Bezpieczeństwo VoIP – mit czy fakt?

Kwestia szeroko rozumianego bezpieczeństwa, w obecnym świecie, nabiera coraz większego znaczenia. Jest to pojęcie bardzo szerokie pojawiające się w wielu aspektach naszego życia. Wydźwięk tego słowa jest zwykle pozytywny – każdy z nas chciałby by wszystko wokół niego było bezpieczne lub chce czuć się bezpieczny.

Potrzeba zapewnienia bezpieczeństwa nie ominęła również obszaru teleinformatyki. Obecnie obserwuje się wzrost znaczenia informacji oraz dążenie społeczeństw do informatyzacji życia codziennego (pojęcie społeczeństwa informacyjnego). Wymaga się, aby informacja ta docierała tylko i wyłącznie do właściwych adresatów i aby w czasie jej transportu nie uległa przekłamaniu lub podsłuchaniu.

I tu rodzi się pytanie: czy jesteśmy jednak absolutnie przekonani, że oferowane nam rozwiązania teleinformatyczne (oprogramowanie, systemy, sieci itp.) są całkowicie bezpieczne, a może jesteśmy za bardzo dociekliwi?

Czym jest VoIP?

Usługa VoIP (Voice over Internet Protocol) nazywana również telefonią IP lub nieco mylnie telefonią internetową (ponieważ termin ten ogranicza zakres działania VoIP jedynie do Internetu) oznacza przesyłanie głosu w czasie rzeczywistym wykorzystując do tego celu pakietową sieć transmisji danych z protokołem IP. Umożliwia ona prowadzenie rozmów w sieciach lokalnych lub rozległych (np. Internecie), pozwalając na komunikowanie się z osobami lub instytucjami w praktycznie dowolnym miejscu na świecie korzystając z przyłączonego do danej sieci komputera bądź aparatu telefonicznego.

Historia tej techniki, co ciekawe, sięga lat siedemdziesiątych – pierwsze publikacje związane z transmisją głosu w sieciach pakietowych opublikowano już w RFC 741 (Specifications for the Network Voice Protocol) w 1977 roku. W tych czasach, jak również przez następne prawie 20 lat, nikt jednak poważnie nie traktował pomysłu telefonii IP – była to raczej ciekawostka pozostająca w kręgu zainteresowań badaczy i hobbystów. Wynikało to z braku rozwiązań zarówno technologicznych jak i ideowych. Dopiero pod koniec XX w. rola techniki VoIP znacznie wzrosła. Miało to związek głównie z niezaprzeczalnym sukcesem Internetu i nierozerwalnie z nim związanym protokołem IP.

Pierwszy system telefonowania IP został opracowany przez firmę VocalTec dopiero w 1995r., a pierwsze urządzenie VoIP (brama) weszła na rynek rok później. To właśnie wtedy użytkownicy mogli po raz pierwszy porozmawiać ze sobą w czasie rzeczywistym, używając do tego celu oprogramowania, które przesyłało przez sieć LAN pakiety zawierające strumienie audio.

Zastosowania telefonii IP

W wykorzystaniu VoIP szczególnie nęcącą jest wizja konwergencji (łączenia) sieci transmisji danych i telefonii w jedną uniwersalną sieć teleinformatyczną. Takie rozwiązanie może prowadzić do znacznych oszczędności, głównie w korporacjach, poprzez wykorzystanie tej samej infrastruktury sieciowej dla obu zastosowań.

W świetle powyższych faktów podstawowymi przyczynami zainteresowania VoIP jest:

- możliwość integracji sieci danych z „głosowymi" tak, aby móc zaspokoić wzrastające zapotrzebowanie na produkty wielousługowe (np. głos, dane i wideo),
- konsolidacja pasma poprzez używanie jednej sieci dla wszystkich rodzajów ruchu,
- olbrzymia popularność protokołu IP obsługiwanego przez większość komputerów PC i stacji roboczych,
- wzrost zapotrzebowania na złożone usługi np. czasu rzeczywistego, czy wideo typu „full motion".

