Bezpieczeństwo protokołów sygnalizacyjnych VoIP: koncepcja bezpiecznej współpracy protokołów SIP i H.323

Wojciech Mazurczyk
Instytut Telekomunikacji
Politechnika Warszawska
E-mail: *W.Mazurczyk@elka.pw.edu.pl*
http://security.tele.pw.edu.pl/

Streszczenie
W artykule dokonano omówienia oraz analizy stanu zabezpieczeń najpopularniejszych obecnie protokołów sygnalizacyjnych dla realizacji usługi VoIP (Voice over Internet Protocol): H.323 oraz SIP (Session Initiation Protocol). Przedstawiono koncepcję bezpiecznej współpracy protokołów SIP i H.323 z wykorzystaniem funkcji IWF SIP-H.323 oraz zaprezentowano szkic wymiany uwierzytelniającej dla mechanizmów SIP Digest oraz HMAC-SHA1-96 (Procedura IA).

1. Bezpieczeństwo VoIP.

Zagwarantowanie bezpiecznych połączeń dla usługi VoIP jest sprawą złożoną. Nie ogranicza się ono jedynie do zapewnienia zabezpieczonego transportu strumieni danych zawierających głos, ważniejszą sprawą jest zabezpieczenie przesyłania wiadomości protokołu sygnalizacyjnego, na którym bazuje VoIP.

Problemy bezpieczeństwa dla usługi telefonii IP w świetle powyższych stwierdzeń, uwzględniając rodzaje ruchu generowanego przez systemy VoIP, można podzielić na:

a. Bezpieczeństwo wiadomości sygnalizacyjnych wymienianych pomiędzy stronami komunikującymi się,
b. Bezpieczeństwo pakietów przenoszących głos (pakiety RTP),
c. Problemy związane z „przechodzeniem" pakietów przez Firewall'e oraz przez mechanizmy translacji adresów wewnętrznych (np. intranetowych) na zewnętrzne (np. internetowe) NAT (Network Address Translation).

Niniejszy artykuł skupia się wyłącznie na tematyce zawartej w punkcie **a**.

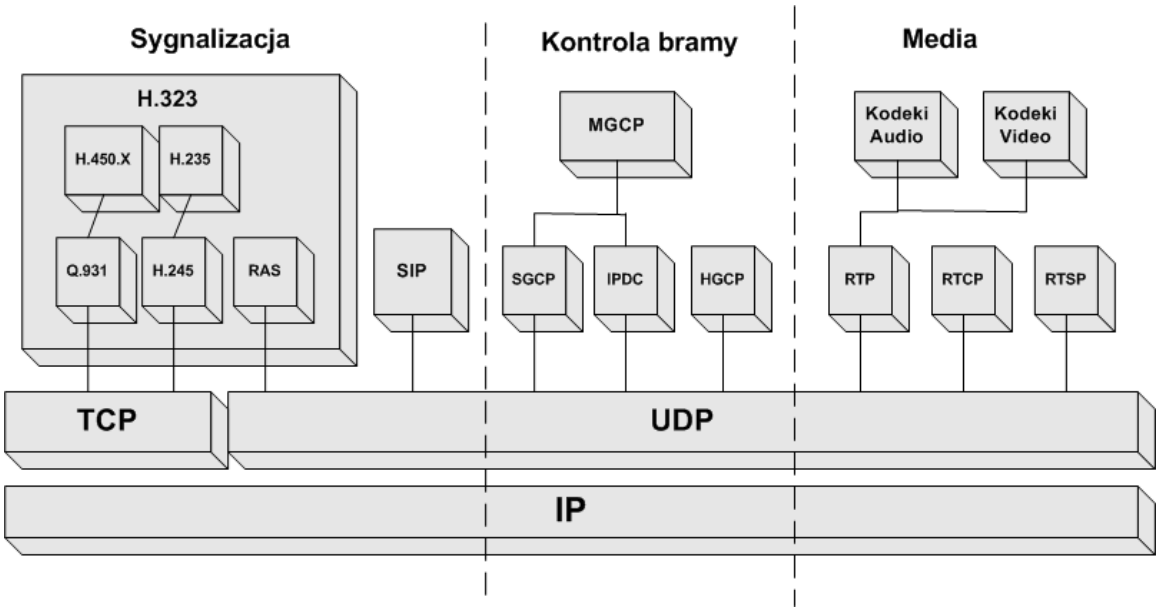
2. Protokoły sygnalizacyjne dla usługi VoIP

Obecnie nie ma jednego ogólnoświatowego standardu protokołu sygnalizacyjnego dla VoIP. Najbardziej znanymi protokołami, obecnie koegzystującymi, są: **H.323** (stworzony przez organizację ITU-T), **SIP** (Session Initiation Protocol – dzieło organizacji IETF), oraz **H.248/Megaco** (wspólny standard ITU-T oraz IETF). Współistnienie protokołów sygnalizacyjnych (szczególnie SIP i H.323) jest zjawiskiem, które w sposób niekorzystny wpływa na popularność i rozwój VoIP. Taka sytuacja jest wynikiem wspierania tego typu rozwiązań przez różne grupy na rynku telekomunikacyjnym: producentów i sprzedawców sprzętu, środowisk akademickich i naukowych, operatorów itp. Każda ze stron oferuje określone rozwiązanie, a przez to swoją wizję i próbuje je wypromować, jako najlepsze. Przykładem może być tu spór ludzi pochodzących z dwóch różnych środowisk telekomunikacyjnych: wywodzących się z tradycyjnych sieci PSTN (*Bellheads*) oraz wywodzących się z sieci IP (*Netheads*) nad ustaleniem modelu architektury sieci telefonii IP: rozproszonego czy zcentralizowanego. Taki brak zgodności owocuje niekompatybilnością i brakiem współpracy protokołów oraz produktów, które je wykorzystują.

W niniejszym artykule ograniczymy się jedynie do rozważań związanych z protokołami SIP i H.323. Na początku należy zaznaczyć, że nie są to protokoły wzajemnie równoważne. Rola protokołu SIP, w przybliżeniu, odpowiada dwóm protokołom Q.931 oraz H.225, które stanowią część protokołu H.323. To właśnie Q.931 oraz H.255 odpowiedzialne są za zestawianie połączeń oraz ich sygnalizację. W dalszej części artykułu często, dla uproszczenia, utożsamia się funkcje protokołów SIP oraz H.323, należy jednak pamiętać jednak o wyszczególnionej powyżej różnicy.

Porównując protokoły SIP oraz H.323, w zakresie ich wykorzystania w telefonii IP opartej wyłącznie o sieć IP (*All IP*), to lepiej sprawdza się protokół SIP. H.323 posiada duży nadmiar informacji sterujących, jest zbyt złożony i gorzej skalowalny. Dla równowagi H.323 ma dla przykładu bardzo dobrze zestandaryzowaną współpracę z sieciami PSTN i możliwości zarządzania. Obecnie trudno rokować, który z wymienionych protokołów sygnalizacyjnych zdobędzie dominującą pozycję. Jednym z prognozowanych scenariuszy jest również ich powolna ewolucja w jedno uniwersalne rozwiązanie.

Poniższy rysunek prezentuje stos wspomnianych powyżej protokołów dla realizacji usługi VoIP według modelu TCP/IP:

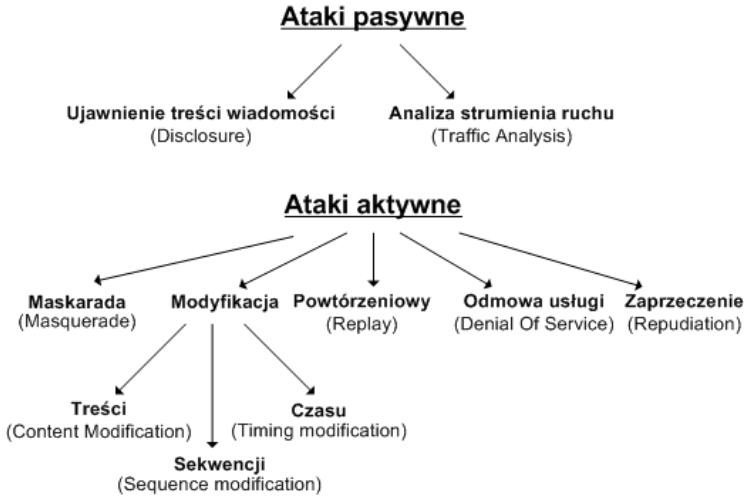


Rys. 1. Stos protokołów dla VoIP

3. Zagrożenia i mechanizmy zabezpieczeń protokołów sygnalizacyjnych VoIP

Zagrożenia powstałe na wskutek celowej akcji ze strony intruza może mieć charakter **pasywny** (istnieje jedynie możliwość podsłuchu lub stwierdzenia faktu przepływu wiadomości) lub **aktywny** (może dojść do ingerencji w przesyłanie wiadomości np. poprzez zmianę jej zawartości).

Podział na poszczególne **klasy ataków** na sieć oraz na komunikowanie się w niej z podziałem na pasywne i aktywne przedstawia poniższy rysunek. Klasyfikacja ta jest zmodyfikowaną wersją podziału wg. Stallingsa [17] uwzględniającą charakterystyczne cechy VoIP.



