jest cała wymiana sygnalizacji, nie tylko jedna konkretna wiadomość. Korzystając z wyników testów opóźnień wprowadzanych przez oznaczanie cyfrowym znakiem wodnym głosu w czasie rzeczywistym można wnioskować, że podobna operacja dotycząca bezpiecznej transmisji pewnych informacji dotyczących wymiany sygnalizacyjnej również nie powinna nastręczać większych trudności.
Podstawową wadą natomiast jest bezsprzecznie brak możliwości wykrycia ataku zaraz po jego nastąpieniu. Zaproponowane rozwiązanie daje tylko wtórną weryfikację wymiany wiadomości sygnalizacyjnych już w trakcie trwania rozmowy. Jednak, jeśli weźmiemy pod uwagę, że obecnie wiadomości sygnalizacyjnych nie zabezpiecza się w ogóle, to lepiej już pokusić się o rozwiązanie, które będzie działało *post factum***.**

Wykorzystanie *watermarkingu* do zabezpieczania wiadomości sygnalizacyjnych zapewnia usługę uwierzytelnienia oraz integralności. Jeśli skonfrontujemy to z istniejącymi mechanizmami zabezpieczeń np. dla usługi VoIP (SIP Digest dla protokołu SIP oraz Procedura I [HMAC-SHA1-96] dla protokołu H.323) to w tym świetle można uznać zaproponowane rozwiązanie za równoważne zdefiniowanym wcześniej. W tej sytuacji stanowi ono równorzędną alternatywę dla klasycznych rozwiązań. Niezbędne natomiast byłoby wykonanie miarodajnych testów porównawczych wprowadzanych opóźnień oraz potrzebnej mocy obliczeniowej, aby określić ich rzeczywistą przydatność.

5.3. Jednoczesne zabezpieczanie audio i sygnalizacji

Ostatnie rozwiązanie (**c**) proponuje jednoczesne zabezpieczanie sygnalizacji oraz głosu. Takie podejście jest najbardziej kompleksowe i daje zapewnienie uwierzytelnienia pełnego całej komunikacji (zarówno głosu, jak i wiadomości sygnalizacyjnych) wymienianej pomiędzy rozmawiającymi. Nie skupiamy się wyłącznie na zabezpieczaniu pojedynczych pakietów – chroniony jest tu cały kontekst wymieniany pomiędzy użytkownikami. Dodatkowo wyliczenie części parametrów do oznaczenia cyfrowym znakiem wodnym przebiega tylko raz – opóźnienie wprowadzane poprzez jednoczesne zabezpieczanie sygnalizacji i głosu jest mniejsze niż wykonywanie tychże operacji osobno. Parametry opisujące głos, jak i wymianę wiadomości sygnalizacyjnych wpisywane są razem, a następnie ich ekstrakcja i weryfikacja przebiega równolegle. Przebieg zabezpieczania sygnalizacji oraz głosu przebiega analogicznie jak na rysunku 3 – zmianie ulega tu jedynie ilość i zawartość wpisywanych informacji, która przedstawia się następująco:

WATERMARK(**H**(H(WS1),H(WS2),…,H(WSn),TS, IDx, PASS, PC1, ... ,PCn))

gdzie PCn oznacza parametr określający cechę treści, którą chcemy przekazać do weryfikacji

Z przedstawionego wyżej wzoru widać, że realizacja usługi uwierzytelnienia dla tego rozwiązania przebiega identycznie tzn. te same parametry mogą zostać wykorzystane, aby uwierzytelnić stronę generującą zarówno głos jak i wymianę wiadomości sygnalizacyjnych. Do fazy oznaczania cyfrowym znakiem wodnym, w porównaniu z poprzednim punktem, dochodzą parametry wskazujące na cechy charakterystyczne przenoszonej treści, czyli gwarancja integralności komunikacji głosowej.
Główną zaletą tego rozwiązania jest to, że wprowadzane opóźnienia i wymagania na moc obliczeniową są większe tylko nieznacznie od parametrów niezbędnych do oznaczania samego głosu. Dzieje się tak, gdyż tak naprawdę dodajemy jedynie więcej informacji do wpisania, natomiast sam proces pozostaje taki jak w przypadku oznaczania samego głosu lub sygnalizacji.
Poprzez wykorzystanie jednego rodzaju metody do zabezpieczania dwóch aspektów komunikacji dla systemów telefonii IP uzyskujemy zmniejszenie wartości opóźnienia oraz zapotrzebowania na moc obliczeniową w porównaniu do dotychczas stosowanych rozwiązań, gdzie do zabezpieczania głosu oraz sygnalizacji wyznaczono rozłączne mechanizmy zabezpieczeń.

Podsumowując – nieznacznie modyfikując dotychczasowe rozwiązania dotyczące oznaczania cyfrowo głosu w czasie rzeczywistym jesteśmy w stanie uzyskać całkiem nową metodę, o dużo szerszym spektrum działania, oferującą dużo więcej bezpieczeństwu systemów telefonii IP.