Obecnie VoIP najczęściej wykorzystuje się jako rozwiązania teleinformatyczne dla firm. W takim przypadku wdrażanie systemu telefonii IP może odbywać się dla różnych sytuacji wejściowych. Jeśli dana korporacja posiada / chce zbudować swoją sieć teleinformatyczną to w zależności, czy jest to budowa „od zera", czy też modyfikacja istniejącej infrastruktury możliwe są następujące scenariusze:

1. Rozwiązaniem najbardziej popularnym jest **łączenie istniejących central telefonicznych poprzez sieć IP** (własną lub Internet). W tej sytuacji rozmowy telefoniczne między centralami przesyłane są z pominięciem sieci telefonicznej – do tego celu wykorzystuje się sieć transmisji danych z protokołem IP. W razie problemów z siecią pakietową połączenia realizowane są poprzez sieć telefoniczną. W tym przypadku oszczędza się głównie na koszcie połączeń.
2. Gdy budowana jest **nowa infrastruktura komunikacyjna**, wtedy zamiast tradycyjnej centrali wybiera się implementację systemu VoIP. W takim przypadku zazwyczaj całość instalacji i infrastruktury (sieć komputerowa i telefoniczna) jest projektowana od nowa. Dzięki temu oszczędza się zarówno na połączeniach jak i na fakcie konieczności utrzymywania tylko jednej infrastruktury sieciowej (oraz jednego „typu" personelu do jej obsługi).
3. **Eksploatowana centrala zostaje zastąpiona** (np. ze względu na jej zużycie techniczne) **lub uzupełniona systemem IP** ze względu na jego szczególne cechy (np. wdrożenie nowych usług) – wtedy koszt implementacji systemu jest obciążony dodatkowo kosztami związanymi z likwidacją lub niewykorzystaniem możliwości dotychczasowej centrali. Zwykle rekompensują to jednak korzyści, uzyskane z dodatkowych elementów wprowadzonych do systemu, np. zaawansowanych aplikacji wspomagających kontakty z klientami (dział handlowy, pomoc techniczna, czy call center).

Dodatkowo należy podkreślić, iż rozwiązania VoIP sprawdzają się najlepiej w zastosowaniach, w których niezbędna jest komunikacja pomiędzy oddalonymi od siebie oddziałami firmy. Przyczyna sukcesu na tym polu jest prosta – gdy firma posiada już korporacyjną sieć transmisji danych, rozszerzenie jej funkcjonalności o usługę telefonii redukuje – praktycznie do zera – koszty klasycznych połączeń komutowanych między oddziałami firmy (głównie międzymiastowych, więc oszczędności są tym większe). Dochodzą do tego wspomniane już wcześniej oszczędności na czasie i kosztach obsługi systemu telefonicznego. Klasyczna sieć telefoniczna wymaga posiadania w każdym oddziale firmy centralki abonenckiej, obsługującej numery wewnętrzne danego oddziału oraz personelu do jej konfiguracji i obsługi sytuacji wyjątkowych (np. awarii).

Natomiast system telefonii IP może być zarządzany centralnie przez jeden serwer dla całej sieci korporacyjnej. Utrzymaniem systemu zajmuje się administrator, który może reagować na awarie jak i modyfikować system,

np. poprzez przeglądarkę WWW (zdalny dostęp).

Telefonia wykorzystująca VoIP na pewno ma szansę stać się techniką, która może mieć ogromny wpływ na przyszły kształt całego rynku telekomunikacyjnego. Potencjał, który może „skusić" abonentów jest ogromny – pytanie tylko czy da się to wszystko w satysfakcjonujący sposób zaimplementować – innymi słowy, czy powstaną odpowiednie protokoły i urządzenia gwarantujące obiecane usługi oraz ich jakość?

Co jest „w środku" telefonii IP...

Całość sesji połączeniowej dla VoIP podzielona jest na dwie fazy: **sygnalizacyjną** (która kontroluje sesję) oraz **transportującą media** (tzn. strumień danych). Połączeniem, w tym przypadku, nazywamy więc jedynie określony stan sygnalizacji pomiędzy urządzeniami końcowymi.