Rys. 2. Podział ataków na sieć oraz komunikację.

Ataki na usługę VoIP są realizowane z wykorzystaniem odpowiednich **technik**, czyli określonych działań oraz narzędzi użytych do przeprowadzenia ataku, wśród których wyróżnia się przede wszystkim: **podszywanie się** (*Spoofing*), **podsłuchiwanie** (*Sniffing*) oraz **odmowa usługi** (*Denial of Service*).

Zdefiniowany powyżej podział, jak i informacje tu zawarte wykorzystane zostaną przy definiowaniu kryterium oceny mechanizmów zabezpieczeń protokołów sygnalizacyjnych VoIP w punkcie 5.

Istnienie wymienionych powyżej rodzajów technik oraz klas ataków powoduje konieczność istnienia określonych rodzajów mechanizmów zabezpieczeń koniecznych, aby im przeciwdziałać. Dla telefonii IP, poziom zabezpieczeń gwarantowany protokołom sygnalizacyjnym może być realizowany z wykorzystaniem dwóch typów mechanizmów zabezpieczeń:

- **Wewnętrznych** wbudowanych w wykorzystywany protokół sygnalizacyjny,
- **Zewnętrznych** – pochodzących z innych aplikacji lub zapewnianych przez mechanizmy warstw niższych niż warstwa aplikacji modelu TCP/IP np. TLS, czy IPSec.

Dodatkowo możliwe jest jednoczesne wykorzystanie obu typów tych mechanizmów.

Niestety obecne implementacje VoIP spychają na drugi plan stosowanie rozwiązań bezpieczeństwa dla wiadomości sygnalizacyjnych. Główne powodami, dla których mechanizmy zabezpieczeń systemów VoIP **nie są** obecnie powszechnie stosowane i implementowane są następujące:

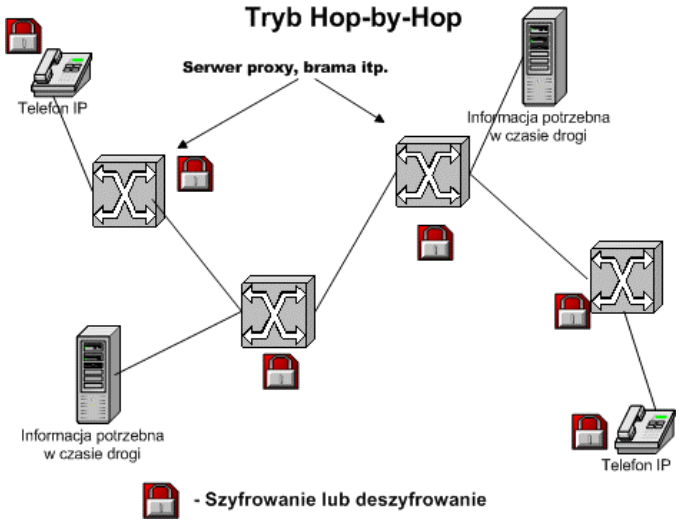
- Wprowadzają one dodatkowe opóźnienie (negatywny wpływ na parametry QoS),
- Zwiększa się obciążenie urządzeń sieciowych,
- Zwiększa się zapotrzebowanie na wymagane pasmo,
- Infrastruktura klucza publicznego nie jest dostępna globalnie,
- Istnieją problemy z przepływem pakietów przez Firewalle i urządzenia wykorzystujące technikę NAT.

W kolejnych częściach artykułu, przy omawianiu konkretnych mechanizmów zabezpieczeń dla protokołów sygnalizacyjnych będziemy jeszcze wracali do powyższych problemów związanych z VoIP.

4. Tryby pracy protokołów sygnalizacyjnych VoIP

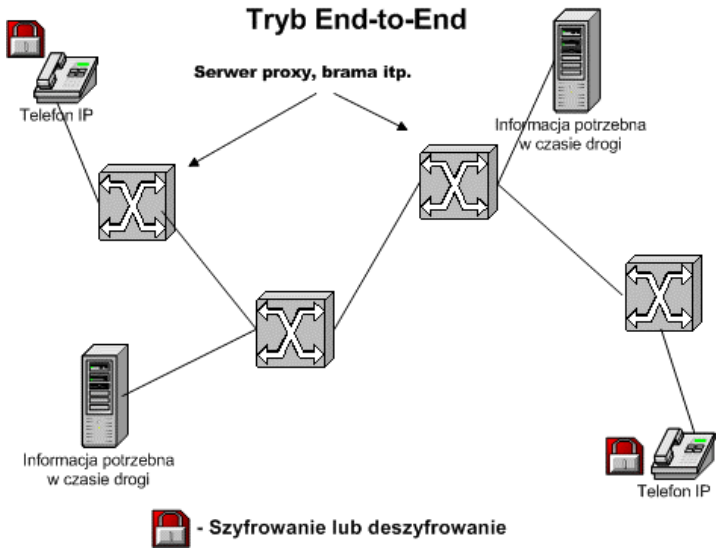
Słabości, luki czy ograniczenia bezpieczeństwa mogą pojawiać się z różnych powodów m.in. z błędnej lub niekompletnej implementacji określonych protokołów VoIP. Dodatkowo sama sieć pakietowa wykorzystująca stos TCP/IP np. Internet wprowadza pewne zagrożenia i ograniczenia (chodzi tu głównie problemy związane z wykorzystaniem Firewalli oraz techniki NAT). W związku z tym, aby zapewnić jak najwyższy poziom zabezpieczeń stworzono dwa odmienne tryby pracy mechanizmów zabezpieczeń: **Hop-by-Hop (HbH)** oraz **End-to-End (E2E)**.

Tryb *Hop-by-Hop* oznacza, iż przy każdym węźle sieci VoIP znajdującym się na drodze komunikacyjnej parametry bezpieczeństwa są weryfikowane oraz przeliczane od nowa tzn. usuwane są poprzednie, „stare" parametry, a na ich miejsce wprowadzane są wyliczone parametry charakterystyczne dla węzła sieci VoIP, w którym się obecnie znajdujemy. Pojęcie „hop" oznacza każdy węzeł sieci VoIP znajdujący się na drodze komunikacyjnej pomiędzy stronami. Realizację tego trybu dla usługi poufności dla przykładowej sieci VoIP przedstawia Rys. 3.



Rys. 3. Działanie trybu Hop-by-Hop dla realizacji usługi poufności

Odmiennie niż w *Hop-by-Hop*, tryb *End-to-End* charakteryzuje się tym, iż wykonanie algorytmów kryptograficznych odbywa się jednie w punktach: źródłowym i docelowym dla danego połączenia (z pominięciem elementów pośrednich). Dla zobrazowania różnic pomiędzy opisywanymi trybami poniżej znajduje się analogiczny jak dla *Hop-by-Hop* rysunek:



Rys. 4. Działanie trybu End-to-End dla realizacji usługi poufności

Oba typy mechanizmów zabezpieczeń posiadają zarówno swoje wady i zalety. Cechy charakterystyczne, w świetle najważniejszych z punktu widzenia bezpieczeństwa, obu trybów oraz ich zestawienie i porównanie zostały zaprezentowane w tabeli numer 1.

Kryterium porównania	Tryb Hop-by-Hop	Tryb End-to-End
Transport	Dostęp do całości wiadomości sygnalizacyjnej w każdym węźle sieci VoIP na drodze komunikacyjnej.	Wiadomość sygnalizacyjna oprócz określonych nagłówków jest niedostępna dla pośrednich węzłów sieci VoIP.
Węzły sieci VoIP	Są bardziej skomplikowane w całej sieci z uwagi na konieczność wykonywania określonych czynności kryptograficznych w każdym węźle na drodze sygnalizacyjnej (większy koszt).	Komplikacja i wymagania wydajnościowe jedynie dla punktów końcowych (mniejszy koszt).
Bezpieczeństwo sygnalizacji	Zapewniane jest zabezpieczenie, co najmniej pierwszego odcinka z całej drogi sygnalizacyjnej (czyli pomiędzy stroną inicjującą, a pierwszym węzłem pośredniczącym) i całej wiadomości	Potencjalnie zabezpieczenie sygnalizacji od punktu inicjującego do docelowego, lecz nie wszystkie pola
Dostępność nagłówków (rutowanie)	Urządzenia pośredniczące mają łatwy dostęp do nagłówków. Nie ma problemów z rutowaniem.	Niemożność zabezpieczenia całej wiadomości w trybie *E2E*, gdyż część informacji niezbędna jest do rutowania
Wpływ na QoS	Negatywny – większy niż w trybie E2E, co w konsekwencji daje większe opóźnienia	Negatywny, ale wprowadza mniejsze opóźnienia niż w trybie HbH
Zaufanie	Wszystkie węzły na drodze sygnalizacyjnej muszą być elementami zaufanymi.	Ograniczone zaufanie do węzłów pośrednich.
Wymagania na pasmo	Większe niż w E2E	Mniejsze niż HbH

Tabela 1 Porównanie własności trybów *Hop-by-Hop* i *End-to-End.*

Z przytoczonych powyżej cech mechanizmów *End-to-End* i *Hop-by-Hop* można wywnioskować, iż trudno jest jednoznacznie określić, którego typu mechanizmy powinny być wykorzystywane. Zarówno jedne jak i drugie posiadają wiele zalet, a jednocześnie poważnych słabości. Oczywiście, jeśli udało by się jakoś w satysfakcjonujący sposób rozwiązać problem QoS w sieciach IP oraz możliwe byłoby zapewnienie odpowiedniej mocy obliczeniowej zarówno w urządzeniach końcowych jak i pośredniczących (co wpływa w znaczący sposób jednocześnie na ich cenę), wtedy w idealnej sytuacji można by korzystać zarówno z jednego, jak i drugiego typu mechanizmów jednocześnie, co pozwoliło by na choć częściowe, wzajemne skompensowanie się ich słabości.

