dr inż. Zbigniew Piotrowski
Wojskowa Akademia Techniczna
zbigniew.piotrowski@wat.edu.pl

dr inż. Krzysztof Różanowski
Warszawska Wyższa Szkoła Informatyki
krozan@wwsi.edu.pl

prof. dr hab. inż. Piotr Gajewski
Wojskowa Akademia Techniczna
piotrgajewski@wat.edu.pl

Bezpieczeństwo połączeń w telefonii PSTN

Safety calls PSTN telephony

Streszczenie

Odpowiednio wczesne zabezpieczenie krytycznych systemów infrastruktury na potencjalnie groźne ataki typu voice spoofing jest warunkowane opracowaniem skutecznych metod i istnieniem dedykowanych rozwiązań technicznych. Metody ataków i obrony przed impersonizacją skupiają się zasadniczo na dwóch obszarach: zmianie głosu abonenta na inny głos (wirtualny lub innej osoby) oraz nieautoryzowanej edycji komunikatów głosowych. W nowych generacjach ataków na łącza telefoniczne, w których następuje zmiana głosu mówcy w czasie rzeczywistym lub odtwarzany jest uprzednio spreparowany komunikat, stosuje się metody obrony polegające na m.in. weryfikacji wspólnie posiadanej wiedzy lub posiadanego klucza.

Słowa kluczowe: voice spoofing, telefonia, impersonalizacja, bezpieczeństwo połączeń, analiza głosu

Abstract

In order to protect critical infrastructure systems early enough against potentially dangerous attacks called spoofing voice it is required to develop effective methods and implement dedicated solutions. Methods of attack and defence against impersonalisation focus basically on two areas: changing of original voice to the voice of other subscriber (virtual simulation or voice of different person) or unauthorized editing of voice messages. The new generations of attacks on telephone lines, in which the speaker's voice is being changed in real time or prepared message is being played, require other methods of defence involving verification of common knowledge or of the authorisation key.

Keywords: voice spoofing, telephony, impersonalisation, security calls, voice analysis

WSTĘP

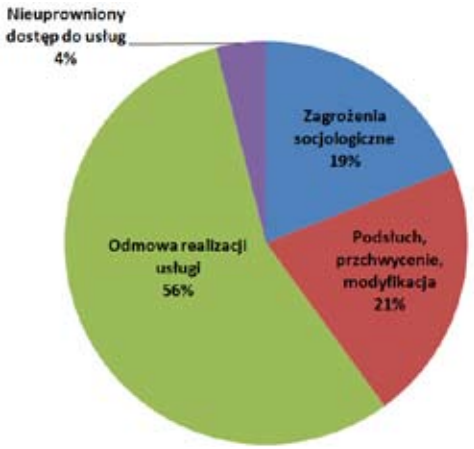
Aktualnie coraz więcej połączeń telefonicznych wykonywanych jest w technologii VoIP. Terminem VoIP (ang. Voice over Internet Protocol) określa się protokół umożliwiający zrealizowanie połączenia głosowego z wykorzystaniem sieci Internet. Jednak wraz z pojawianiem się nowych technologii pojawiają się nowe zagrożenia z nią związane. Korzystając z faktu, iż możliwe są połączenia pomiędzy telefonią internetową, a użytkownikami klasycznej telefonii PSTN, zostały opisane przypadki podszywania się pod dowolny numer telefonu. Tego typu działanie określane jest terminem caller-ID-spoofing. Najczęściej w tym celu wykorzystuje się programową centralę telefoniczną umożliwiającą wykonywanie połączeń pomiędzy użytkownikami telefonii internetowej, a klasycznej telefonii. Najpopularniejszą tego typu centralą jest darmowe oprogramowanie Asterisk działające pod kontrolą systemu operacyjnego z rodziny Linux. Usługę zmiany numeru identyfikującego osoby dzwoniącejm, tak zwany CallerID, można zrealizować w oparciu o tani sprzęt komputerowy. Należy dysponować komputerem klasy PC z minimum procesorem PIII 500 MHz, 128MB pamięci RAM oraz około 1GB miejsca na dysku twardym. Na dedykowanej maszynie należy zainstalować oprogramowanie Asterisk. Można w tym

celu posłużyć się gotowymi dystrybucjami systemu Linux wyposażonymi domyślnie w program Asterisk. Najpopularniejszą tego typu dystrybucją jest FreePBX. Okazuje się, iż podszycie się pod dowolny numer telefonu nie jest zadaniem trudnym i nie wymaga dużych nakładów finansowych. Jednak istnieją jeszcze prostsze metody podszycia się pod cudzy numer telefonu. Wystarczy w wyszukiwarce internetowej wpisać hasło „caller ID spoofing", aby otrzymać adresy komercyjnych serwisów oferujących taką usługę odpłatnie [1-4]. Większość z wymienionych serwisów działa jedynie na terytorium Stanów Zjednoczonych oraz w innych krajach, w których prawo nie w pełni reguluje tego typu usługi. Usługa Caller ID spoofing może być również wykorzystywana do zmiany numeru nadawcy wiadomości SMS w telefonii GSM. W tym celu również można skorzystać z jednego z wielu komercyjnych serwisów internetowych oferujących tego typu usługę.