W VoIP całość działań realizowana jest poprzez **zespół protokołów**, który można podzielić na cztery podstawowe grupy:

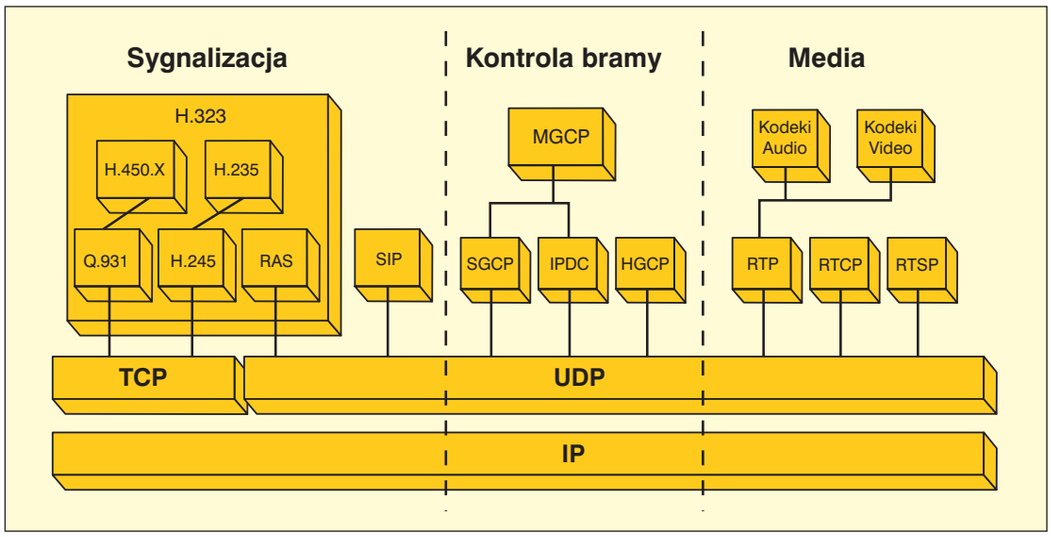
1. kodeków mowy (np. G. 729),
2. protokołów transportowych (RTP, UDP, TCP),
3. protokołów sygnalizacyjnych (H. 323, SIP, MGCP, H. 248/ /Megaco),
4. protokołów uzupełniających (SDP, RTSP, RSVP).

Najważniejszą spośród powyższych grup jest zbiór protokołów sygnalizacyjnych, ponieważ są one „sercem" telefonii internetowej. To właśnie od nich zależy architektura sieci, realizacja zaawansowanych usług oraz współdziałanie z tradycyjnymi sieciami telefonicznymi. Do podstawowych funkcji protokołów sygnalizacyjnych należy zaliczyć:

- translację adresów i lokalizację użytkownika wywoływanego,
- otwieranie i zamykanie sesji,
- negocjację parametrów sesji i ewentualnie ich modyfikację w trakcie połączenia,
- zarządzanie grupą uczestników sesji,
- zarządzanie przebiegiem połączeń.

Niestety obecnie nie ma jednego międzynarodowego standardu protokołu sygnalizacyjnego dla VoIP (co jest z pewnością czynnikiem hamującym popularność tej techniki). Najbardziej znanymi protokołami tego typu są: **SIP (Session Initiation Protocol), H. 323, MGCP (Media Gateway Control Protocol)** oraz **H. 248/Megaco**.

Poniższy rysunek prezentuje stos protokołów dla realizacji usługi VoIP dla poszczególnych protokołów sygnalizacyjnych opisanych powyżej:



Rys. 1. Stos protokołów dla VoIP

Bezpieczeństwo VoIP

Zagwarantowanie bezpiecznych połączeń dla usługi VoIP jest sprawą złożoną. Nie ogranicza się ono tylko do zapewnienia zabezpieczonego transportu strumieni danych zawierających głos. O wiele ważniejszą sprawą jest fakt, w jakich warunkach przesyłane są wiadomości protokołu sygnalizacyjnego, na którym bazuje VoIP. Bez bezpiecznej sygnalizacji nie ma połączenia, czyli transportu strumienia danych (de facto rozmowy). Poza tym, każdy negatywny wpływ na przepływ wiadomości sterujących może spowodować natychmiastowe zerwanie trwającego połączenia.

W świetle powyższych stwierdzeń, problemy bezpieczeństwa dla usługi telefonii IP można podzielić na:

a/ bezpieczeństwo wiadomości sygnalizacyjnych wymienianych pomiędzy stronami komunikującymi się,

b/ bezpieczeństwo strumieni mediów przenoszących głos (pakiety RTP),

c/ problemy związane z „przechodzeniem" pakietów przez ściany przeciwogniowe (Firewalls) oraz przez mechanizmy translacji adresów wewnętrznych (np. intranetowych) na zewnętrzne (np. internetowe) NATs (Network Address Translators).