Jednak do takiej sytuacji jest obecnie daleko, dlatego też pozostaje stosowanie rozwiązań, na które pozwalają rozwiązania i parametry techniczne wykorzystywanej sieci i urządzeń w niej się znajdujących. Należy jednak wykluczyć sytuację, w której nie stosowane będą żadne mechanizmy zabezpieczeń.

W dalszej części pracy zostaną scharakteryzowane dostępne mechanizmy zabezpieczeń w zależności od wykorzystanego protokołu sygnalizacyjnego dla usługi VoIP z uwzględnieniem właśnie podziału na tryby HbH oraz E2E.

5. Kryterium oceny mechanizmów zabezpieczeń protokołów sygnalizacyjnych VoIP

Aby usystematyzować przegląd mechanizmów zabezpieczeń a następnie je oceniać należy ustalić kryterium, według którego nastąpi ich analiza. Przy wyborze należy kierować się zarówno specyfiką usługi VoIP, wybranych protokołów sygnalizacyjnych (SIP, H.323) i charakterem potencjalnych zagrożeń, technik oraz ataków (ostatnie zagadnienia zostały scharakteryzowane w punkcie 3).

W artykule zdecydowano się na wybór rozwiązania będącego modyfikacją podziału zawartego w normie ISO 7498-2, według którego bezpieczeństwo w systemach otwartych należy rozpatrywać w kontekście możliwości zapewnienia pięciu podstawowych usług ochrony informacji: kontroli dostępu (*Access Control*), uwierzytelnienia (*Authentication*), integralności danych (*Data Integrity*), poufności danych (*Confidentiality*) oraz niezaprzeczalności (*Non-repudation*).

Po uwzględnieniu zarówno specyfiki protokołów sygnalizacyjnych SIP i H.323 jak i charakteru potencjalnych na niego ataków, przyjęto kryterium, zdefiniowane jako umiejętność zapewnienia dwóch głównych usług ochrony informacji oraz komunikacji w sieci tzn.:

- **Poufności** – dającej ochronę przed atakami pasywnymi oraz zabezpieczającej wiadomości sygnalizacyjne, wymieniane pomiędzy komunikującymi się jednostkami, przed ich nieuprawnionym uzyskaniem przez strony do tego nieupoważnione;
- **Uwierzytelnienia** – gwarantującego ochronę przed atakami aktywnymi oraz kontrolę tożsamości stron i wiadomości sygnalizacyjnych wymienianych pomiędzy nimi. Dodatkowo na potrzeby późniejszej analizy mechanizmów zabezpieczeń (głównie protokołu H.323) podział tej usługi na: **uwierzytelnienie pełne** (uwierzytelnienie + integralność) oraz **niepełne** (tylko usługa uwierzytelnienia).

Spełnienie powyższego kryterium jest wystarczające do uznania protokołu sygnalizacyjnego, na którym bazuje VoIP, za bezpieczny. Ponieważ jak wykazano w punkcie 1, bezpieczne przesyłanie wiadomości sygnalizacyjnych, w znaczny sposób, rzutuje na bezpieczeństwo całej usługi VoIP, dlatego też prawdziwym jest stwierdzenie, iż dzięki temu cały system VoIP jest bezpieczniejszy.

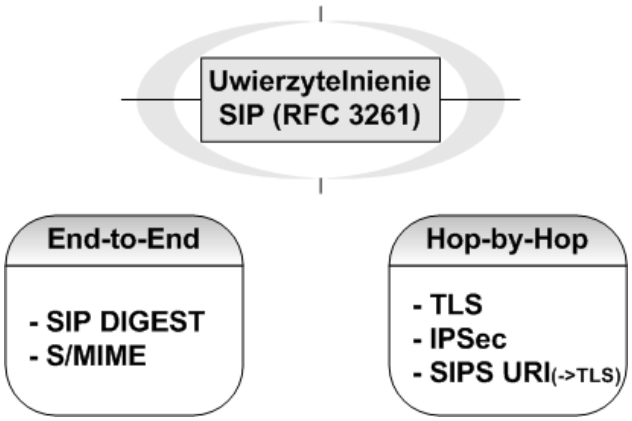
Kolejne punkty charakteryzują bezpieczeństwo dwóch wybranych protokołów sygnalizacyjnych dla realizacji usługi VoIP: SIP oraz H.323.

6. Bezpieczeństwo SIP

Wyczerpująca analiza wszystkich dostępnych mechanizmów zabezpieczeń dla protokołu SIP zarówno dla zalecenia RFC 2543 (marzec 1999) oraz nowego RFC 3261 (lipiec 2002) znajduje się w [8]. Tutaj zaprezentujemy rozwiązania zawarte jedynie w obowiązującym obecnie standardzie (RFC 3261).

6.1 Usługa uwierzytelnienia w SIP

Mechanizmy zastosowane dla realizacji usługi uwierzytelnienia dla SIP w wersji drugiej zostały zamieszczone na rysunku poniżej:



Rys. 5. Realizacja usługi uwierzytelnienia w SIP wg RFC 3261

Do realizacji **uwierzytelnienia S/MIME** wykorzystuje tunelowanie oraz podpisy cyfrowe. Przebiega to następująco: wykonuje się pełną lub częściową kopię nagłówków wiadomości SIP i umieszcza wraz z oryginalnym ciałem w jednostce MIME, która reprezentuje ciało nowej wiadomości. Następnie jest ona podpisywana cyfrowo z wykorzystaniem funkcji skrótu SHA-1. Dodatkowo wykorzystuje się algorytm klucza publicznego RSA do wymiany kluczy, a w konsekwencji do bezpiecznego przesłania obliczonego skrótu do właściwego odbiorcy. Po osiągnięciu celu

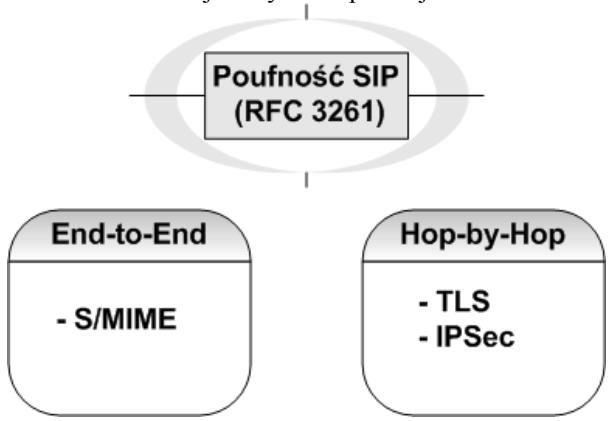
adresat wiadomości weryfikuje dostarczony podpis cyfrowy. Jeśli jest on prawidłowy to dodatkowo dokonuje się porównania tych nagłówków, które nie były wykorzystywane przez urządzenia znajdujące się na drodze komunikacyjnej, ponieważ one mogły być modyfikowane (zapewnienie podstawowej integralności wiadomości).

Jeśli natomiast, jako mechanizm gwarantujący uwierzytelnienie został wybrany **SIPS URI** to cała droga komunikacyjna powinna być zabezpieczona z wykorzystaniem protokołu TLS (czyli musi on zostać zaimplementowany w całej sieci, gdyż jest to warunek konieczny do prawidłowego funkcjonowania SIPS URI). Jeśli taki warunek nie może zostać spełniony - nie dochodzi do nawiązania połączenia.

Mechanizm SIP Digest został opisany w punkcie 8.3.

6.2 Usługa poufności w SIP

Jeśli natomiast chodzi o realizację drugiej usługi zdefiniowanej w wybranym przez nas kryterium to stosuje się tu przede wszystkim mechanizm szyfrowania. Prezentuje to rysunek poniżej:



Rys. 6. Realizacja usługi poufności w SIP wg RFC 3261

Realizacja usługi **poufności** z wykorzystaniem mechanizmu **S/MIME** przebiega podobnie jak w przypadku realizacji usługi uwierzytelnienia (również wykorzystywana jest enkapsulacja części wiadomości w jednostce MIME) z tą różnicą, że zamiast funkcji skrótu stosuje się tu szyfrowanie 3DES.

