WOJCIECH MAZURCZYK
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail:wmazurczyk@tele.pw.edu.pl
http://mazurczyk.com

Aspekty bezpieczeństwa sieci P2P na przykładzie Skype

STRESZCZENIE

W artykule przedstawiono architekturę i sposób działania najpopularniejszego obecnie systemu telefonii IP, jakim jest Skype. W odróżnieniu od zestandaryzowanych systemów VoIP (Voice over IP) bazujących na protokołach sygnalizacyjnych takich jak: SIP (Session Initiation Protocol), czy H.323 wykorzystujących model sieci oparty na modelu klient-serwer, Skype działa w oparciu o model peer-to-peer (P2P). Specyfika organizacji i działania tego typu sieci jest zupełnie odmienna szczególnie w kontekście usługi telefonii. Dodatkowo należy wziąć pod uwagę fakt, iż jest to dotychczas jedyny tego typu system, który odniósł sukces komercyjny na taką skalę. Dlatego warto zapoznać się z jego charakterystycznymi elementami i funkcjami. W pracy dokonano również analizy i oceny bezpieczeństwa tego typu sieci oraz wskazano kryterium oceny bezpieczeństwa sieci telefonii IP opartej na P2P.

1. Wstęp

Telefonię IP można nazwać najpopularniejszą usługą sieci komputerowych początku XXI wieku. W ciągu ostatniej dekady szybkość pojawiających się standardów i produktów ją implementujących zwiększa się lawinowo. Można mówić o swoistej modzie na przesyłanie rozmów poprzez sieci pakietowe z protokołem IP, które dotychczas były wykorzystywane jedynie do transmisji danych. Zalet jakie niesie za sobą technologia VoIP (Voice over IP) jest wiele począwszy od konwergencji dwóch infrastruktur sieciowych w jedną, aż po spadek cen połączeń (bądź w ogóle ich brak).

Pomimo wciąż rosnącej popularności obecnie telefonia IP boryka się z kilkoma palącymi problemami, które hamują rozwój tego typu systemów. Mimo, iż systemów i produktów VoIP jest coraz więcej, szybkość rozwoju rynku nie jest tak imponująca jak przewidywano. Przyczyną takiego stanu rzeczy są przede wszystkim:

- niewystarczająca „zdolność pokonywania" firewalli oraz urządzeń implementujących NAT (Network Address Translation),
- brak gwarancji jakości rozmowy,
- problemy bezpieczeństwa zarówno sygnalizacji jak i transmisji głosu [10].

Na tym tle odpowiedź i triumf bezpłatnej aplikacji Skype [8] jest bezsprzeczny. Od sierpnia 2003 lat liczba użytkowników tego systemu cały czas rośnie i obecnie przekracza 50 milionów użytkowników. Jest to wynik jakim nie mogą poszczycić się żadni inni konkurenci na rynku rozmów pakietowych. O takim stanie rzeczy zadecydowały przede wszystkim:

- możliwość darmowego prowadzenia rozmów wewnątrz sieci Internet,
- bardzo dobra jakość prowadzonej rozmowy,
- brak problemów z pokonywaniem firewalli i urządzeń z NAT,
- prostota obsługi samej aplikacji (liczne wersje językowe, wsparcie wielu systemów operacyjnych),
- integracja innych popularnych usług internetowych: instant messaging (IM), utrzymywania listy kontaktów oraz konferencji.

Dodatkowo możliwe do wykupienia są usługi SkypeIn i SkypeOut. Pierwsza z nich umożliwia odbieranie telefonów z tradycyjnych sieci telefonicznych (PSTN), druga możliwość wykonywania połączeń wychodzących do tego typu sieci.

W czym należy upatrywać sukces komercyjny Skype, który to sprzedano za 3 miliony dolarów firmie eBay w 2005 roku [6] i w czym różni się od tradycyjnych systemów telefonii VoIP? Odpowiedź jest prosta: w fundamentalnym podejściu do architektury sieci. Dotychczasowe systemy telefonii IP bazują na rozpowszechnionym, poprzez sukces Internetu, modelu klient-serwer podczas, gdy twórcy Skype bazując na swoich doświadczeniach przy powstawaniu systemów takich jak Kaaza [9] wykorzystali model peer-to-peer (P2P).