STATYSTYKA ZAGROŻEŃ W SIECIACH VOIP

Ze względu na niski poziom złożoności otwartych protokołów sygnalizacyjnych jak np. H.323 oraz SIP, które działają w oparciu o pakiety zawierające informacje kodowane w formacie ASCII, w relatywnie prosty sposób łatwo jest dokonać manipulacji. Zagrożenia związane z telefonią internetową klasyfikuje się według taksonomii ustanowionej przez organizację VoIPSA (ang. Voice over IP Security Alliance) [5]. Zagrożenia dotyczące systemów jak i użytkowników danego systemu mozna podzielić na następujące kategorie:

- Zagrożenia socjologiczne – są to zagrożenia związane z czynnikiem ludzkim, skierowane bezpośrednio przeciwko użytkownikom systemu. Najczęściej są podstawą do przestępstw dokonywanych metodą socjotechniczną takich jak np. phishing. Do grupy tej zalicza się również marketing telefoniczny inaczej zwany SPIT (ang. Spam over Internet Telephony), czyli spam przez telefon;
- Zagrożenia podsłuchu, przechwycenia i modyfikacji wiadomości – zagrożenia te wynikają z implementacji systemu VoIP na technologii IP która początkowo nie przewidywała szyfrowania pakietów. Większość domyślnych konfiguracji systemów VoIP nie przewiduje szyfrowania. Jeśli brak jest szyfrowania to z łatwością można dokonać ataków;
- Odmowa realizacji usług – tego typu zagrożenie może wynikać z dwóch przyczyn. Poprzez wygenerowanie tak dużej liczby zgłoszeń, iż serwer nie będzie w stanie ich obsłużyć, a w konsekwencji przestanie przyjmować kolejne zgłoszenia. Drugą przyczyną może być fizyczne uszkodzenie łączy dostępowych, lub sieci energetycznej, lub każdy inny czynnik fizyczny powodujący uszkodzenie strategicznych węzłów sieci;
- Nieuprawniony dostęp do usług - są to zagrożenia związane z nieuprawnionym dostępem do usług. Najczęściej polegają na oszukaniu systemu bilingowego lub kradzieży impulsów telefonicznych;
- Zagrożenia związane z fizycznym dostępem do sieci - są to wszelkie zagrożenia związane z nieprawidłowym zabezpieczeniem infrastruktury sieciowej.
- Przerwanie realizacji usług - są to zagrożenia spowodowane przez czynniki niezależne od implementacji oraz czynnika ludzkiego. Na przykład utrata zasilania na skutek niekorzystnych warunków atmosferycznych przy braku zapasowego zasilania.



Rys.1. Procentowy udział poszczególnych zagrożeń.

Na Rys.1. przedstawiono procentowy udział poszczególnych zagrożeń spośród 219 incydentów zarejestrowanych w bazie CVE przeanalizowanych oraz przedstawionych w [6]. Baza danych CVE (ang. Common Vulnerabilities and Exposures) [7] zawiera informacje na temat wszelkich zgłoszonych błędów lub luk bezpieczeństwa w systemach teleinformatycznych. Baza ta jest niezmiernie pomocna podczas implementacji oraz utrzymaniu poprawnego działania systemu. Wszelkie nowe wpisy pojawiające się w tej bazie powinny być analizowane przez administratora systemu w celu zapobieżeniu możliwości wykorzystania opublikowanej luki. Równocześnie baza ta jest pierwotnym miejscem zasięgania informacji dla osób pragnących dokonać ataku. Tak więc niezmiernie istotnym jest aby administrator dotarł do informacji na temat luki dotyczącej jego systemu przed atakującym, aby na czas zabezpieczyć system.