6. Bezpieczeństwo telefonii IP wykorzystującej watermarking

Skuteczność zastosowanych rozwiązań zabezpieczania głosu i sygnalizacji będzie na tyle dobra, na ile zapewnimy bezpieczeństwo cyfrowego znaku wodnego wbudowanego w przesyłany głos. Zakładamy, że wpisany przez nas znak wodny posiada właściwe wartości parametrów opisanych w [4], [5], [7] i [10] które są wymagane, aby uzyskać znak wodny odporny na ataki na samą technikę watermarkingu. Jeśli powyższy warunek jest spełniony to możemy stwierdzić, że zapewnione zostaną usługi uwierzytelnienia oraz integralności (uwierzytelnienia pełnego). Nadal jednak nie mamy zapewnionej usługi **poufności**, która jest jedną z podstawowych składowych bezpieczeństwa systemu telefonii IP. Jak już wspomniano wcześniej usługa ta nie może być realizowana z wykorzystaniem techniki watermarkingu. Wykorzystuje ona kanał odkryty przeznaczony pierwotnie do przenoszenia komunikacji głosowej, aby dodatkowo przetransportować pewne informacje dotyczące zarówno samej treści głosowej, jak i np. sygnalizacji. Wydaje się, więc, że stosując same metody cyfrowego oznaczania danych nie zapewnimy kompletnej architektury bezpieczeństwa telefonii IP. Co nie oznacza, że zaproponowane tu rozwiązania są bezwartościowe, gdyż mogą stanowić interesującą alternatywę lub uzupełnienie klasycznych mechanizmów zabezpieczeń.

7. Podsumowanie i zagadnienia do przyszłej analizy

W artykule zaproponowano możliwe sposoby potencjalnego wykorzystania metod watermarkingu do zabezpieczania głosu i wiadomości sygnalizacyjnych dla telefonii IP. Nowa metoda pozwoli, przy stosunkowo nieznacznym wzroście opóźnień i zapotrzebowania na moc obliczeniową, na zapewnienie usług: uwierzytelnienia i integralności. Może ona uzupełnić lub zastąpić dotychczasowe rozwiązania – mechanizmy zabezpieczeń. Dodatkowo rozwiązanie te jest bardzo elastyczne i niezależne od wykorzystywanego protokołu sygnalizacyjnego telefonii IP.

Zagadnień do przyszłego rozważenia pozostaje wiele. Pierwsze polegałoby na rozważeniu i określeniu najlepszych parametrów dla realizacji usług uwierzytelnienia i integralności, które powinny być wpisywane w transportowany głos – tak, aby uzyskać jak najpewniejsze zabezpieczenie przed potencjalnymi atakami.

Następnie niezbędne jest wykonanie miarodajnych testów na porównanie wprowadzanych opóźnień oraz potrzebnej mocy obliczeniowej, aby określić rzeczywistą przydatność rozwiązań np. zabezpieczania sygnalizacji z wykorzystaniem watermarkingu, w stosunku do mechanizmów zabezpieczeń usługi VoIP wspomnianych wcześniej: SIP Digest oraz Procedury I.

LITERATURA:

[1] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries - „Security Considerations for Voice Over IP Systems" - Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, kwiecień 2004
[2] W. Mazurczyk – „Bezpieczeństwo SIP jako protokołu sygnalizacyjnego VoIP" - XIX Krajowe Sympozjum Telekomunikacji KST 2003, Bydgoszcz, wrzesień 2003
[3] P. Tomsich, S. Katzenbeisser – „Towards a secure and de-centralized digital watermarking infrastructure for the protection of intellectual property", 2000
[4] M. Steinebach, J. Dittmann, F. Siebenhaar, C. Neubauer, U. Roedig, R. Ackermann – „Intrusion Detection Systems for IP Telephony Networks", Fraunhofer Institute IPSI
[5] J. Dittmann, A. Mukherjee, M. Steinebach – „Media-independent Watermarking Classification and the need for combining digital video and audio watermarking for media authentication", German National Research Center for Information Technology, Institute (IPSI)
[6] S. Yuan, S. Huss – „Audio Watermarking Algorithm for Real-time Speech Integrity and Authentication", Technical University of Darmstadt
[7] M. Arnold – „Attacks on Digital Audio Watermarks and Countermeasures", Department for Security Technology for Graphics and Communication Systems, Fraunhofer-Institute for Computer Graphics
[8] CERT, "Advisory CA-2004-01 Multiple H.323 Message Vulnerabilities", styczeń 2004
[9] CERT, „CA-2003-06 Multiple vulnerabilities in implementations of the SIP", luty 2003
[10] S. Voloshynovskiy, S. Pereira, T. Punn, J. Eggers, J. Su – "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks and Benchmarks", IEEE Communications Magazine, wrzesień 2001
[11] C. Lu, H. Liao, L. Chen – "Multipurpose Audio Watermarking" – Institute of Information Science, Academia Sinica, Taiwan, IEEE 2000
[12] S. Craver, M. Wu, B. Liu – "What can we reasonably expect from watermarks?" – Department of Electrical Engineering, Princeton University, IEEE Workshop on Applications of Signal Processing to Audio and Acoustics
[13] T. Mizrahi, E. Borenstein, G. Leifman, Y. Cassuto, M. Lustig, S. Mizrachi, N. Peleg – „Real-Time Implementation for Digital Watermarking in Audio Signals Using Perceptual Masking", 3rd European DSP Education and Research Conference, ESIEE, Noisy Le Grand, Paris, październik 2000

ARTYKUŁ RECENZOWANY