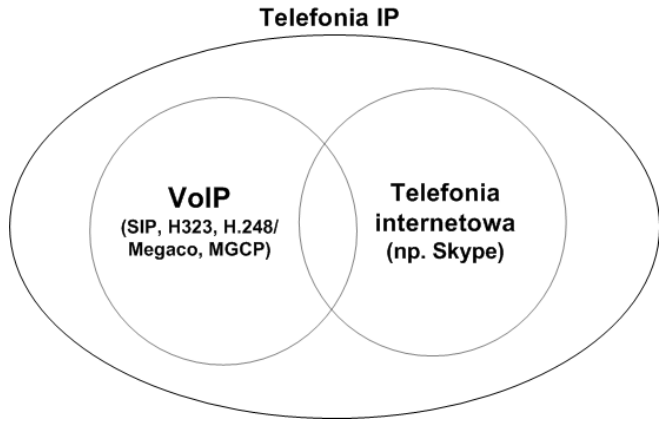
Pomimo tego, że oficjalnie producenci Skype nie udostępnili dokładnych specyfikacji sposobu implementacji tegoż systemu i mechanizmów w nim wykorzystanych, to na podstawie ostatnich badań [1, 2, 4, 5, 6] oszacowana zostanie przydatność architektury P2P dla sieci telefonii IP w kontekście oferowanego bezpieczeństwa w porównaniu do bieżących standardów VoIP.

Artykuł zorganizowany jest następująco: w punkcie drugim przedstawiony jest podział systemów telefonii IP. W trzecim scharakteryzowano najważniejsze cechy i elementy architektury Skype, a następnie w punkcie 4 dokonano analizy wybranych aspektów bezpieczeństwa. W kolejnym punkcie sformułowano kryterium oceny bezpieczeństwa systemów telefonii IP opartych na modelu sieci P2P. Całość kończy podsumowanie w punkcie 6.

2. Podział systemów telefonii IP

Zanim przejdziemy do charakteryzowania sieci telefonii IP opartej na modelu P2P niezbędne jest odpowiednia klasyfikacja i usystematyzowanie systemów telefonii pakietowej. Uprości to następnie samą ich analizę. Obecnie część podstawowych terminów związanych z telefonią pakietową jest często mylona, bądź uznawana za synonimy. Proponuję przyjąć podział zgodnie z rysunkiem 1, a w związku z tym rozgraniczyć pojęcia VoIP, telefonii IP i telefonii internetowej, biorąc pod uwagę przede wszystkim trzy aspekty:

- wykorzystywane protokoły sygnalizacyjne,
- zasięg wykorzystywanej sieci,
- model architektury systemu.



Rysunek 1. Proponowany podział systemów telefonii IP

Przy podziale kierowano się następującymi przesłankami:

1) Termin **VoIP** odnosi się do systemów telefonii IP, które oparte są na generycznych standardach protokołów sygnalizacyjnych takich jak: SIP (Session Initiation Protocol) [14], H.323 [15], czy H.248/Megaco [16], które zostały opracowane przez organizacje standaryzacyjne (w tym przypadku ITU i IETF),
2) Określenie **telefonia internetowa** oznacza systemy telefonii IP, które zasięgiem swoim ograniczają się do sieci Internet (np. Skype). Dodatkowo pod względem wykorzystanych

protokołów sygnalizacyjnych telefonia internetowa może być różna od VoIP (przykłady: własne, firmowe protokoły sygnalizacyjne dla Skype, czy aplikacji Yahoo Messenger).

3) Zazębianie się (cześć wspólna) telefonii internetowej z VoIP. Taką sytuację możemy zaobserwować np. w aplikacji MSN Messenger, która zasięgiem obejmuje sieć Internet i jednocześnie bazuje na SIP.
4) Terminem najogólniejszym spajającym dwa poprzednie terminy jest określenie **telefonii IP**.

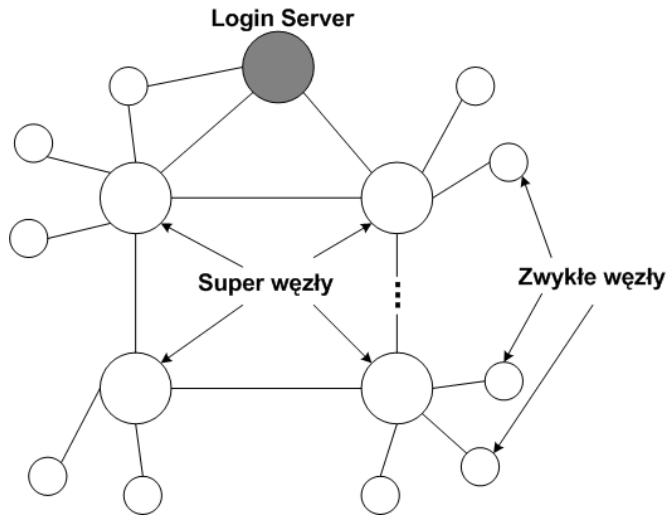
Dodatkowo klasyfikację, którą można zastosować przy podziale sieci telefonii IP, jest wykorzystywany model sieci. W tym przypadku sieci można podzielić na takie, które wykorzystują model klient-serwer (np. protokół H.323, SIP), lub P2P (Skype, P2P-SIP [13]). Wtedy w części wspólnej na rysunku 1 znajdować się będą wszelkie systemy hybrydowe np. taki jak zaproponowano w [13].