Incydenty z bazy CVE można podzielić, opierając się na ogólnej klasyfikacji zagrożeń dotyczących systemów telekomunikacyjnych. Według tej klasyfikacji zagrożenia oddzialywują na poufność, integralność oraz dostępność:

- Poufność zapewnia, iż osoby postronne nie mają możliwości wglądu do informacji wymienianych pomiędzy dwoma lub większą liczbą korespondentów. Do tego celu najczęściej używa się funkcji szyfrujących;
- Integralność daje pewność, iż otrzymana wiadomość nie została zmodyfikowana w trakcie transmisji. Do tego celu najczęściej wykorzystuje się funkcje skrótu;
- Dostępność umożliwia realizację usługi na którą zgłoszono zapotrzebowanie. Odmowa realizacji usługi z różnych przyczyn skutkuje niedostępnością danej usługi.

Należy pamiętać, iż wszelkie zagrożenia mają swoje przyczyny, dlatego też aby obiektywnie ocenić bezpieczeństwo danej technologii należy wykryte zagrożenia sklasyfikować pod względem ich przyczyn. Najczęstszą przyczyną luki w systemie jest nieprawidłowa implementacja lub konfiguracja. Zagrożenia związane z protokołem są niezmiernie rzadkie. Dlatego też implementacja jak i konfiguracja danej usługi wymaga od administratorów systemu dużej wiedzy oraz staranności.

IMPERSONACJA GŁOSU ORAZ NIEAUTORYZOWANA EDYCJA KOMUNIKATÓW GŁOSOWYCH W PUBLICZNEJ SIECI TELEFONII KOMUTOWANEJ

Zagrożenia w telefonii komutowanej PSTN (ang. Public Switched Telephone Network) polegają głównie na podsłuchiwaniu, modyfikowaniu, powtarzaniu i zakłócaniu przekazywanych wiadomości. Z biegiem czasu wypracowano i wciąż wypracowuje się nowe mechanizmy bezpieczeństwa mające na celu zapobiegać powyższym zagrożeniom. Publiczna, komutowana sieć telefoniczna PSTN jest najstarszym i w związku z tym najbardziej rozwiniętym systemem przekazu wiadomości. Charakterystycznym urządzeniem końcowym tej sieci jest klasyczny (stacjonarny) aparat telefoniczny. Komunikacja odbywa się za pomocą głosu – środka najwygodniejszej komunikacji dla ludzi, który jednocześnie pozwala na rozpoznanie nastroju, emocji itp. współrozmówcy znajdującego się na drugim końcu łącza telefonicznego. Do podstawowych zagrożeń w sieci telefonicznej bazującej na nieszyfrowanych łączach można zaliczyć [8]:

- Podsłuch – dostępność linii telefonicznych, łatwość w realizacji podsłuchu
- Atak z wykorzystaniem emisji ujawniającej telefonu i łącza – zaawansowana metoda podsłuchu
- Pozbawienie usługi – celowe działanie mające na celu pozbawienie użytkownika podstawowej usługi jaka jest transmisja sygnału mowy
- Podszywanie się pod tożsamość głosową abonenta

W zakresie łączności telefonicznej jednym z podstawowych zagrożeń (obok podsłuchu) jest podszywanie się pod tożsamość abonenta (ang. masquerade). Na ataki podszywania się pod tożsamość abonenta narażeni są przede wszystkim tacy abonenci telefonicznej sieci PSTN jak np: przedstawiciele organów rządowych, przedstawiciele organizacji porządku publicznego (np. policja, organizacje paramilitarne), przedstawiciele wysokiego szczebla handlu i bankowości, wyspecjalizowane biura i agencje rządowe.

Opisane poniżej portale internetowe i usługi telefoniczne pomimo, iż w zamyśle ich twórców mają służyć celom rozrywkowym i nie są dedykowane osobom zamierzającym dokonywać ataków na abonentów sieci telefonicznej PSTN to jednak znakomicie umożliwiają one realizację takich czynności.

Portal „Wykręćnumer"