6.3 Słabe punkty w architekturze bezpieczeństwa SIP w zaleceniu RFC 3261

Protokół SIP zdefiniowany w zaleceniu RFC 3261 definiuje architekturę bezpieczeństwa, która jest poprawna i minimalizuje prawdopodobieństwo przeprowadzenia udanego ataku na system oparty na tym protokole sygnalizacyjnym. Mimo tego, posiada ona klika słabości. Zostały one zebrane w tabeli i są one następujące:

Mechanizm zabezpieczeń	Słabości i uwagi
SIP Digest	- wykorzystanie schematu współdzielonego sekretu (*Shared Secret*)
	- brak gwarancji całkowitej integralności wiadomości
S/MIME	- zdefiniowany w SIP system wymiany kluczy jest nieodporny na atak typu *Man-in-the-Middle*
	- wykorzystanie tego mechanizmu może owocować dużymi (w sensie objętości) wiadomościami sygnalizacyjnymi
	- problem rzadkich serwerów sieciowych (którego prawidłowe działanie zależy od możliwości dostępu i modyfikowaniu ciała wiadomości SIP) na drodze komunikacyjnej – mechanizm ten skutecznie uniemożliwi prawidłowe funkcjonowanie takiego elementu sieciowego

Tabela 2 Zestawienie słabości protokołu sygnalizacyjnego SIP

Dla protokołu SIP (a dalej się okaże, że i dla H.323) typem ataku, przed którym nie ma całkowitej ochrony jest atak typu **Odmowa Usługi** (*Denial of Service*). Bez względu na rodzaj zaimplementowanych mechanizmów zabezpieczeń zawsze możliwe jest „zalanie" serwera (głównie chodzi tu w przypadku SIP o serwery *proxy*) poprzez wysyłanie nadmiernej ilości zwykle niepoprawnych wiadomości, w ten sposób powodując odmowę świadczenia usług dla poprawnych wiadomości wysłanych przez użytkownika, dla których dana jednostka została stworzona.

Niestety tego typu ataku nie da się wyeliminować całkowicie, ponieważ wiązałoby się to z ograniczeniem podstawowych funkcji serwerów sieciowych. Jednym z rozwiązań, które może w sposób satysfakcjonujący ograniczyć prawdopodobieństwo wystąpienia takiego ataku jest przeprowadzanie wzajemnego uwierzytelnienie serwerów *proxy* z wykorzystaniem protokołu TLS.

7. Bezpieczeństwo H.323

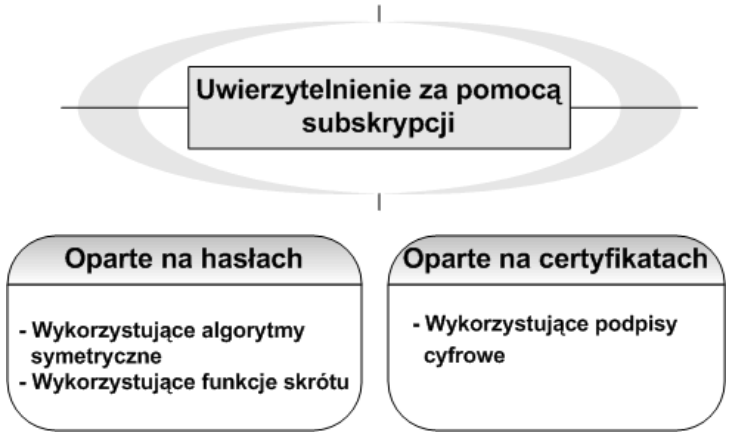
Mechanizmy i sposób zabezpieczeń systemu VoIP bazującego na tym protokole reguluje osobne zalecenie organizacji ITU – H.235. Dostarcza ono rozwiązania kryptograficzne niezbędne do zabezpieczenia zarówno kanałów sygnalizacyjnych (RAS, H.225.0 i H.245) jak i tych, w których przesyłany jest głos.

Analiza mechanizmów zabezpieczeń dla systemów H.323 zostanie zaprezentowana w podobny sposób jak to odbyło się w przypadku protokołu SIP, czyli poprzez przedstawienie realizacji usług ochrony informacji i komunikacji w sieci IP, czyli uwierzytelnienia oraz poufności.

7.1 Usługa uwierzytelnienia w H.323

Zalecenie H.235 definiuje dwa możliwe rodzaje mechanizmów uwierzytelnienia opartych na subskrypcji. Jeden bazuje na metodzie współdzielonego sekretu, natomiast drugi wykorzystuje infrastrukturę PKI.

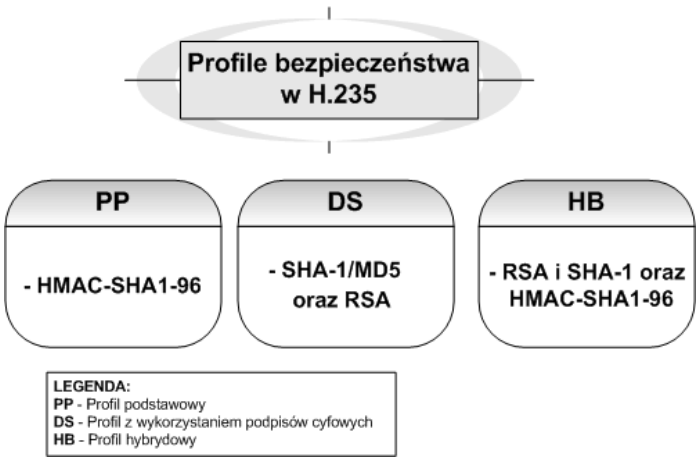
Mechanizmy subskrypcji wykorzystywane w H.235 można zaklasyfikować tak, jak na rysunku poniżej:



Rys. 7. Podział mechanizmów uwierzytelnienia w H.235

Profile bezpieczeństwa w H.323

Dodatkowo w zaleceniu H.235 [3] zdefiniowano trzy profile bezpieczeństwa: podstawowy (*Baseline security profile*) bazujący na hasłach, wykorzystujący podpisy cyfrowe (*Signature profile*) oraz hybrydowy (*Hybryd profile*). Wszystkie trzy wskazują, już bezpośrednio, istniejące rozwiązania kryptograficzne, z których należy korzystać przy opracowywaniu architektury bezpieczeństwa H.323. Podział na profile wraz z mechanizmami zabezpieczeń, które wykorzystują przedstawiono na rysunku 8:



Rys. 8 Profile bezpieczeństwa w H.235

Podstawowe cechy charakteryzujące wskazane na rysunku 7 profile opisano w tabeli 3:

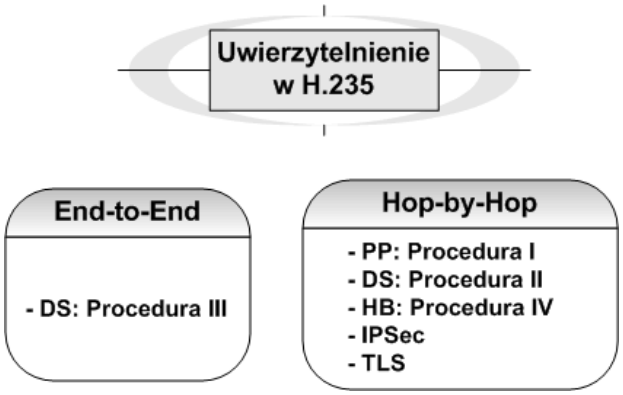
Cecha:	Profil podstawowy	Profil wykorzystujący podpisy cyfrowe	Profil hybrydowy
Rodzaj modelu systemu H.323	Ze Strażnikiem (*Gatekeeper*)	Ze Strażnikiem (*Gatekeeper*)	Ze Strażnikiem (*Gatekeeper*)
Implementacja	Konieczna	Konieczna	Konieczna

procedury Fast Connect			
Wykorzystywane rozwiązania kryptograficzne	Współdzielony sekret i szyfrowanie symetryczne	Podpisy cyfrowe	Szyfrowanie symetryczne i podpisy cyfrowe
Zdefiniowane procedury	I, IA	II, III	IV
Gwarantowane usługi ochrony	Uwierzytelnienie pełne (Proc. I), niepełne (Proc. IA)	Uwierzytelnienie pełne, niezaprzeczalność	Uwierzytelnienie pełne, niezaprzeczalność – tylko dla pierwszej wiadomości
Tryb wykorzystywanych mechanizmów	Hop-by-Hop	Hop-by-Hop (Proc. II) lub End-to-End (Proc. III)	Hop-by-Hop
Status w implementacji	Opcjonalny	Opcjonalny	Opcjonalny
Skalowalność dla globalnych rozwiązań VoIP	Słaba	Dobra	Dobra
Dodatkowe wymagania dla protokołu H.323	-	-	Tunelowanie H.245
Główne zalety	Łatwość implementacji	Nie wymaga wcześniejszego kontaktu stron; dodatkowo usługa niezaprzeczalności	Łączy zalety dwóch pierwszych profili
Główne wady	Administracja współdzielonymi kluczami, wymaga wcześniejszego kontaktu	Większe zapotrzebowanie na pasmo oraz moc obliczeniową; trudniejszy w implementacji niż profil podstawowy	Wykorzystanie technik poprzednich profili - częściowe skompensowanie ich wad

Tabela 3 Cechy profili bezpieczeństwa w H.235

Podsumowanie mechanizmów uwierzytelnienia

Podsumowanie mechanizmów opisanych w H.235v4 [3], które mają na celu gwarantowanie usługi uwierzytelnienia dla systemów H.323 przedstawia poniższy rysunek:

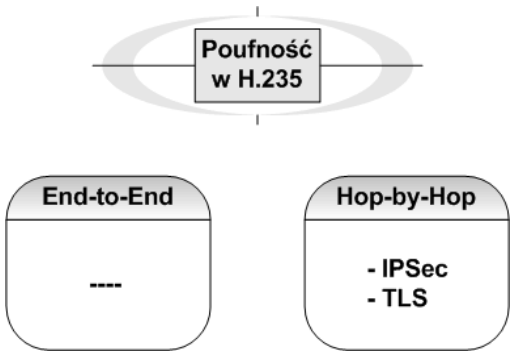


Rys.9. Realizacja usługi uwierzytelnienia w H.323

Dodatkowo należy wspomnieć, iż realizacja uwierzytelnienia w trybie *Hop-by-hop* możliwa jest w H.323 również poprzez wykorzystanie protokołów warstw niższych niż aplikacji modelu odniesienia TCP/IP, czyli: TLS oraz IPSec. Implementacja obu protokołów nie jest jednak obowiązkowa.