3. Wykorzystanie P2P w telefonii IP na przykładzie Skype

Skype bazuje na własnych, firmowych mechanizmach oraz rozwiązaniach i w małym stopniu wykorzystuje dostępne obecnie protokoły znane chociażby z innych systemów telefonii IP. Dlatego, też wysunąć stwierdzenie, że jest on przypisany do konkretnego, komercyjnego produktu (pewnego zestawu usług). W związku z tym nie może być brany pod uwagę przy opracowywaniu uniwersalnego standardu nowoczesnej sieci telefonii IP (np. poprzez brak możliwości współpracy z innymi systemami telefonii IP i przez to, że nie wykorzystuje zestandaryzowanych protokołów). Wiedzę/doświadczenia zebrane z analizy Skype można natomiast wykorzystać po to, aby ułatwić proces tworzenia uniwersalnego standardu VoIP bazującego na P2P.

3.1. Architektura sieci P2P w Skype

Jak wspomniano wcześniej przy tworzeniu Skype'a wykorzystano podobnie jak w systemie wymiany plików P2P – Kazaa - sieć nakładkową (overlay network). W sieci można wyróżnić dwa rodzaje węzłów: Zwykłe (Ordinary Nodes) i Super Węzły (Super Nodes). Dodatkowo sieć Skype cechuje się jedynym centralnym komponentem sieci, czyli tzw. Login Server. Przechowuje on pary: nazwa użytkownika – hasło, co gwarantuje unikalność nazwy użytkownika w obrębie sieci. Schemat prezentujący wszystkie wspomniane komponenty architektury Skype znajduje się na rysunku 2.



Rysunek 2. Architektura sieci P2P implementowana w Skype

Każdy węzeł staje się elementem sieci nakładkowej w momencie instalacji aplikacji w swoim systemie operacyjnym. Następnie w zależności od tego jakimi zasobami on dysponuje (parametry

brane pod uwagę to: CPU, ilość pamięci, szerokość pasma, czy adres sieciowy jest adresem publicznym) może stać się **SN - Super Węzłem** (w przypadku posiadania dużych zasobów i publicznego adresu IP) lub **ON - Zwykłym Węzłem** (w przypadku przeciwnym). Użytkownik nie ma wpływu na to czy maszyna, na której zainstalował Skype stanie się Super Węzłem, czy też nie – elekcja jest wyniesiona poza ingerencję użytkownika.

To, że dana maszyna stała się SN oznacza tyle, iż oprócz funkcji właściwych dla ON (np. możliwość wykonywania połączeń telefonicznych) taki węzeł będzie wykorzystany również do pomocy pewnej liczbie Zwykłych Węzłów, z którymi pozostaje w relacji. Nawiązując więc do architektury sieci VoIP np. opartej na protokole SIP, funkcje zcentralizowanych serwerów sieciowych SIP (proxy, redirect, registar) przejmuje rozproszona sieć Super Węzłów.

W sieci jak na rysunku 2 pewna liczba Zwykłych Węzłów jest obsługiwana przez jeden Super Węzeł, czyli pozostaje z nim w relacji tzw. sąsiedztwa. Również Super Węzły nawiązują relacje z sąsiednimi Super Węzłami tworząc sieć relacji. Zatem możemy wyróżnić dwie podstawowe warstwy (hierarchię) węzłów w sieci P2P Skype. Zwykłe Węzły komunikują się z siecią tylko poprzez właściwego mu SN (lub kilka SN), natomiast właściwy rdzeń sieci nakładkowej jest realizowany poprzez sieć połączonych Super Węzłów.

3.2. Charakterystyka podstawowych etapów działania Skype

Główne operacje jakie wykonuje Zwykły Węzeł można Skype można podzielić na kilka podstawowych etapów [2]:

- **Inicjalizacji** – podczas której nawiązywana jest relacja sąsiedztwa z właściwym SN (bądź ich większą liczbą). Podczas uczestniczenia w sieci P2P aplikacja zbiera informacje o dostępnych Super Węzłach. Lista taka (tzw. host cache) zawierająca nie więcej niż 200 takich rekordów (pary: adres IP i port) znajduje się w pliku XML o nazwie shared.xml, przechowywanej na maszynie, na której jest zainstalowany Skype. Jeśli takiej listy nie ma wtedy wykorzystywane są adresy sieciowe SN na stałe wpisane w plik wykonywalny Skype. W trakcie tej fazy na podstawie komunikacji z SN węzeł sprawdza, czy jest za NAT i firewallem oraz determinuje ich rodzaj (wykorzystanie protokołów podobnych do mechanizmów STUN [11] i TURN [12]). Informacja ta zostaje również zapisana we wspomnianym powyżej pliku.
- **Logowania** – jedynym centralnym komponentem architektury Skype jest Login Server, który odpowiada za uwierzytelnienie użytkowników, czyli umożliwienie dostępu do usługi oraz unikalność ich nazw w ramach całej sieci. Na tym serwerze trzymana jest również lista kontaktów użytkownika. Użytkownik posiada również jej lokalną kopię w pliku XML: config.xml.
- **Wyszukiwanie użytkowników** bazuje na własnym rozwiązaniu nazwanym Global Index, które jak się przypuszcza działa na podobnej zasadzie jak Chord [17]. Jest to rozproszone wyszukiwanie i gwarantuje odnalezienie użytkownika, jeśli logował się on do sieci w ciągu ostatnich 72 godzin.
- **Nawiązywanie połączenia** w zależności od umiejscowienia użytkowników korzysta bądź nie z pomocy SN przy transmisji zza NAT i firewalli. W najgorszym przypadku (oboje użytkownicy za NAT i firewall) strumień głosu jest przesyłany z wykorzystaniem protokołu TCP (w większości systemów telefonii IP do transmisji głosu wykorzystywany jest jedynie bezpołączeniowy protokół UDP). Obciążenie ruchem sieci użytkowników w Skype jest większe niż w dotychczasowych systemach, ponieważ część rozmów prowadzona jest za darmo, część po niskich kosztach. Z badań wynika, że średnia długość rozmowy telefonicznej w Skype wynosi ok. 13 minut [1], przy ok. 3 minutach w telefonii tradycyjnej,
- **Transfer strumieni mediów** – odbywa się z lub bez pośrednictwa Super Węzłów i jak wspomniano odbywa się bądź z wykorzystaniem protokołu UDP, bądź w trudnych przypadkach TCP w warstwie transportowej. Dodatkowo przesyłany głos charakteryzuje

się wykorzystaniem kodeków firmy Global IP Sound [18, 19, 20]. Wielkość takiego pakietu waha się w granicach 40-120 bajtów, szybkość wymiany to ok. 33 pakiety/sek, a zajętość pasma to 3-16 KB/s,

- **Podtrzymywania relacji** z właściwym Super Węzłem (bądź kilkoma) – co określony interwał czasu relacja z SN jest odnawiana, w przypadku braku komunikacji we wskazanym okresie czasu użytkownik uznawany jest za niedostępnego.

3.3. Cechy, obciążenie i kontrola Super Węzłów

Jak widać na podstawie informacji zawartych w poprzednich punktach jakość działania sieci Skype zależy od ilości i wydajności Super Węzłów. W [1] poprzez prawie pięć miesięcy gromadzenia ruchu Skype udało się wykryć ok. 250 tys. takich węzłów (ok. 30-40% jest zwykle jednocześnie aktywnych). W [2] natomiast wykazano, że znaczny procent SN stanowią serwery należące do uczelni rozrzuconych po całym świecie. Wskazuje to na fenomen rozwiązania ponieważ praktycznie przy braku infrastruktury telekomunikacyjnej/sieciowej udało się zaangażować wielką liczbę urządzeń, których właścicielem nie jest Skype. Można również wysunąć hipotezę, iż jeśli udało by się namówić znaczną liczbę właścicieli super węzłów do odinstalowania tej aplikacji (bądź zastosowania techniki „free riding", czyli celowego ograniczenia swoich parametrów dostępnych dla Skype po to, by węzeł nie został SN) to przy 50 milionach zarejestrowanych użytkowników (szacuje się jednocześnie może być aktywnych ok. 4 milionów użytkowników) mogło by to doprowadzić do paraliżu tego systemu w dość krótkim czasie.

Dodatkowo liczba SN w sieci podlega ciągłej zmianie. W [1] wykazano zbieżność liczby aktywnych użytkowników (zarówno ON jak i SN) z dniami tygodnia oraz porami dnia. Największa ilość użytkowników jest aktywna od poniedziałku do piątku w godzinach pracy. Dodatkowo liczba Zwykłych Węzłów waha się w ciągu dnia o ok. 40% o tyle liczba i dostępność Super Węzłów jest stabilniejsza i wykazuje zmiany rzędu 25% dziennie. Ma to logiczne wytłumaczenie, ponieważ jak wspomniano często SN to fizycznie serwery, na których zainstalowano Skype.

Obciążenie, które jest generowane w Super Węźle nie może być zbyt duże, bo to mogło by zniechęcić potencjalnego użytkownika do instalacji oprogramowania. I w rzeczywistości SN Skype zużywa średnio ok. 400 b/s, w znacznej części przeznacza zajęte pasmo na przesyłanie wiadomości sygnalizacyjnych, tylko w ok. 10% czasu będąc pośrednikiem w wymianie pakietów z głosem (wtedy zużycie pasma wzrasta średnio do 60kb/s).