Dodatkowo należy stwierdzić, iż dla VoIP bezpieczeństwo przepływu pakietów „z głosem" jest zapewniane niezależne od gwarantowania bezpiecznej sygnalizacji.

Natomiast trzecia grupa problemów dotyczy raczej sieci będącej implementacją usługi VoIP. W takim systemie z powodu wymienionych „przeszkód" może dojść do uniemożliwienia:

- nawiązania połączenia z powodu blokowania pakietów zawierających wiadomości sygnalizacyjne,
- porozumiewania się przez strony żądające komunikacji ze względu na blokowanie pakietów RTP.

Zagrożenia i mechanizmy bezpieczeństwa VoIP

Ataki na telefonię IP są realizowane z wykorzystaniem odpowiednich technik, wśród których wyróżnia się przede wszystkim: **podszycie się** (spoofing), **podsłuchiwanie** (sniffing) oraz **blokowanie działania** (Denial of Service).

Podstawowymi atakami na telefonię IP wykorzystującymi przedstawione powyżej techniki są:

– **Blokowanie działania** (Denial of Service) – zwykle skupia się na celowym „wyłączeniu" funkcjonalności poszczególnych urządzeń znajdujących się w sieci VoIP poprzez jego przeciążenie (wykorzystuje głównie technikę blokowania działania),

– **Kradzież usługi** (Theft of Service) – atak wymierzony w dostawcę usług mający na celu nielegalne, nieodpłatne skorzystanie z usług dostawcy (wykorzystuje przede wszystkim technikę podszycia się),

– **Naruszenie prywatności** (Invasion of privacy) – zwykle atak tego typu wykorzystuje techniki podsłuchiwania czy podszycia się i jest to działanie wymierzone w użytkownika.

Aby przeciwdziałać atakom na usługę VoIP, bezpieczeństwo gwarantowane

protokołom sygnalizacyjnym może być realizowane na dwa sposoby z wykorzystaniem mechanizmów bezpieczeństwa:
- **Wewnętrznych** wbudowanych w protokół sygnalizacyjny,
- **Zewnętrznych** – pochodzących z innych aplikacji lub zapewnianych przez mechanizmy warstw niższych niż warstwy aplikacji modelu odniesienia TCP/IP, np. TLS, czy IPSec.

Dodatkowo możliwe jest jednoczesne wykorzystanie obu typów tych mechanizmów.

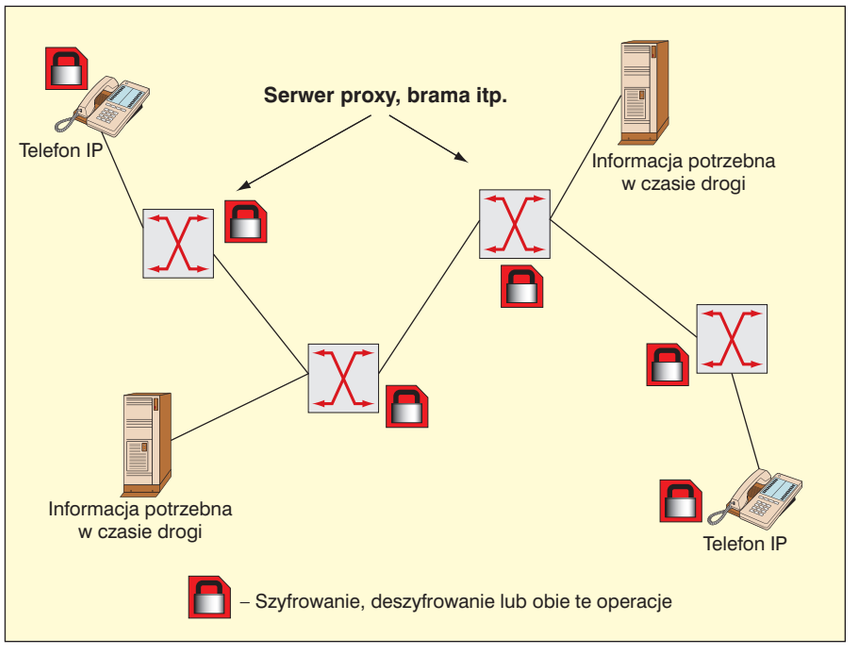
Porównanie bezpieczeństwa telefonii IP z jej klasycznym odpowiednikiem

