Planowanie bezpiecznej komunikacji w sieciach komputerowych zgodnej z zaleceniami ITU-T

Marcin Niemiec, Andrzej R. Pach, Piotr Pacyna (e-mail: {niemiec, pach, pacyna}@kt.agh.edu.pl)
Katedra Telekomunikacji Akademii Górniczo-Hutniczej, Kraków

STRESZCZENIE

Niniejszy artykuł omawia problematykę projektowania architektury bezpieczeństwa dla komunikacji pomiędzy użytkownikami końcowymi w sieci komputerowej. Szczególną uwagę zwrócono na zgodność mechanizmów odpowiadających za ochronę danych z zaleceniami międzynarodowej organizacji normalizacyjnej ITU-T (International Telecommunication Union). Przedstawione zostały metody ochrony danych oraz techniki, za pomocą których realizowana jest bezpieczna komunikacja. Opisane zostały dwie przykładowe architektury bezpieczeństwa: jedna, powszechnie używana w środowiskach sieciowych, i druga, będąca własną propozycją autorów. Omawiając przedstawione rozwiązania, zwrócono dużą uwagę na wydajność obu systemów.

ABSTRACT

Design the secure communication for computers networks compatible with ITU-T recommendations

This paper introduces design considerations of a security architecture for network systems providing end-to-end communications. We present eight dimensions of a security architecture which are based on recommendations of International Telecommunication Union and a few security techniques that are often employed to protect against major security threats. We also present two examples of security architectures: the first of them is currently being deployed and exploited in production networks while the second is our own proposition.

1. Wstęp

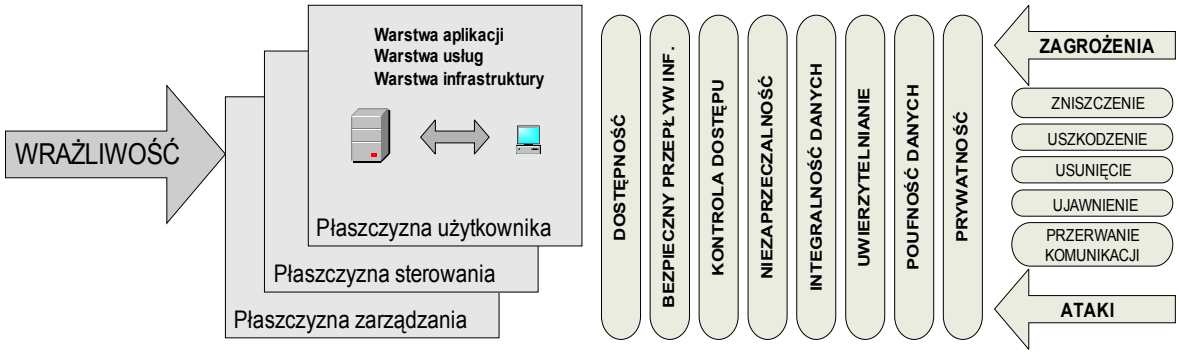
Bezpieczeństwo danych przesyłanych w sieci staje się jednym z najpoważniejszych problemów, z którymi styka się współczesna telekomunikacja. Obecnie ogromne środki przeznaczane są na poprawę bezpieczeństwa i nowe techniki ochrony, co obrazuje, jak żywym problemem stała się dziś poufność informacji. Informacja elektroniczna narażona jest na szereg różnych zagrożeń ze strony osób nieuprawnionych do dysponowania nią. Istnieje realne niebezpieczeństwo odczytania informacji prywatnej, jej modyfikacji czy sfabrykowania. W celu jej zabezpieczenia, projektowane są coraz nowsze sposoby ochrony, które razem tworzą jedną architekturę bezpieczeństwa dla informacji elektronicznej.

W terminie „bezpieczeństwo" zawiera się całokształt problemów związanych z ochroną danych zgromadzonych i przesyłanych w sieci telekomunikacyjnej. Tak rozumiane bezpieczeństwo obejmuje między innymi kwestie: zachowania poufności danych, weryfikację tożsamości osoby lub urządzenia końcowego, problemy związane z protokołami komunikacyjnymi, błędami w oprogramowaniu systemowym, nieprawidłowościami w pracy administratorów i użytkowników sieci, problematykę nadużyć i ataków, a także nietechniczne środki ochrony. W artykule skupimy się nad technicznymi problemami bezpieczeństwa danych przesyłanych w sieciach komputerowych, a więc ich poufności, integralności itp. Poprzez termin „architektura bezpieczeństwa" będziemy rozumieć zorganizowany zestaw procedur, za pomocą których realizowana jest ochrona danych w sieci. W skład tak rozumianej architektury bezpieczeństwa wejdą zarówno algorytmy ochrony danych, jak i protokoły zapewniające bezpieczną komunikację, a także specjalna struktura pakietów przesyłających dane użytkowe.