4. Aspekty bezpieczeństwa Skype

W przypadku systemu telefonii IP wykorzystującej model sieci P2P bezpieczeństwo musi być zagwarantowane podobnie, jak w przypadku systemów VoIP, dla obu faz nawiązywania połączenia. Wyróżniamy dwie takie fazy:

- **sygnalizacyjną** - zabezpieczanie w tym wypadku odnosi się do wiadomości wykorzystanego protokołu sygnalizacyjnego
- **wymiany strumieni głosu**, czyli rozmowy – tutaj zabezpieczaniu podlega sama konwersacja.

Zwykle użytkownik końcowy zainteresowany jest przede wszystkim poufnością swojej rozmowy i nie zwraca uwagi na bezpieczeństwo wiadomości sygnalizacyjnych, co przy równej beztrosce implementujących może doprowadzić do wielu potencjalnych nadużyć [24]. Poniżej w punktach przedstawiono wybrane aspekty bezpieczeństwa Skype oraz ich analizę, co posłuży nam w dalszej części pracy do określenia kryterium bezpieczeństwa dla systemów telefonii IP opartej na modelu sieci P2P.

4.1. Tajemnica istotnym elementem bezpieczeństwa Skype?

Od początku istnienia Skype budzi kontrowersje, jeśli chodzi o poziom zapewnianego bezpieczeństwa, zarówno w odniesieniu do Zwykłych jak i Super Węzłów. Składają się na tą pewną

nieufność do tego oprogramowania dwa aspekty: wykorzystanie części własnych mechanizmów zarówno do komunikacji, jak i tych gwarantujących bezpieczeństwo oraz to, że do dnia dzisiejszego nie zostały udostępnione kody źródłowe programu, ani sposoby ich działania (algorytmy). Podejście open-source, czyli darmowe udostępnienie źródeł pozawala każdemu użytkownikowi, jeśli posiada odpowiednie umiejętności na osobistą weryfikację jakości i niezawodności rozwiązania. Niestety to, że Skype utrzymuje w tajemnicy sposoby zabezpieczania ruchu przesyłanego w sieci w żaden sposób nie zapewnia niezawodności zastosowanych mechanizmów, ani tego, że nie uda się znaleźć w nich luk [23]. Takie zabiegi spowolnią jedynie proces dojścia do prawdy. Historia teleinformatyki pokazuje, że czasami całe bezpieczeństwo systemu tkwi jedynie w jego tajności. Jako przykład może posłużyć sprawa szyfrów A5/1 i A5/2, używanych do kodowania transmisji głosu pomiędzy telefonem GSM a stacją bazową. Operatorzy GSM trzymali te algorytmy w sekrecie, gdy w 1998 roku grupa Smartcard Developer Association zastosowała inżynierię wsteczną (reverse engineering) i opublikowała ich kody źródłowe. W wyniku przeprowadzonej analizy tych algorytmów okazało się, że posiadają wiele słabych punktów, pozwalających m.in. na klonowanie kart SIM. W tym czasie z telefonii GSM w Europie korzystało ponad 100 milionów użytkowników. Można odnaleźć w podanej historii kilka analogii do obecnej sytuacji Skype. Jedyne informacje o bezpieczeństwie Skype pochodzą z zapewnień producenta [8], raportu kryptografa Toma Bergsona [3], którego Skype zatrudnił w celu oceny bezpieczeństwa oraz najistotniejsze i najnowsze informacje uzyskane właśnie poprzez inżynierię wsteczną [5]. Strzępy informacji pochodzące z tych źródeł łącza się jednak powoli w jedną całość wraz z upływem czasu. Twórcy Skype'a nie chcąc podzielić losu operatorów wspomnianych GSM dołożyli wszelkich starań, aby maksymalnie utrudnić możliwość odkrycia szczegółów implementacyjnych poprzez disasemblację kodu. Zastosowano więc m.in. kilku poziomowe szyfrowanie wewnątrz kodu, blokowanie programów do debbugingu (np. SoftIce), liczne sprawdzenia integralności (ponad 300) oraz celową nadmiarowość i brak porządku w kodzie.

4.2. Analiza mechanizmów zabezpieczeń sygnalizacji i przesyłanej rozmowy

Coraz więcej wiadomo również o mechanizmach zabezpieczeń w odniesieniu do wiadomości protokołu sygnalizacyjnego i pakietów z głosem. Szyfrowanie pakietów składa się z dwóch faz:

- Fazy szyfrowania pakietów 256-bitowym algorytmem AES (Rijndael). Klucz wykorzystywany do tego celu jest wymieniany między węzłami Skype przy pomocy algorytmu RSA. Podkreślmy, iż ten etap dotyczy **jedynie** zabezpieczania pakietów zawierających głos i ma na celu zapewnienie poufności rozmowy.
- Faza szyfrowania bazująca na wykorzystaniu algorytmu RC4. Ten etap jest właściwy wszystkim pakietom Skype, więc zarówno wiadomościom sygnalizacyjnym jak i ponownie pakietom z głosem. Etap ten ma na celu tylko nadanie losowości zawartości pakietu, co pozwala na ukrycie prawdziwej treści pakietu przed firewallami i systemami monitorującymi IDS/IPS (Intrusion Detection/Prevention System). Sam sposób generowania 128-bitowego klucza bazujący na adresach źródłowym i docelowym oraz identyfikatorze pakietu jest słaby, a sposób jego pozyskania przedstawiono w [5], ale jak wspomniano powyżej wszystko wskazuje na to, iż zabezpieczenie pakietu jest tutaj celem drugorzędnym względem randomizacji zawartości pakietu.