Aby telefonia internetowa stała się atrakcyjna dla użytkowników musi oferować podobny poziom usług jak w przypadku tradycyjnej telefonii, a dodatkowo zachęcać innymi zaletami, których nie posiada jej konkurent. Zagwarantowanie bezpieczeństwa połączeń jak i wymiany wiadomości sygnalizacyjnych jest z pewnością ważnym aspektem dla tej usługi i może w znacznym stopniu wpływać na jej popularność. Zatem oferowany przez systemy VoIP poziom bezpieczeństwa nie może być mniejszy niż jej klasycznego odpowiednika. Dodatkowo należy uwzględnić charakterystyczne cechy sieci transportowej, którą jest w tym przypadku sieć wykorzystująca protokół IP.

Dlatego też porównanie bezpieczeństwa oferowanego przez telefonię IP (bez zastosowania mechanizmów bezpieczeństwa) z tą samą cechą telefonii tradycyjnej wychodzi na niekorzyść telefonii internetowej. Dzieje się tak z dwóch podstawowych powodów:
- Przy przesyłaniu niezaszyfrowanych pakietów VoIP (czy to sygnalizacyjnych, czy RTP) intruz, aby wykonać udany atak (np. poprzez penetrację zawartości pakietu) musi posiadać jedynie odpowiednią aplikację tzw. „sniffer". Znalezienie takiego programu przy dostępie do sieci Internet nie jest wcale zadaniem trudnym. W przypadku telefonii tradycyjnej (z wyłączeniem sieci komórkowych), aby osiągnąć ten sam cel atakujący musi posiadać specjalne urządzenie, fizycznie przyłączone do sieci (potencjalnie trudniejsze wykonanie),
- Sieć IP jest trudniej zabezpieczyć, ponieważ właściwie każdy użytkownik (nie tylko systemu VoIP, ale w ogóle sieci IP) może być potencjalnym atakującym. Natomiast, jeśli chodzi o sieć z komutacją łączy (PSTN) to nie jest ona wcale całkowicie zabezpieczona, ale gwarantowany przez nią poziom bezpieczeństwa jest akceptowalny przez jej użytkowników.

Możliwości bezpieczeństwa VoIP

Stosowane w telefonii IP mechanizmy bezpieczeństwa powinny gwarantować przede wszystkim dwie podstawowe usługi ochrony informacji oraz komunikacji w sieci – uwierzytelnienie oraz poufność zdefiniowane następująco:
- **Poufność** – dająca ochronę przed atakami pasywnymi oraz zabezpieczającej wiadomości sygnalizacyjne wymieniane pomiędzy komunikującymi się jednostkami przed ich nieuprawnionym uzyskaniem przez strony do tego nieupoważnione;
- **Uwierzytelnienie (zawierające integralność)** – gwarantujące ochronę przed atakami aktywnymi oraz kontrolę tożsamości stron i wiadomości sygnalizacyjnych wymienianych pomiędzy nimi.



Rys. 2. Działanie mechanizmu Hop-by-Hop dla realizacji usługi poufności

Słabości, luki czy ograniczenia bezpieczeństwa mogą pojawiać się w systemach wykorzystujących telefonię internetową z różnych powodów, m.in. z błędnej lub niekompletnej implementacji określonych protokołów dla stosu protokołów VoIP. Dodatkowo sama sieć pakietowa, np. Internet wprowadza pewne zagrożenia i ograniczenia. Chodzi tu głównie o wspomniane już problemy związane z wykorzystaniem elementów Firewall i NAT oraz stosunkowo niewielką wiedzę wymaganą do przeprowadzenia udanego ataku w sieciach IP.

Aby sprostać wymaganiom dla bezpiecznego systemu VoIP, stworzono dwa typy mechanizmów bezpieczeństwa: **Hop-by-Hop** oraz **End-to-End**. Oba posiadają zarówno wady i zalety.