7.2 Usługa poufności w H.323

Ponieważ żaden z opisanych profili bezpieczeństwa nie gwarantuje usługi poufności **dla sygnalizacji** systemów H.323, dlatego też jedyną możliwością jej zapewnienia jest zastosowanie wspomnianych niższych poprzednim punkcie rozwiązań warstw niższych, co przedstawia poniższy rysunek:



Rys.10. Realizacja usług poufności w H.323

Z rysunku widać, że szyfrowanie, które umożliwia realizację usługi poufności zapewniane jest jedynie przez protokoły TLS oraz IPSec.

7.3. Słabe punkty w architekturze bezpieczeństwa H.323

Trwające ciągle prace organizacji ITU-T nad rozwojem bezpieczeństwa dla systemów bazujących na protokole H.323 umożliwiają zapewnienie poprawnej architektury bezpieczeństwa. Obecna wersja protokołu H.235v4 (sierpień 2003 [3]) dostarcza trzy opisane wyżej profile, które można wykorzystywać w zależności od warunków i wymagań stawianych sieci VoIP.

Oczywiście zarzuty, co do stosowania mechanizmów współdzielonego sekretu pozostają te same, co w przypadku mechanizmów zawartych w SIP – nie są to rozwiązania bezpieczne, w porównaniu z algorytmami klucza publicznego. Natomiast, aby umożliwić, wymieniane w tej pracy jako jedne z kluczowych rozwiązań dla bezpieczeństwa systemu VoIP, wzajemne uwierzytelnienie konieczne jest wykorzystanie algorytmów klucza publicznego. Dodatkowo są praktycznie jedynym środkiem umożliwiającym zapewnienie usługi uwierzytelnienia dla sieci rozległych (poprzez bezpieczną dystrybucję kluczy w niezabezpieczonej sieci). Dodatkowo mogą gwarantować również usługę niezaprzeczalności. Z drugiej jednak strony algorytmy klucza publicznego posiadają wady, w kontekście wykorzystania ich jako mechanizmów zabezpieczeń dla systemów VoIP np. słaby popyt na tego typu usługi oraz łatwość uzyskania fałszywego certyfikatu.

Podsumowując źródła problemów i luk w bezpieczeństwie rozwiązań VoIP bazujących na protokole sygnalizacyjnym H.323 pozostają podobne jak w przypadku SIP. Pomimo zdefiniowania wielu możliwych rozwiązań bezpieczeństwa nie są one implementowane ze względu na zbyt duże wprowadzane opóźnienia bądź, dlatego, że ich stosowanie jest opcjonalne (lub wykorzystywane przez nie procedury np. Fast Connect pozostają opcjonalne).

Innym źródłem luk bezpieczeństwa, jak już wspomniano wcześniej, są błędy w implementacji samego protokołu sygnalizacyjnego. Zarówno dla protokołu H.323 [13], jak i wcześniej SIP [14] organizacja CERT opublikowała wiele nieprawidłowości w komercyjnych produktach opartych na tych protokołach sygnalizacyjnych, co w konsekwencji prowadzi do istnienia dodatkowych zagrożeń dla rozwiązań telefonii IP.

8. Współpraca systemów VoIP opartych na różnych protokołach sygnalizacyjnych

Jak opisano w punkcie 2, w najbliższej przyszłości prognozuje się jako najbardziej prawdopodobne współistnienie sieci VoIP opartych na różnych protokołach sygnalizacyjnych. W związku z tym, rosnącym problemem staje się brak możliwości współpracy systemów VoIP bazujących na różnych protokołach sygnalizacyjnych. Natomiast jednym z najważniejszych do rozwiązania aspektów współpracy systemów VoIP jest współdziałanie protokołów sygnalizacyjnych H.323 oraz SIP. Wynika to przede wszystkim z podobieństwa funkcji, jakie pełnią w systemie VoIP oraz miejsca w sieci. Dodatkowo należy uwzględnić fakt mniej więcej jednakowej popularności obu protokołów oraz liczne prognozy raczej ich koegzystowania, niż wyparcia jednego przez drugi. Oba będą służyły zestawianiu multimedialnych konferencji i telefonicznych rozmów w sieciach IP. Dlatego dla popularyzacji i uniwersalności rozwiązań VoIP bardzo ważne jest zapewnienie współdziałania rozwiązań bazujących na różnych protokołach sygnalizacyjnych.

Niestety obecnie spotykamy się nie tylko z brakiem kompatybilności pomiędzy protokołami sygnalizacyjnymi, ale również z brakiem współdziałania pomiędzy produktami w ramach jednego protokołu sygnalizacyjnego, co opisane zostało dokładniej w [16]. Również nie widać pośpiechu w pracach producentów sprzętu do umożliwienia łatwej współpracy z rozwiązaniami innych producentów. Dzieje się tak oczywiście głównie z powodów finansowych. Dlatego, aby dbać o właściwy kierunek rozwoju, tak ważną sprawą jest standaryzacja protokołów sygnalizacyjnych VoIP. Obecnie trwają intensywne prace nad współpracą pomiędzy SIP i H.323. Najprężniej działa w tym kierunku organizacja IETF oraz dodatkowo inne ciała: ETSI TIPHON oraz ITU-T.

Zapewnienie współpracy w podstawowych aspektach pomiędzy wymienionymi protokołami jest możliwe tym bardziej, że oba wykorzystują część tych samych protokołów m.in. IP czy RTP (**Cecha I**). Dodatkowo, ponieważ nie istnieje potrzeba konwersji danych zawierających głos (**Cecha II**), rozwiązaniem problemu współpracy jest

wprowadzenie elementu, który dokonywałby translacji jedynie (aż!) wiadomości sygnalizacyjnych H.323 na SIP i odwrotnie. Proponowane jest wprowadzenie funkcji, którą za [1], [11], [15] będziemy nazywać **IWF SIP-H.323** (SIP-H.323 InterWorking Function).

Głównym zadaniem IWF SIP-H.323 jest zapewnienie translacji wiadomości sygnalizacyjnych dla wszystkich faz połączenia. Jeśli z jednej strony sieci zostanie przysłana wiadomość sygnalizacyjna – zadaniem IWF jest wysłanie na drugą stronę sieci wiadomości ekwiwalentnej wiadomości otrzymanej.

W ciągu prac badawczych udało się opracować wsparcie dla wielu podstawowych aspektów współpracy protokołów SIP i H.323 m.in. mapowania poszczególnych wiadomości sygnalizacyjnych, zestawiania połączenia, rejestracji użytkowników, translacji adresów itp. Jednak cały czas kwestią do końca nierozwiązaną oraz pozostawianą na uboczu jest kwestia zapewnienia bezpieczeństwa wiadomości sygnalizacyjnych wymienianych pomiędzy sieciami wykorzystującymi różne protokoły sygnalizacyjne. Dzieje się tak zapewne, dlatego, iż zastosowanie jakichkolwiek mechanizmów zabezpieczeń wpływa negatywnie na jakość przesyłanego głosu w telefonii IP (parametry QoS - Quality of Service), a problem zapewnienia parametrów QoS dotychczas sieciach IP, takich jak np. Internet, mimo licznych prób, nie posiada dotychczas sprawdzonego rozwiązania.

Jednak pozostawienie usługi VoIP bez zupełnie żadnych zabezpieczeń spowoduje brak zainteresowania wykorzystaniem komercyjnym takich systemów. Będą one potencjalnie narażone na liczne ataki, co w konsekwencji może prowadzić do zmniejszenia lub nawet zaniku zainteresowania VoIP oraz spowolnienie lub zatrzymanie prac badawczych nad telefonią IP na dużą skalę. Mimo takiej groźby nadal nie opracowano potrzebnych założeń współpracy dla mechanizmów zabezpieczeń, choć prace nad tematem współpracy trwają od roku 2000. Przyjmuje się jednak jako priorytetowe umożliwienie współpracy obu protokołów dla prostych scenariuszy i jak najprostszymi środkami, a kolejnymi istotnymi aspektami zajmuje się dopiero na końcu. Przypomina to nieco sytuację, w której zawodowemu bokserowi każe się ćwiczyć jedynie zadawanie ciosów tak, aby zwiększyć maksymalnie ich siłę, zapominając przy tam jak ważną dla tego sportu jest praca nóg.