Jakie zatem wnioski można wyciągnąć na podstawie tej fragmentarycznej wiedzy? Pierwsza informacja jest taka, że o ile o bezpieczeństwo rozmowy nie ma się co obawiać, o tyle protokół sygnalizacyjny nie jest wystarczająco zabezpieczany (bądź zabezpieczenia te nie zostały jeszcze wystarczająco poznane).

4.3. Problem „zaradności" Skype

Oprócz problemów nakreślonych w poprzednich punktach twórcy Skype chcąc zapewnić użytkownikom możliwość nawiązywania połączeń w każdych „warunkach sieciowych" (maszyna

użytkownika może mieć adres publiczny, być za NAT i/lub za firewall) zastosowali znane chociażby z Kaazy, a w tym przypadku dodatkowo rozwinięte techniki ich pokonywania. Po rozpoczęciu komunikacji Zwykły Węzeł inicjuje komunikację, która ma na celu detekcję rodzaju NAT i firewall. W ten właśnie sposób można w przypadku nawiązywania połączenia wybrać odpowiedni scenariusz obsługi przychodzących/wychodzących połączeń (z pośrednictwem Super Węzła, bądź bez). Poza tym Skype dodatkowo stosuje kilka innych udowodnionych technik omijania firewalli. Tak jak wiele aplikacji P2P, korzysta ze dynamicznie zmienianych portów UDP, a jeśli taki sposób nie przynosi sukcesu to próbuje łączyć się na port 80/TCP, który zazwyczaj jest odblokowany. Na tym właśnie porcie (wykorzystywanym zwykle przez protokół HTTP) oraz dodatkowo na 443 (HTTPS) Skype nasłuchuje również komunikacji z zewnątrz umożliwiając w ten sposób obejście niewygodnych mu urządzeń. Poprzez wspomnianą randomizację zawartości pakietu z wykorzystaniem szyfru RC4 również systemy monitorujące IDS/IPS są bezradne. Co gorsze będąc już „wewnątrz" sieci, jeśli zostanie on wypuszczony tylko przez serwer proxy, Skype próbuje pozyskać hasło do tego serwera z ustawień przeglądarki Internet Explorer. Opisany sposób zachowań nie może budzić zaufania, szczególnie jeśli chodzi o jego wykorzystanie do np. sieci korporacyjnych.

W związku z tym nietrudno jest sobie wyobrazić scenariusz, w którym specjalnie (np. w celach komercyjnych: spyware, malware) lub z powodów luk bezpieczeństwa w tym oprogramowaniu do sieci stworzonej z wszystkich węzłów posiadających zainstalowany Skype zostanie „podczepiony" odpowiednio napisany robak. W [5] francuscy badacze zademonstrowali w jaki sposób węzeł Skype można łatwo zmienić w zdalny skaner sieciowy właśnie poprzez wykorzystanie „zwykłych" funkcji Skype, które umożliwiają poprawne nawiązywanie połączeń telefonii IP (pokonywanie firewalli, NAT, możliwość zdalnego wydawania komend). Stąd biorąc pod uwagę wymienione zarzuty bardzo często trudno, bądź wręcz niemożliwością jest, pogodzenie korzystania ze Skype z polityką bezpieczeństwa firm, czy instytucji. Przykładami mogą być CERN oraz University of Cambridge [21, 22], które zabroniły instalacji tego oprogramowania na swoich zasobach sieciowych.

4.4. Rola i ruch przechodzący przez Super Węzłów w sieci P2P

Nieufność budzi również utajnianie informacji o tym jaki dokładnie ruch i czy tylko w celu pomocy zwykłym węzłom przechodzi przez Super Węzeł. Podkreślmy Super Węzłem ma szansę stać się potencjalnie każdy węzeł w sieci spełniający określone warunki. Dodatkowo, jak wspomniano na początku, nie jest to decyzją użytkownika, czy dany węzeł zostanie włączony do sieci Skype jako Zwykły, czy jako Super Węzeł. Istnieją więc obawy, czy same Super Węzły nie są wykorzystywane również w innych celach (np. pseudokomercyjnych).