Do niedawna w Internecie funkcjonował portal o nazwie „WYKRECNUMER", adres: *www.wykrecnumer.pl* umożliwiający wykonanie połączenia telefonicznego na dowolny wybrany numer w sieci VoIP, GSM lub PSTN oraz wybór dowolnego numeru telefonicznego jaki wyświetlałby się na wyświetlaczu abonenta wywoływanego (wybieranego). Serwis, który zarejestrowany był na fikcyjną (nie figurowała w rejestrze firm telekomunikacyjnych) firmę z pewnością swą usługą otwierał drogę do wielu nadużyć. Umożliwiał bowiem podszywanie się pod dowolny numer telefoniczny, w tym pod numery alarmowe. Sprawa stała się na tyle poważna, iż zainteresowała się nią Helsińska Fundacja Praw Człowieka [9]. Po zażądaniu wyjaśnień przez tą organizację problemem serwisu „WYKRECNUMER" zajął się w kraju Urząd Komunikacji Elektronicznej (UKE) oraz Agencja Bezpieczeństwa Wewnętrznego (ABW), która jednoznacznie stwierdziła, że działalność portalu stanowi zagrożenie dla bezpieczeństwa Państwa, dając nieograniczone możliwości popełniania nadużyć gospodarczych i obyczajowych. Dodatkowo, bilingi połączeń praktycznie tracą znaczenie dowodowe, gdyż figurują na nich podmienione numery abonentów nawiązujących połączenie (wspomniany CallerID spoofing). Pomimo, iż wiele tego typu portali funkcjonuje m.in. w USA i Wielkiej Brytanii [1-4], UKE oraz ABW podjęły decyzję o skierowaniu zawiadomienia do prokuratury o możliwości popełnienia przestępstwa przez firmę, właściciela serwisu „WYKRECNUMER". Twórcy portalu wykorzystali lukę istniejącą w polskim prawie telekomunikacyjnym, które mówi, iż numer abonenta na całej drodze połączeniowej musi być taki sam lecz nie precyzuje, że musi on być prawdziwy.

Usługa „Żartofon"

Jest to usługa funkcjonująca w sieci Plus, przez operatora określana jest jako Portal Głosowo-Rozrywkowy [10]. Jej idea polega udostępnieniu abonentowi jednego z trzech dostępnych scenariuszy rozmowy. Po połączeniu się ze specjalnym numerem *7177 abonent może wybrać jedną z trzech opcji:

- Zmiana swojego głosu - serwis umożliwia dokonanie połączenia z wybraną osobą i rozmowę zmienionym głosem. Abonent ma do wyboru trzy różne głosy. Po wybraniu głosu, za pomocą klawiszy (podpowiedź głosowa) należy podać numer abonenta z którym chcemy uzyskać połączenie. Numer abonenta inicjującego połączenie (w ramach usługi Żartofonu) nie jest wyświetlany na ekranie telefonu abonenta wywoływanego.
- Chcesz kogoś wkręcić - serwis umożliwia wybór jednego z trzech scenariuszy imitujących prawdziwą rozmowę telefoniczną. Po wybraniu jednego z trzech scenariuszy należy podać numer abonenta z którym chcemy uzyskać połączenie. Abonent wywoływany słyszy odtwarzane nagranie sprawiające wrażenie prawdziwej rozmowy telefonicznej której przysłuchuje się abonent wywołujący. Może on w każdej chwili włączyć się do tego imitowanego „dialogu". Numer abonenta inicjującego połączenie (w ramach usługi Żartofonu) nie jest wyświetlany na ekranie telefonu abonenta wywoływanego.
- Zapewnij sobie alibi – serwis umożliwia zmianę tła dźwiękowego w trakcie trwania rozmowy z wybranym numerem. Może to być tło dźwiękowe przypominające odgłosy w różnych miejscach publicznych, np. dworzec PKP, lotnisko, dyskoteka itp., lub też tło może stanowić rozmowa osób postronnych. W trakcie trwania rozmowy istnieje możliwość zmiany tła dźwiękowego z klawiatury aparatu telefonicznego. Numer abonenta inicjującego połączenie (w ramach usługi Żartofonu) nie jest wyświetany na ekranie telefonu abonenta wywoływanego tylko w przypadku gdy jest on zastrzeżony.

W przypadku pierwszych dwóch opcji, po zakończeniu połączenia abonent wywoływany otrzymuje wiadomość SMS z informacją o numerze abonenta inicjującego połączenie.

Telefony z wbudowaną funkcją zmiany głosu

Technika zmiany (morfingu) głosu została zaimplementowana w niektórych modelach aparatów telefonicznych telefonii komórkowej. Przykładem są produkty chińskiej firmy BAREL. Aparaty tej firmy oprócz wielu właściwości i funkcji, np. metalowa obudowa, możliwość użycia dwóch kart SIM, zaimplementowany odbiornik TV (wybrane modele) posiadają tzw. funkcję Magic Voice umożliwiającą zmianę głosu osoby korzystającej z aparatu. Do wyboru użytkownik ma następujące opcje: głos kobiecy (3 opcje), głos męski (2 opcje), głos dziecięcy (3 opcje), głos starca (2 opcje). Zmiana tła rozmowy (kilka scenariuszy), np. dworzec kolejowy, ruch uliczny, restauracja itp. W przeciwieństwie do usługi „ŻARTOFON" użytkownik może w trybie on-line tzn. z wykorzystaniem klawiatury telefonu, wybrać interesującą go opcję zmiany głosu.