Przestawione poniżej rozważania mają na celu uzupełnić te luki i stanowią bazę wyjściową dla zapewnienia współpracy mechanizmów zabezpieczeń protokołów sygnalizacyjnych SIP i H.323.

8.1. Wymagania dla sieci łączonych z IWF SIP-H.323 z punktu widzenia bezpieczeństwa

Opis współpracy protokołów SIP i H.323 został szerzej omówiony w [11] oraz [15]. Właśnie na tej bazie będziemy się starali stworzyć bezpieczny z punktu widzenia protokołów sygnalizacyjnych łączony system SIP i H.323. Na potrzeby dalszych rozważań należy, z tych dokumentów, przytoczyć następujące cechy IWF:

Założenie A: IWF nie powinno wykorzystywać elementów opcjonalnych architektury funkcjonalnej obu sieci,
Założenie B: IWF może zostać zintegrowane ze Strażnikiem H.323 (*Gatekeeper*) lub serwerem SIP (np. *proxy* lub *redirect*),
Założenie C: IWF nie musi dokonywać konwersji strumieni mediów (wynika to bezpośrednio z Cech: I oraz II),
Założenie D: IWF powinien wspierać procedurę protokołu H.323 Fast Connect oraz tunelowanie H.245,
Założenie E: IWF powinno wspierać oba protokoły warstwy transportowej modelu TCP/IP, czyli TCP oraz UDP
Założenie F: Terminale obu sieci powinny być nieświadome istnienia i pośrednictwa IWF,
Założenie G: IWF powinien obsługiwać SIP w wersji RFC3261 oraz H.323 w wersji 2 lub późniejszej,
Założenie H: Translacja sygnalizacji nie może wprowadzać zmian ani do protokołu SIP, ani do H.323.

Jeśli chodzi o założenia bezpośrednio dotyczące mechanizmów zabezpieczeń to dokument [11] zakłada jako najważniejsze, że:

Założenie S1: IWF powinien wykorzystywać przypisane protokołom sygnalizacyjnym mechanizmy zabezpieczeń (np. S/MIME dla SIP, czy rozwiązania protokołu H.235 dla H.323).
Założenie S2: IWF musi posiadać procedury uniknięcia ataków typu Denial of Sernice (DoS).
Założenie S3: IWF musi być elementem zaufanym dla obu stron sieci.

Poniżej przedstawiono autorskie wymagania dla IWF SIP-H.323 z punktu widzenia bezpieczeństwa dla obu stron sieci. Wynikają one przede wszystkim z ustosunkowania się do wymienionych powyżej założeń i często pozostają z nimi w sprzeczności. Niestety czasami ceną za bezpieczeństwo sygnalizacji jest utrata innych cech obu protokołów np. elastyczności.

Według kryterium podanego w punkcie 5 protokół sygnalizacyjny, na którym bazuje VoIP możemy uznać za bezpieczny, jeśli zapewnienia on dwie podstawowe usługi ochrony informacji i komunikacji w sieci: uwierzytelnienie oraz poufność. Połączenie dwóch sieci bazujących na różnych protokołach sygnalizacyjnych tworzy nowy system VoIP, który chcemy, aby również spełniał to kryterium. Dlatego, aby osiągnąć nasz cel, jednostka logiczna IWF powinna spełniać następujące wymagania:

Wymaganie 1: Ponieważ wszystkie profile bezpieczeństwa dla protokołu H.323 zakładają wykorzystanie modelu sieci ze Strażnikiem (*Gatekeeper*) (patrz Tabela 3), dlatego też dla bezpiecznego łączonego systemu VoIP z jednostką IWF **konieczne** jest również wykorzystywanie tego modelu (niezgodne z Założeniem A).
Wymaganie 2: Z podobnych, co w Wymaganiu 1 powodów **niezbędne** jest wspieranie przez IWF procedur charakterystycznych dla protokołu H.323 – Fast Connect oraz tunelowania H.245 (niezgodne z Założeniem D).

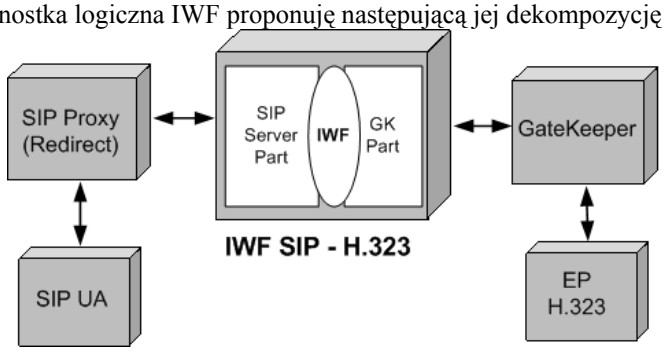
Wymaganie 3: Ponieważ wykorzystywany będzie model systemu H.323 ze Strażnikiem (z Wymagania 1) oraz ponieważ elementem obowiązkowym architektury funkcjonalnej są serwery SIP (*proxy* lub *redirect*) wynika, że rozważana będzie następująca konfiguracja opisana w [15] jako scenariusz numer 4 – wykorzystujący zarówno Strażnika jak i serwer SIP (*proxy* lub *redirect*).
Wymaganie 4: Skoro pojedynczo obie sieci muszą być bezpieczne, więc połączenie ich z wykorzystaniem IWF **musi** gwarantować każdej z sieci poziom bezpieczeństwa adekwatny do tego, jaki oferuje wewnątrz. Również mechanizmy zabezpieczeń wykorzystane po jednej stronie IWF powinny być adekwatne do rozwiązań drugiej strony.
Wymaganie 5: W przypadku, gdy nie jest zapewniony żaden mechanizm gwarantujący usługę uwierzytelnienia połączenie **nie może** zostać nawiązane. Podobnie postępujemy w przypadku niemożności zapewnienia usługi poufności. Wynika to z faktu nie wypełnienia kryterium uznania protokołu sygnalizacyjnego VoIP za bezpieczny – patrz punkt 5.
Wymaganie 6: Istotnym aspektem dla współpracy protokołów sygnalizacyjnych SIP i H.323 jest problem zakresu przezroczystości IWF SIP-H.323. W tym przypadku pozostaje w mocy Założenie F.

Ważna jest również odpowiedź na pytanie, czy IWF jest elementem zaufanym sieci (*Trusted Element*). Za obowiązującą definicję elementu zaufanego przyjmujemy definicję zawartą w zaleceniu H.235v4 [3], rezultatem zaufania określonej jednostce jest możliwość powierzenia mu pewnych parametrów kryptograficznych (np. klucza szyfrującego, parametrów charakterystycznych) bez narażenia na ich pozyskanie przez stronę trzecią do tego nie upoważnioną, czyli bez narażenia na utratę swojego bezpieczeństwa. Stąd kolejne wymaganie postaci:
Wymaganie 7: IWF **musi** być elementem zaufanym dla obu stron sieci (zgodne z Założeniem S3). W innym przypadku nie jest możliwe przeprowadzenie m.in. uwierzytelnienia pomiędzy dwoma punktami końcowymi dla tych sieci, a tym samym taki system, połączonych protokołów sygnalizacyjnych, nie może być uznany za bezpieczny (w świetle kryterium z punktu 5).

Inne założenia z dokumentów [11] i [15] dotyczące IWF SIP-H.323 pozostają w mocy, jeśli nie kolidują z Wymaganiami 1-7. Szczególnie dotyczy to wymagań dotyczących bezpieczeństwa.

8.2 Dekompozycja funkcjonalna IWF SIP-H.323

Zgodnie ze zdefiniowanymi w poprzednim punkcie wymaganiami dla bezpieczeństwa sygnalizacji łączonych sieci VoIP, w których występuje jednostka logiczna IWF proponuję następującą jej dekompozycję funkcjonalną:



Rys. 12. Dekompozycja funkcjonalna IWF SIP-H.323

Części występujące na rysunku opisano poniżej:
GK Part – część IWF, która widziana jest od strony części H.323 jako Strażnik, posiadająca podobne funkcje i własności (szczególnie w zakresie wspierania mechanizmów zabezpieczeń),
SIP Server Part – część IWF, która widziana jest od strony sieci SIP jako Serwer SIP (*proxy* lub *redirect*), posiadająca podobne funkcje i własności (szczególnie w zakresie wspierania mechanizmów zabezpieczeń),
IWF – część zapewniająca funkcję konwersji sygnalizacji SIP-H.323 oraz inne niezbędne do współpracy funkcje. Ta cześć nie zajmuje się wyliczaniem parametrów kryptograficznych (np. wyliczanie skrótu) – może jedynie pośredniczyć w ich przekazywaniu pomiędzy pozostałymi częściami.