Istnieje również drugi aspekt sprawy. Chodzi o sytuację w, której użytkownik chce celowo wykorzystać fakt tego, że jego węzeł pośredniczy i pomaga w transmisji pomiędzy użytkownikami. W takim przypadku może on blokować wiadomości inicjujące połączenie, zwracać użytkownikowi nieprawdziwe informacje (np. o dostępności osób na liście kontaktów), bądź blokować strumienie pakietów z głosem. Nie pomoże w takim przypadku fakt, iż rozmowa jest zaszyfrowana. Nawet w przypadku działania pasywnego sam fakt odbycia rozmowy i tego, że wiemy, gdzie/do kogo została ona skierowana, nawet bez podsłuchania jej zawartości stanowi cenną informację.

Dodatkowo, na koniec analizy aspektów bezpieczeństwa, w stosunku w Skype można odnaleźć również pewne inne „praktyczne" braki bezpieczeństwa. Chodzi tu przede wszystkim trzymanie listy kontaktów w postaci nieszyfrowanej na dysku lokalnym maszyny, na którym został zainstalowany (plik w lokalizacji <dysk>\Documents and Settings\<użytkownik>\Application Data\Skype\<użytkownik Skype>\config.xml) oraz listy super węzłów wraz z adresami IP i portami (plik: w lokalizacji <dysk>\Documents and Settings\<użytkownik>\Application Data\Skype\shared.xml). Przejęcie choć takich informacji przez osobę postronną wskazuje na brak wystarczającego poziomu zapewniania prywatności użytkownika oraz dodatkowo odsłania

strukturę sieci - co można wykorzystać np. do przeprowadzenia ataków DoS (Denial of Service) na Super Węzły (maksymalnie 200 maszyn), co może spowodować przynajmniej u części użytkowników problemy z nawiązywaniem połączeń.

5. Usługi bezpieczeństwa w sieci opartej na P2P

W punkcie 4 przedstawiono wybrane aspekty oraz analizę bezpieczeństwa dotyczące jedynego działającego z sukcesem komercyjnym systemu telefonii IP wykorzystującego model sieci P2P, czyli Skype. Część z przedstawionych problemów dotyczyła jedynie tego konkretnego produktu. Miało to na celu, w świetle ostatnich badań, stonowanie informacji podawanych przez producentów, a bezkrytycznie przyjmowane, czy też bagatelizowane przez część użytkowników, czy inne środowiska np. media. W trakcie analizy poruszono jednak pewną liczbę problemów i zagrożeń, które można zidentyfikować w dowolnej sieci P2P oferującej usługę telefonii IP. Obecnie w środowisku naukowym trwają prace nad stworzeniem standardów sieci VoIP P2P (np. P2P-SIP w [13]), która była by w stanie zapewnić architekturę nowoczesnej sieci telekomunikacyjnej na skalę globalną. Tym bardziej istotne jest w tym wypadku zapewnienie odpowiedniego poziomu bezpieczeństwa.

Biorąc to pod uwagę oraz bazując na kryterium podanym w [25] najważniejszymi usługami bezpieczeństwa dla tej usługi czasu rzeczywistego (podobnie jak dla VoIP) są:

Poufność – dająca ochronę przed atakami pasywnymi oraz zabezpieczająca ruch (zarówno sygnalizacyjny jak i użytkownika), wymieniany pomiędzy komunikującymi się jednostkami, przed ich nieuprawnionym uzyskaniem przez strony do tego nieupoważnione.

Uwierzytelnienie (zawierające usługę integralności) – gwarantujące ochronę przed atakami aktywnymi oraz kontrolę tożsamości stron i wymienianego ruchu.

Zatem w przypadku sieci telefonii IP opartej na P2P podane kryterium bezpieczeństwa jest również prawdziwe. Następuje jednak pewna zamiana akcentu. W sieciach VoIP elementy centralne – serwery sieciowe użytkownik uznawał (raczej) za elementy zaufane, jako część infrastruktury dostarczyciela usługi. W sieciach wykorzystujących model P2P wszystkie węzły sieci oprócz swojego można uznać de facto jako obce, względem których należy zachować ostrożność. Nie ma tu praktycznie zaufanych elementów infrastruktury znanej z klasycznych sieci VoIP (oprócz np. Login Server w Skype), stąd dodatkowo potrzeba rozszerzenia kryterium o usługę **prywatności**, po to, aby kontrolować ilość informacji udostępnianych innym węzłom w sieci.

Dla każdej z wymienionych usług bezpieczeństwa konieczne jest opracowanie mechanizmów zabezpieczeń podobnie, jak to ma miejsce w przypadku VoIP (zarówno dla protokołu sygnalizacyjnego, na którym jest oparta, jak i dla przesyłanego głosu). Niezbędne jest jednak dostosowanie tych mechanizmów do specyfiki sieci P2P.