SPOSOBY OCHRONY PRZED IMPERSONACJĄ

Jednym ze sposobów walki z atakami na zmianę tożsamości głosowej jest celowa weryfikacja wspólnej wiedzy posiadanej przez obu abonentów w łączu telefonicznym („to co wiem"). Podczas rozmowy padają zapytania o unikalną wiedzę znaną tylko abonentom a na podstawie otrzymanych odpowiedzi można autoryzować rozmówcę lub zakończyć połączenie. Innym sposobem jest weryfikacja abonenta na podstawie posiadanego przez niego klucza dostępowego „to co mam". Opracowana w Wojskowej Akademii Technicznej metoda uwierzytelniania polega na zastosowaniu techniki ukrywania informacji (watermarking) celem przesyłania przez łącze dodatkowej informacji w sposób skryty razem z sygnałem mowy [11,12]. Ta dodatkowa informacja jest przesyłana za pomocą tzw. sygnału znaku wodnego, który jest niesłyszalny w obecności sygnału mowy. Po stronie odbiorczej łącza, sygnał znaku wodnego jest dekodowany celem uzyskania numeru PIN abonenta a następnie tak uzyskany PIN jest porównywany w bazie danych terminala. W przypadku zgodności obu PIN-ów: nadawanego i przechowywanego po stronie odbiorczej, następuje uwierzytelnienie abonenta. Na Rys. 2 przedstawiono widok opisywanego urządzenia – mikrotelefonu z funkcją skrytego uwierzytelniania MAK. Opisane rozwiązanie jest chronione krajowym i europejskim zgłoszeniem patentowym.

Rys.2 Mikrotelefon z funkcją skrytego uwierzytelniania MAK.

WNIOSKI

Przedstawiona problematyka impersonizacji i zachowania integralności komunikatu głosowego jest jednym z wiodących zagadnień związanych z bezpieczeństwem współczesnej telekomunikacji. Okazuje się, że zwykła, subiektywna alokacja głosu rozmówcy do danej osoby może być błędna czy to na skutek

niecelowych zdarzeń losowych: szum otoczenia, zbliżone cechy morfologiczne głosu do innego mówcy ale również i zamierzona jako celowe działanie intruza. Należy zauważyć, że brak dostępnych, oficjalnych publikacji dotyczących statystyk zjawiska impersonizacji jest kolejnym argumentem za ważnością problematyki. Żadna instytucja państwowa czy firma prywatna nie jest zainteresowana i nie ma obowiązku publikacji takich danych a w szczególności informowania publicznie o metodach stosowanych przez wyspecjalizowane grupy „intruzów" sieci telekomunikacyjnej. Należy jednak wyprzedzić potencjalny, możliwy do realizacji atak typu voice spoofing na warstwę komunikacyjną oraz warstwę transmisyjną systmeów telefonicznych m.in. poprzez analizę i przewidywanie potencjalnie groźnych i niebezpiecznych scenariuszy. Celem takich działań jest przede wszystkim wypracowanie gotowej odpowiedzi generowanej przez kluczowe systemy w infrastrukturze bezpieczeństwa Państwa oraz posiadanie zawczasu wypracowanych strategii przeciwdziałania nowym zidentyfikowanym zagrożeniom.

BIBLIOGRAFIA

[1] http://spoofapp.com/

[2] http://www.spoofcard.com/

[3] https://www.phonegangster.com/

[4] http://spooftel.com/

[5] VoIP Security Alliance, VoIP Security and Privacy Threat Taxonomy, version 1.0, http://www.voipsa.org/Activities/taxonomy.php

[6], A.D. Keromytis: A look at VoIP vulnerabilities. Login Magazine vol. 35 s. 41-50, 2010.

[7] http://cve.mitre.org/cve/

[8] R.J. Sutton: Secure Communications. Applications and Management, John Wiley & Sons Ltd., 2002.

[9] http://www.hfhrpol.waw.pl/interwencja/images/stories/ad46.pdf

[10] http://www.plus.pl/ Regulamin Promocji Portalu Głosowo-Rozrywkowego „Żartofon – połączenie z numerem *7177"

[11] Z. Piotrowski, P. Gajewski: Identity management in VHF radio systems, Computational Methods and Experimental Measurements XV, CMEM XV, WIT Press 2011, Southampton, Boston, pp.473-481, 2011.

[12] Z. Piotrowski: The National Network-Centric System and its components in the age of Information Warfare, Safety and Security Engineering III, SAFE III, WIT Press 2009, Southampton, Boston, pp.301-309, 2009.