Rozwiązania End-to-End cechują się tym, że:
- jedynie dostawca usług musi posiadać klucz publiczny – użytkownik końcowy nie jest zobowiązany go posiadać,
- gwarantowane jest zabezpieczenie, co najmniej pierwszego odcinka połączeniowego na całej drodze sygnalizacyjnej (czyli pomiędzy użytkownikiem końcowym a pierwszym węzłem pośredniczącym),
- urządzenia pośredniczące mają łatwy dostęp do nagłówków, bądź innych potrzebnych informacji, ale za to są bardziej skomplikowane,
- wszystkie elementy funkcjonalne muszą ufać wszystkim urządzeniom pośredniczącym na drodze sygnalizacyjnej,
- mechanizmy tego typu są już wykorzystywane i sprawdzają się np. w sieci Internet,
- wykonywanie tych samych operacji (szyfrowanie, deszyfrowanie) w każdym urządzeniu pośredniczącym wprowadza dodatkowe opóźnienia, co wpływa ujemnie na parametr QoS (Quality of Service), który jest krytyczny dla jakości rozmowy VoIP.

Natomiast mechanizmy End-to-End odróżnia od mechanizmów Hop-by-Hop:
- uniemożliwienie odczytania wiadomości w czasie jej transportu,
- niemożliwość zabezpieczenia ca-

łej wiadomości za ich pomocą, gdyż część informacji niezbędna jest do rutowania,
- urządzenia końcowe muszą posiadać odpowiednią moc obliczeniową potrzebną do obsługi wykorzystywanego mechanizmu.

Z przytoczonych powyżej cech zarówno mechanizmów End-to-End jak i Hop-by-Hop można wywnioskować, iż trudno jest jednoznacznie określić, którego typu mechanizmy są skuteczniejsze. Zarówno jedne, jak i drugie posiadają wiele zalet, a jednocześnie poważnych słabości. W idealnej sytuacji, oczywiście, można by korzystać zarówno z jednego, jak i drugiego typów mechanizmów jednocześnie. Byłoby to możliwe, jeśli udałoby się w satysfakcjonujący sposób rozwiązać problem QoS w sieciach IP i dodatkowo zapewnić odpowiednią moc obliczeniową w urządzeniach końcowych oraz pośredniczących (co wpływa jednocześnie na ich cenę). To pozwoliłoby na wzajemne skompensowanie się ich słabości.

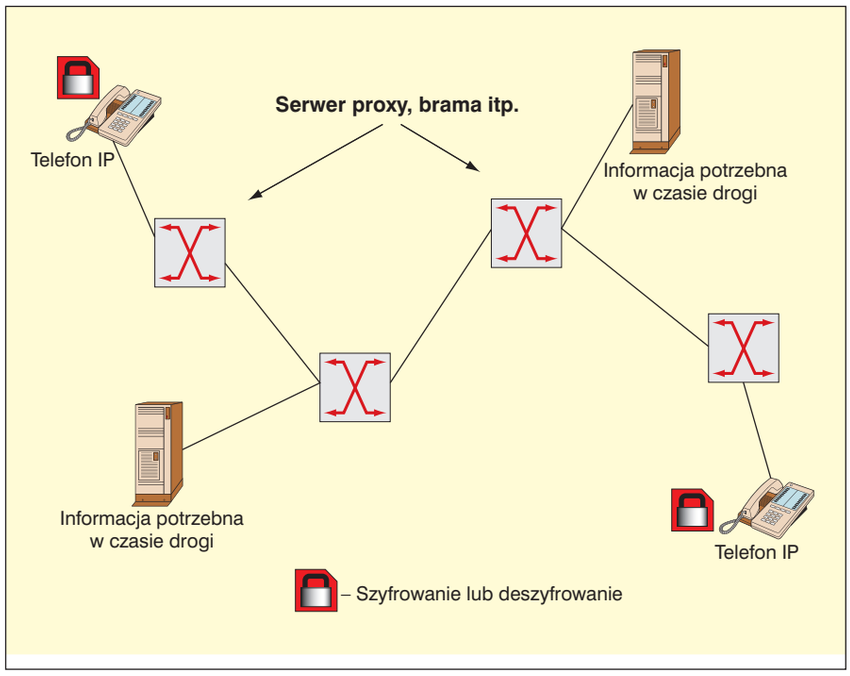
Jednak oczywiście do takiej sytuacji jest obecnie daleko, dlatego też pozostaje stosowanie takich rozwiązań, na które pozwalają parametry techniczne wykorzystywanej sieci i urządzeń się w niej znajdujących. Należy jednak bezwzględnie wykluczyć sytuację, w której nie stosowane będą żadne mechanizmy bezpieczeństwa.

