Wojciech MAZURCZYK, Krzysztof SZCZYPIORSKI
Instytut Telekomunikacji, Politechnika Warszawska,
00-665 Warszawa, ul. Nowowiejska 15/19,
E-mail: {W.Mazurczyk, K.Szczypiorski}@elka.pw.edu.pl,
http://security.tele.pw.edu.pl

BEZPIECZEŃSTWO VOIP OPARTEGO NA SIP

W referacie przedstawiono zagadnienia związane z bezpieczeństwem protokołu SIP (Session Initiation Protocol) jako najbardziej obiecującego protokołu sygnalizacyjnego dla realizacji usługi VoIP (Voice over IP). Skupiono się przede wszystkim na zagadnieniach związanych z bezpieczeństwem wiadomości sygnalizacyjnych wymienianych pomiędzy komunikującymi się stronami.

Szczególny nacisk położono na analizę mechanizmów bezpieczeństwa zastosowanych w dwóch zaleceniach organizacji IETF (The Internet Engineering Task Force) dla SIP: RFC 2543 (dot. pierwszej wersji SIP z 1999 r.) oraz RFC 3261 (dot. drugiej wersji SIP z 2002 r.). Do oceny protokołu przyjęto kryterium bazujące na usługach i mechanizmach ochrony informacji według normy ISO 7498-2.

Poddano dokładnej analizie zagadnienia związane z realizacją usług poufności i uwierzytelnienia, jako wyznaczników jakości bezpieczeństwa usługi VoIP opartej na SIP. Uwzględniono również podział mechanizmów bezpieczeństwa (dla obu zaleceń) zarówno dla usługi uwierzytelnienia jak i poufności ze względu na obszar realizacji danej usługi w odniesieniu do drogi komunikacyjnej. Stąd wprowadzono podział na mechanizmy typu: *End-to-End* oraz *Hop-by-Hop*.

Następnie wskazano potencjalne możliwości oraz techniki ataku na omawiany protokół oraz słabe punkty architektury bezpieczeństwa SIP dla obydwu wspomnianych powyżej wersji SIP. Poprzez ich analizę, czyli porównanie obu istniejących zaleceń wykazano słuszność opracowania nowszego z nich (RFC 3261).

Przedstawiono również wyniki przeprowadzonych badań praktycznych wybranych aplikacji, będących implementacjami Agenta Użytkownika SIP - interfejsu pomiędzy użytkownikiem a telefonią internetową. Głównym celem wykonanych doświadczeń było wykazanie wyższości implementowania nawet najprostszych mechanizmów bezpieczeństwa opisanych w zaleceniach SIP nad nie stosowaniem ich w ogóle.

Zbadano odporność zestawianego lub istniejącego już połączenia, pomiędzy dwoma systemami końcowymi, na potencjalne ataki na sygnalizację SIP. Dodatkowo omówiono wyniki testów zgodności Agentów Użytkownika SIP z zaleceniami, na których bazują - niedokładność w implementowaniu tego typu aplikacji może być przyczyną poważnych luk w ich bezpieczeństwie.

Przeprowadzone doświadczenia wykorzystywały wcześniej opracowane testy, których postać stanowiły odpowiednio przygotowane wiadomości sygnalizacyjne protokołu SIP, czasem niepoprawne, stworzone celowo tak, by oddać jak najszersze spektrum możliwych zagrożeń dla bezpieczeństwa SIP. Następnie dokonano interpretacji otrzymanych wyników.

Na koniec zaproponowano przykład bezpiecznej konfiguracji usługi Voice over IP opartej na SIP w wersji drugiej tj. bazującej na zaleceniu RFC 3261. Wskazano na istotną kwestię w projektowaniu takiej konfiguracji poprzez umiejętny dobór dostępnych mechanizmów bezpieczeństwa oferowanych przez SIP pomiędzy określonymi jednostkami funkcjonalnymi tego protokołu sygnalizacyjnego (np. pomiędzy Agentem Użytkownika a serwerem Proxy czy Redirect).

Dodatkowo koncepcja takiego systemu bazuje na definicji „zaufanej domeny", w której jedynym węzłem połączonym bezpośrednio z siecią zewnętrzną jest brzegowy serwer proxy, który wykorzystując *firewalling* dopuszcza ruch do „wnętrza" domeny tylko jednostek wcześniej uwierzytelnionych.