6. Podsumowanie

W artykule przedstawiono cechy i funkcje systemu telefonii IP opartej na modelu sieci peer-to-peer na przykładzie komercyjnego systemu Skype. W oparciu o najnowsze opublikowane badania wskazano w nim wiele problemów i znaków zapytania dotyczących oferowanego bezpieczeństwa szczególnie w odniesieniu do protokołu sygnalizacyjnego. Część ze wskazanych problemów wynika z samej specyfiki i funkcji oferowanych przez sieci P2P. Analiza bezpieczeństwa Skype posłużyła następnie do stworzenia ogólnego kryterium oceny bezpieczeństwa systemów telefonii P2P, w którym wskazano na trzy najważniejsze usługi bezpieczeństwa: uwierzytelnienie, poufność oraz prywatność.

Komercyjny sukces Skype i akceptacja użytkowników wytycza nową drogę ewolucji systemów telefonii IP. Wykorzystanie modelu P2P jest odpowiedzią na największą bolączkę obecnych systemów tzn. problemów z przechodzeniem przez firewalle i NAT. Dodatkowo Skype gwarantuje dobrą jakość głosu, czego również nie można było powiedzieć o jego tradycyjnych poprzednikach w sieciach na dużą skalę (VoIP). Jeśli więc opracuje się dla tego rodzaju sieci poprawną

architekturę bezpieczeństwa, wtedy uniwersalny standard telefonii IP (ale również innych usług) oparty na sieciach nakładkowych P2P stanie się faktem. Taka sytuacja może stać się fundamentem w wyznaczaniu nowej architektury nowoczesnych sieci teleinformatycznych.

Literatura

[1] Saikat Guha, Neil Daswani, Ravi Jain, An Experimental Study of the Skype Peer-to-Peer VoIP System, Sixth International Workshop on Peer-to-Peer Systems (IPTPS), luty 2006

[2] Baset, S. A., Schulzrinne, H. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. In Proceedings of the INFOCOM '06 (Barcelona, Spain, Kwiecień 2006)

[3] Tom Berson Anagram Laboratories, Skype Security Evaluation, 18 październik 2005 http://www.skype.com/security/files/ 2005-031 security evaluation.pdf

[4] Simson L. Garfinkel, VoIP and Skype Security, 26 stycznia 2006 http://www.simson.net/ref/2005/OSI_Skype6.pdf

[5] Biondi, P., Desclaux, F., Silver Needle in the Skype, Konferencja Black Hat Europe. Marzec 2006. http://www.secdev.org/conf/skype_BHEU06.handout.pdf

[6] Debbie Cheng, Skype versus server-based VoIP**,** IS 250 Computer Based Communications Networks & Systems, 2006 http://www.sims.berkeley.edu:8000/academics/courses/is250/s06/protected/students/dcheng/

[7] Peer-to-Peer IP Telephony, folk.uio.no/paalee/publications/Skype-for-telektronikk-2005.pdf

[8] Skype. URL http://www.skype.com/

[9] Kazaa. URL. http://www.kazaa.com/

[10] 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 (2004).

[11] Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, STUN—Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC 3489, Marzec 2003

[12] J. Rosenberg , R. Mahy , C. Huitema, Traversal Using Relay NAT (TURN), http://www.ietf.org/internet-drafts/draft-rosenberg-midcom-turn-07.txt

[13] K. Singh, H. Schulzrinne, Peer-to-Peer Internet Telephony using Skype, Columbia Computer Science Technical Report, 2004 http://www1.cs.columbia.edu/~library/2004.html

[14] H.323 - Packet-based multimedia communications systems, ITU-T

[15] M. Handley, H. Schulzrinne, J. Rosenberg, SIP: Session Initiation Protocol, IETF RFC 3261, czerwiec 2002

[16] F. Cuervo, N. Greene, A. Rayhan, C. Huitema, B. Rosen, J. Segers, Megaco Protocol Version 1.0, IETF RFC 3015, listopad 2000

[17] Ion Stoica, Robert Morris, David Karger, Frans Kaashoek, Hari Balakrishnan, Chord: A scalable peer-to-peer lookup service for internet applications, *SIGCOMM*, San Diego, CA, USA, sierpień 2001.

[18] iLBC codec - http://www.globalipsound.com/datasheets/iLBC.pdf

[19] iSAC codec - http://www.globalipsound.com/datasheets/iSAC.pdf

[20] iPCM codec - http://www.globalipsound.com/datasheets/iPCM-wb.pdf

[21] CERN IT Department http://security.web.cern.ch/security/skype/

[22] University of Cambridge http://connect.educause.edu/blog/catherine/university_of_cambridge_department_bans_skype_citing_security_concerns/1400

[23] Skype Security Bulletins http://www.skype.com/security/bulletins.html

[24] VOIPSA. VoIP Security and Privacy Threat Taxonomy www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

[25] Wojciech Mazurczyk, Bezpieczeństwo SIP jako protokołu sygnalizacyjnego VoIP, XIX Krajowe Sympozjum Telekomunikacji KST 2003, Bydgoszcz, wrzesień 2003