Niniejszy artykuł porusza kwestię bezpieczeństwa danych przesyłanych w sieciach komputerowych. Duży nacisk położono na zgodność mechanizmów odpowiadających za ochronę danych z zaleceniami międzynarodowej organizacji normalizacyjnej ITU-T (*International Telecommunication Union*) [4]. Przedstawiono metody ochrony danych oraz techniki, za pomocą których realizowana jest bezpieczna komunikacja. Podane zostały również przykładowe algorytmy ochrony danych. W końcowej części artykułu opisane zostały dwie architektury bezpieczeństwa, dzięki którym można zrealizować bezpieczną komunikację w sieciach komputerowych.

2. Zalecenie ITU-T X.805

Planując architekturę bezpieczeństwa, należy zadbać o to, aby była ona zgodna ze standardami lub zaleceniami międzynarodowych jednostek normalizujących w dziedzinie telekomunikacji. Jednym z najnowszych zaleceń międzynarodowej organizacji normalizacyjnej ITU-T w dziedzinie bezpieczeństwa jest opracowany w 2003 roku dokument X.805 *Security architecture for systems providing end-to-end communications* [3]. Zalecenie to przedstawia strukturę bezpieczeństwa dla komunikacji między punktami końcowymi sieci. Schemat tej struktury bezpieczeństwa został przedstawiony na rysunku 1.



Rys. 1. Elementy struktury bezpieczeństwa wg ITU-T (zalecenie X.805)

Zgodnie z zaleceniem X.805, każdy system cechuje pewna wrażliwość na zagrożenia (*vulnerability*). Parametr ten definiuje wady lub słabości systemu, które mogą być wykorzystane do naruszenia jego bezpieczeństwa. Tak zdefiniowana wrażliwość może być efektem złego zaprojektowania, złej implementacji, złej obsługi i konfiguracji oraz innych specyficznych wad systemu.

Dwa dalsze pojęcia, równie istotne przy projektowaniu architektury bezpieczeństwa, to zagrożenie i atak. Zagrożenia (*threats*) mają miejsce we wrażliwych systemach i mogą doprowadzić do naruszenia ich bezpieczeństwa.

Zdefiniować można pięć typów zagrożeń:

1) zniszczenie danych,
2) uszkodzenie danych,
3) usunięcie danych,
4) ujawnienie informacji,
5) przerwanie komunikacji.

Atak ma miejsce wtedy, kiedy konkretne zagrożenie ma miejsce we wrażliwym systemie. Jest on próbą naruszenia bezpieczeństwa systemu przez osobę niepowołaną do podejmowania pewnych działań.

Opisując architekturę bezpieczeństwa dla komunikacji między jednostkami, zalecenie X.805 wprowadza pojęcia warstw i płaszczyzn bezpieczeństwa. Autorzy zalecenia zdefiniowali trzy warstwy bezpieczeństwa (*security layers*).

Są to kolejno warstwy:

1) aplikacji,
2) usług sieciowych,
3) infrastruktury.

Ochrona systemu powinna odbywać się w każdej z warstw. Jest rzeczą oczywistą, że inaczej będzie realizowana kwestia bezpieczeństwa z punktu widzenia infrastruktury sieci – ruterów, przełączników czy serwerów, inaczej z punktu widzenia dostępnych usług sieciowych, np.: DHCP (*Dynamic Host Configuration Protocol*), DNS (*Domain Name Service*), VPN (*Virtual Private Network*), a jeszcze inaczej z punktu widzenia aplikacji używanych przez użytkowników końcowych.

Obok warstw bezpieczeństwa zdefiniowano płaszczyzny bezpieczeństwa (*security planes*), czyli strefy działań, gdzie powinno się zapewnić ochronę systemu. Wśród nich zalecenie ITU-T wyróżnia płaszczyznę zarządzania, sterowania i użytkownika końcowego. Ochrona danych powinna być realizowana w każdej strefie. Przykładowo rozważmy usługę VoIP (*Voice over IP*): płaszczyzna zarządzania odpowiadać będzie za reguły dostępu do tej usługi dla różnych użytkowników, płaszczyzna sterowania będzie odpowiadała za sygnalizację pomiędzy telefonem a centralą, natomiast płaszczyzna użytkownika zabezpieczać będzie sygnał głosu przesyłany między abonentem a centralą telefoniczną.