SIP UA (SIP User Agent) – Agent Użytkownika SIP,
EP H.323 (End Point H.323) – punkt końcowy H.323.
SIP Proxy (Redirect) – elementy architektury funkcjonalnej protokołu SIP: serwery Proxy lub Redirect
GateKeeper (Strażnik) – element architektury funkcjonalnej protokołu H.323

Taki podział funkcji IWF jest najbardziej intuicyjny i najprostszy (abstrahujemy od aspektów finansowych realizacji takiego urządzenia). Głównymi zaletami takiego rozwiązania są przede wszystkim:

- Możliwość zapewnienia usługi uwierzytelnienia oraz poufności dla wiadomości sygnalizacyjnych sieci łączonych. Dotychczas proponowane rozwiązania nie spełniały postawionych przez nas wymagań bezpieczeństwa lub spełniały tylko ich część.

- Z obu stron sieci element ten jest rozpoznawany jako jeden z „normalnych" komponentów architektury funkcjonalnej: Strażnik lub jeden z serwerów SIP. Takie rozwiązanie **nie** wymaga, więc modyfikacji zarówno protokołu SIP jak i H.323. W przypadku nie odnalezienia w swojej części sieci punktu końcowego, do którego adresowana jest wiadomość SIP Serwer oraz GK wiedzą, że należy się kontaktować z częścią IWF odpowiednio będącą serwerem SIP (*SIP Serwer Part*) lub Strażnikiem (*GK Part*).
- Prosta współpraca mechanizmów zabezpieczeń SIP i H.323.
- Gwarancja pełnej przezroczystości dla komunikacji pomiędzy punktami końcowymi.

8.3 Szkic uwierzytelnienia łączonych systemów SIP-H.323

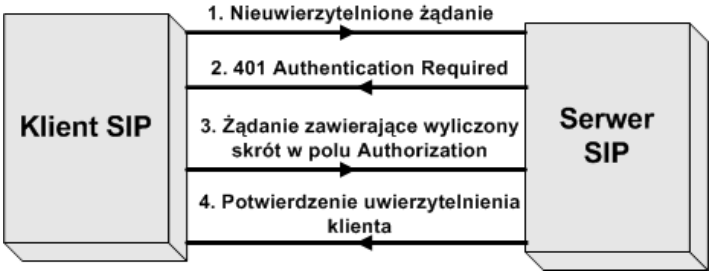
Jak wspomniano dla SIP obowiązkowym mechanizmem zabezpieczeń dla gwarancji usługi uwierzytelnienia jest SIP Digest. Opcjonalnie dostępny jest również protokół S/MIME.

Tę samą usługę dla H.323 realizuje się z wykorzystaniem opisanego w zaleceniu H.235v4 mechanizmu pochodzącego z profilu podstawowego (Procedura IA) o nazwie HMAC-SHA1-96. Alternatywą dla wspomnianego rozwiązania są mechanizmy zawarte w profilach: wykorzystującym podpisy cyfrowe oraz hybrydowym.

Skoncentrujmy się na możliwości poszukania, odpowiednika rozwiązania SIP Digest, gdyż jest to, jak już wspomniałem, mechanizm, który **musi** być implementowany obligatoryjnie w systemie VoIP bazującym na SIP. Spośród dostępnych rozwiązań w H.323 najbardziej naturalnym, pozwalającym zminimalizować wprowadzane opóźnienie, jest mechanizm HMAC-SHA1-96 oraz Procedura IA.

Aby pokazać słuszność tego wyboru należy przypomnieć krótko najważniejsze cechy oraz sposób działania obu rozwiązań:

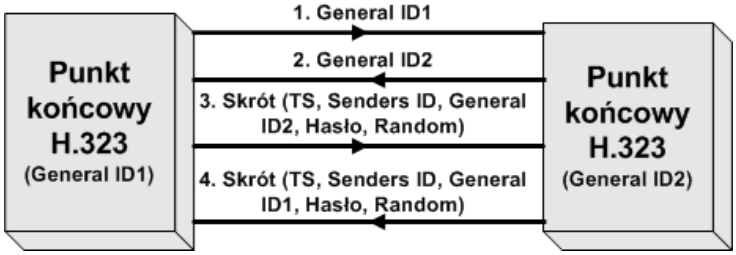
Mechanizm SIP Digest – wykorzystuje schemat współdzielonego sekretu oraz metodę wyzwanie/odpowiedź (*challenge/response*) wraz z funkcją skrótu. Jest to mechanizm typu *End-to-End*. Przebieg realizacji omawianej usługi dla mechanizmu SIP Digest został przedstawiony na rysunku poniżej:



Rys. 13. Przebieg uwierzytelnienia SIP Digest

Dokładny opis przebiegu uwierzytelnienia dla tego mechanizmu można znaleźć w [8].

Mechanizm HMAC-SHA1-96 - również wykorzystuje metodę współdzielonego sekretu oraz funkcje skrótu. Jest to mechanizm typu *Hop-by-Hop*. Przebieg uwierzytelnienia przedstawia rysunek poniżej:



Rys. 14. Przebieg uwierzytelnienia opartego na mechanizmie HMAC-SHA1-96 (Procedura IA)

W pierwszej fazie wymieniane są identyfikatory punktów końcowych. Kolejnym etapem jest przesłanie do drugiej strony skrótu, który został obliczony z parametrów zawartych w sekcji *CryptoToken*, czyli: znacznika czasowego (TS), identyfikatorów źródła i przeznaczenia (Senders ID oraz General IDx), współdzielonego hasła oraz wartości losowej (Random). Uwierzytelnienie następuje po odebraniu skrótu, obliczeniu analogicznego po stronie odbiorczej i ich porównaniu zakończonym sukcesem. Dokładny opis działania mechanizmu znajduje się w [3].

W obu algorytmach (tzn. SIP Digest oraz HMAC-SHA1-96) założono istnienie wzajemnie akceptowalnego odniesienia czasowego, z którego korzysta się w przypadku generowania znaczników czasowych. To, jakie odchylenia czasowe są akceptowalne, zależy już od konkretnej implementacji. Zastosowanie znaczników czasowych może zminimalizować ryzyko podsłuchania wiadomości, a następnie wykorzystania zdobytych informacji w celu wysłania fałszywej wiadomości mechanizmów z doklejonym zdobytym skrótem.

Jak widać w obu przypadkach wygenerowany zostaje pewien skrót, oba mechanizmy działają na zasadzie współdzielonego sekretu oraz w obu możliwe jest wykorzystanie tej samej funkcji skrótu SHA1.

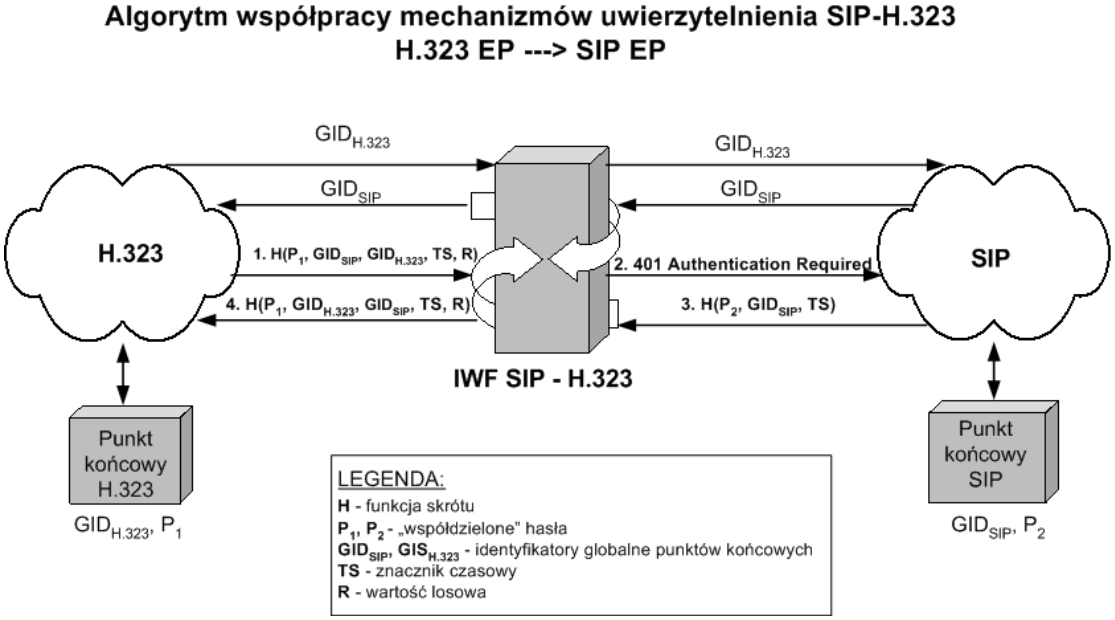
W przypadku SIP skrót jest tworzony z trzech podstawowych elementów: współdzielonego hasła, parametru *nonce* oraz nazwy użytkownika, czyli:

SIP Digest: H (Password, UserName, Nonce)

Analogicznie w H.323 do generacji skrótu wykorzystuje się pięć podstawowych elementów, a są to: współdzielone hasło, globalny identyfikator strony wysyłającej i docelowej, znak czasowy (*Timestamp*) oraz liczba losowa, czyli:

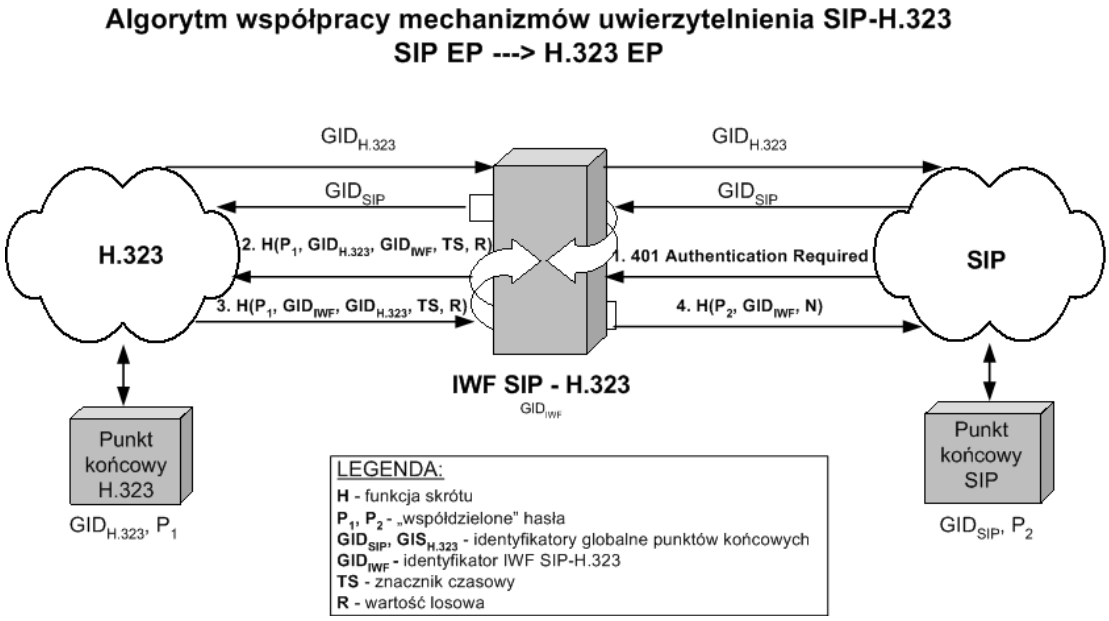
HMAC-SHA1-96: H (Password, SendersID$_S$, GID$_X$, TimeStamp, Random)

Przykładowy sposób współdziałania opisanych mechanizmów, w którym uczestniczą zarówno urządzania końcowe SIP i H.323 oraz IWF SIP-H.323 przedstawiają dwa poniższe rysunki. Pierwszy obrazuje sytuację, w której stroną inicjującą jest terminal H.323, natomiast drugi sytuację odwrotną.



Zakładamy, że w pierwszej fazie wymieniane są unikalne identyfikatory punktów końcowych sieci. Następnie punkt końcowy H.323, jako strona inicjująca, przesyła wyliczony przez siebie skrót (zgodnie ze swoim mechanizmem uwierzytelnienia – Procedura IA) (1) do IWF. Po odebraniu tego skrótu IWF wysyła do punktu końcowego SIP wiadomość numer *401 Authentication Required*, żeby wymusić wysłanie skrótu SIP Digest (3). Po jego otrzymaniu IWF wylicza analogiczny skrót jak punkt końcowy SIP, a następnie porównuje je. Jeśli oba skróty są sobie równe to IWF wysyła skrót (4) do sieci H.323, aby dokończyć realizację uwierzytelnienia. Ta ostatnia czynność implikuje fakt, iż IWF **musi** być elementem zaufanym, ponieważ znany jej będzie współdzielony sekret obu punktów końcowych.

Natomiast sytuację, w której stroną inicjującą jest punkt końcowy SIP przedstawia rysunek:



Podobnie jak w poprzednim przypadku zakładamy, iż w pierwszej fazie wymieniane są unikalne identyfikatory punktów końcowych sieci. Następnie punkt końcowy SIP, jako inicjująca strona, żąda uwierzytelnienia strony H.323, dlatego też wysyła żądanie *401 Authentication Required* (1). Po odebraniu tej wiadomości funkcja IWF przesyła do punktu końcowego H.323 skrót wykorzystujące parametry charakterystyczne dla tegoż punktu (2). Kolejny na drodze komunikacyjnej element H.323 po otrzymaniu tegoż skrótu odpowiada zgodnie z działaniem algorytmu uwierzytelniającego swoim skrótem (3). Ostatnią rzeczą jest wysłanie z IWF do punktu końcowego SIP odpowiedniego skrótu (4) tak, aby po swojej stronie punkt końcowy mógł dokonać porównania obu skrótów i zakończyć proces uwierzytelnienia. Również w tym przypadku funkcja IWF **musi** być elementem zaufanym, ponieważ do przeprowadzenia wzajemnego uwierzytelnienia niezbędna jest znajomość współdzielonego sekretu punktów końcowych.

Po stronie sieci H.323 uwierzytelnienie przebiega w trybie *Hop-by-Hop*, czyli przy każdej parze elementów sieciowych wartości skrótu ulegają ponownemu wyliczeniu. Końcowy ‘hop’ przypada wtedy, gdy urządzeniem docelowym jest IWF. Następnie wysyła ona (już w trybie *End-to-End*) żądanie uwierzytelnienia do punktu końcowego SIP.

Gdy stroną inicjującą jest punkt końcowy SIP możemy napotkać na następujący problem. IWF wysyła swój skrót do pierwszego elementu sieciowego H.323. Ten odpowiada jej wyliczonym przez siebie skrótem. Daje to pewność uwierzytelnienia na pierwszym odcinku za IWF SIP-H.323. Potencjalnie może pojawić się problem, gdy operacja uwierzytelnienia nie „dojdzie” do punktu końcowego H.323.

8.4. Poufność łączonych systemów SIP-H.323

Zapewnienie usługi poufności wiąże się przede wszystkim z wykorzystaniem techniki szyfrowania. Dla obu protokołów metoda realizacji usługi poufności jest zapewniania poprzez wykorzystanie mechanizmów warstw niższych: TLS i IPSec. Dla SIP obowiązkowe jest implementowanie algorytmu TLS, natomiast IPSec jest opcjonalne. Dla H.323 oba rozwiązania są opcjonalne.

Istnieje, zatem potrzeba implementowania tego rodzaju rozwiązań, szczególnie, dlatego, iż w H.323 w inny sposób nie da się zagwarantować poufności. W związku z tym, że w protokole SIP niezbędne jest wykorzystywanie mechanizmu TLS, dlatego też proponuje się, aby dla bezpiecznej współpracy łączonych systemów VoIP, stosowano w części z H.323 również **obowiązkowo** ten mechanizm. A ponieważ możliwe jest dodatkowo w SIP stosowanie mechanizmu SIPS URI, dlatego też niezwykle ważne jest, aby mechanizmów sieci H.323 wszystkie odcinki drogi komunikacyjnej pomiędzy elementami: źródłowym mechanizmów docelowym były również zabezpieczone mechanizmów wykorzystaniem TLS.

Literatura

[1] K. Singh, H. Schulzrinne, „Interworking Between SIP/SDP and H.323", IPTel, Maj 2000
[2] "Packet-based multimedia communications systems" – H.323, Telecommunication Standardization Sector, ITU-T, lipiec 2003
[3] "Security and Encryption for H-Series (H.323 and other H.245-Based) multimedia terminals"s, Telecommunication Standardization Sector, ITU-T, sierpień 2003.
[4] ETSI TR 101 308, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; SIP and H.323 Interworking", grudzień 2001
[5] Mika Marjalaakso, "Security Requirements and Constraints of VoIP", Helsinki University of Technology Department of Electrical Engineering and Telecommunications
[6] Johann Thalhammer, "Security in VoIP - Telephony Systems", Institute for applied information processing and communications, Graz University of Technology, 2002
[7] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", Request for Comments: 2104, luty 1997
[8] W. Mazurczyk, „Bezpieczeństwo SIP jako protokołu sygnalizacyjnego VoIP" – Krajowe Sympozjum Telekomunikacji (KST), wrzesień 2003, artykuł recenzowany
[9] F. Cuervo, N. Greene, A. Rayhan, "Megaco Protocol Version 1.0" - IETF RFC 3015 listopad 2000
[10] M. Handley, H. Schulzrinne, J. Rosenberg "SIP: Session Initiation Protocol" – IETF RFC 3261 lipiec 2002
[11] H. Schulzrinne, C. Agboh, "Session Initiation Protocol (SIP) - H.323 Interworking Requirements", Internet Draft, luty 2004 (draft-agrawal-sip-h323-interworking-reqs-06)
[12] F. Echezabal, "Voice over Internet Protocol Security", SANS Institue, marzec 2003
[13] CERT, "Advisory CA-2004-01 Multiple H.323 Message Vulnerabilities", styczeń 2004
[14] CERT, „CA-2003-06 Multiple vulnerabilities in implementations of the SIP", luty 2003
[15] H. Agrawal, C. Agboh, H. Schulzrinne, „SIP-H.323 Interworking", IETF Internet Draft, lipiec 2001
[16] N. Leavitt, "Will Interoperability Problems Give IP Telephony a Busy Signal?", Computer.org,marzec 2004
[17] W. Stallings - "Cryptography and Network Security : Principles and Practice, Second Edition". Prentice-Hall, June 1998.

Artykuł recenzowany