Podsumowując, głównymi powodami, dla których mechanizmy bezpieczeństwa systemów VoIP nie są obecnie stosowane powszechnie są następujące:
- wprowadzają one dodatkowe opóźnienie (negatywny wpływ na 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 NAT'y.

Wymagania bezpieczeństwa dla VoIP

Jak w przypadku każdego produktu (np. telefonii) wymagania odnośnie bezpieczeństwa stawiane są przez **użytkowników**. Nikt nie będzie inwestował swoich pieniędzy oraz korzystał z określonej usługi, jeśli nie będzie miał całkowitego przekonania, co do jej jakości, czy wiarygodności.

Dla usługi telefonii ważne jest, aby zarówno informacje oraz parametry wymieniane w czasie rozmowy, jak i przy zestawianiu połączenia były niedostępne dla osób trzecich – jedyną akceptowalną stroną jest dostawca takiej usługi.



Rys. 3. Działanie mechanizmu End-to-End dla realizacji usługi poufności

W związku z tym istnieje potrzeba, aby każdy **bezpieczny** system VoIP spełniał, co najmniej następujące wymagania bezpieczeństwa:
- wszystkie połączenia pomiędzy poszczególnymi elementami sieci powinny być szyfrowane,
- zarówno klienci jak i serwery powinny być zabezpieczone przed atakiem typu Blokowanie działania (Denial of Service),
- uwierzytelnienie typu End-to-End powinno być zapewniane w terminalach,
- wszystkie urządzenia końcowe dla danego połączenia powinny zawsze dokonywać wzajemnego uwierzytelnienia (mutual authentication), co skutecznie zapobiegnie przeprowadzeniu ataku typu Man-In-The-Middle (MITM).

Dodatkowo, szczególnie dla rozwiązań korporacyjnych zaleca się, aby ruch głosowy (jak i dane) był przenoszony zarówno ze względów bezpieczeństwa jak i zapewnienia jakości rozmowy poprzez wydzierżawione osobne łącza z gwarantowaną przepustowością. To rozwiązanie jest obecnie najbardziej popularnym zastosowaniem usługi VoIP.

Podsumowania i prognozy

Z zaprezentowanych tutaj faktów można odnieść mylne wrażenie, iż nie da się połączyć zapewnienia satysfakcjonującego poziomu bezpieczeństwa usługi VoIP tak, aby nie odbijało się to w sposób negatywny na jej jakości i innych ważnych parametrach (np. cenie).

Jedynym oczywistym rozwiązaniem w takiej sytuacji jest odpowiednio wyważony kompromis. Dla przykładu, jeśli nie dysponujemy odpowiednimi mocami obliczeniowymi wszystkich elementów sieci, to należy zaimplementować jedynie te mechanizmy bezpieczeństwa, przy których jakość rozmowy jest akceptowalna przez użytkowników.

Pamiętajmy, iż każdy dodatkowy mechanizm bezpieczeństwa w systemie, nawet prymitywny, podnosi jego wartość, w sensie odporności na atak, gdyż jest kolejną „cegiełką w murze" budowanym przeciw potencjalnemu intruzowi. Pozostawienie wymiany wiadomości sygnalizacyjnych, czy strumienia danych bez jakichkolwiek zabezpieczeń może być fatalne w skutkach. Dlatego też, jeśli przykładowo system / sieć nie pozwala na całkowite szyfrowanie pakietów, wtedy należy skłonić się ku szyfrowaniu jedynie najważniejszych (z punktu widzenia bezpieczeństwa) jego pól nagłówka itp.

Dodatkowo zarówno przy zakupie sprzętu jak i oprogramowania VoIP należy bezwzględnie zwrócić uwagę na zastosowane w nim rozwiązania gwarantujące bezpieczeństwo. Na szczęście obecnie wybór takich rozwiązań daje duże pole manewru potencjalnemu nabywcy. Praktycznie każdy jest w stanie, przy posiadaniu pewnego stopnia świadomości zagrożeń dla VoIP oraz sieci pakietowych, dobrać odpowiedni dla swoich potrzeb „arsenał" mechanizmów bezpieczeństwa.

WOJCIECH MAZURCZYK