W tak zdefiniowanych warstwach i płaszczyznach bezpieczeństwa, zalecenie X.805 wprowadza metody ochrony wrażliwego systemu przed atakami. Każda z metod chroni przed innym rodzajem zagrożeń, a wspólnie tworzą pełny system bezpieczeństwa.

W dalszej części przedstawiono osiem metod ochrony systemu.

1) Prywatność (*privacy*) – prawo nadzorowania i wyłącznego dysponowania informacją na swój temat oraz do zachowania jej tylko dla siebie lub udostępnienia go określonym osobom.
2) Poufność danych (*data confidentiality*) – wiąże się z ograniczeniem dostępu do danych. Dane poufne to takie, które są znane tylko pewnej grupie osób, a przed innymi są trzymane w tajemnicy.
3) Uwierzytelnianie (*authentication*) – jest czynnością polegającą na potwierdzeniu czyjejś tożsamości wobec innej jednostki.
4) Integralność danych (*data integrity*) – właściwość danych, która gwarantuje, że ewentualna modyfikacja lub utrata części danych w trakcie transmisji zostanie wykryta przez odbiorcę.
5) Niezaprzeczalność (*non-repudiation*) – zdolność do udowodnienia pewnemu podmiotowi, że wykonał daną czynność.
6) Kontrola dostępu (*access control*) – ochrona przed nieuprawnionym dostępem do zasobów.
7) Bezpieczny przepływ informacji (*communication security*) – zapewnia wymianę danych pomiędzy uprawnionymi jednostkami.
8) Dostępność (*availability*) – zapewnia, że nie ma ograniczeń w dostępie do informacji, zasobów ani korzystania z usług czy działania aplikacji.

Zalecenie X.805 stwierdza, że każdy system ma pewną wrażliwość na zagrożenia i ataki. Komunikacja między jednostkami w sieci może odbywać się w sposób bezpieczny dzięki temu, że w trzech warstwach (aplikacji, usług sieciowych i infrastruktury) oraz płaszczyznach ochrony (zarządzania, sterowania i użytkownika końcowego) wprowadzone są wymienione wcześniej metody ochrony systemu.

Nie wszystkie stworzone dotychczas architektury bezpieczeństwa systemów realizują ochronę danych we wszystkich warstwach i płaszczyznach bezpieczeństwa, oraz nie wszystkie stosują przedstawione metody bezpieczeństwa. W takich systemach zagrożenie atakiem, który może zakończyć się powodzeniem, jest o wiele większe.

3. Techniki ochrony danych

Poprawna architektura bezpieczeństwa będzie składała się z różnych metod ochrony danych, które realizowane są za pomocą dobranych odpowiednio technik. Ważne jest, aby techniki budujące system bezpieczeństwa były stosowane w odpowiedniej kolejności tak, aby zapewnić najwyższy stopień bezpieczeństwa.

Uwierzytelnianie

Uwierzytelnianie pozwala potwierdzić tożsamość danej jednostki wobec pewnego podmiotu. Dzięki niemu użytkownik może być poprawnie rozpoznany, jeśli wiarygodnie potwierdzi swoją tożsamość. Dzięki uwierzytelnieniu można udostępnić pewne zasoby jedynie dla osób, które mają do nich prawo. Każda próba podszycia się osoby nieuprawnionej pod użytkownika uprawnionego powinna zakończyć się niepowodzeniem.

Obecnie spotyka się wiele sposobów uwierzytelniania użytkowników w sieci komputerowej. Do najprostszych należy stosowanie identyfikatorów i haseł. Podstawową zaletą haseł jest prostota ich stosowania oraz niski koszt implementacji i utrzymania systemu. Poza tym hasła są przenośne, więc nie ma trudności z uwierzytelnianiem użytkowników zmieniających punkt dostępu do sieci, w którym następuje uwierzytelnienie. W przypadku gdy hasło zostaje zapomniane, w prosty sposób można je zmienić na inne. Jednak opisywana metoda ma kilka poważnych wad. Przede wszystkim, gdy użytkownik nie przestrzega podstawowych zasad poufności swojego hasła, użytkownik nieuprawniony może je podejrzeć lub podsłuchać. Metoda staje się mało bezpieczna w przypadku, gdy użytkownik wprowadził hasło proste do odgadnięcia lub zbyt krótkie.

Bezpieczniejszą metodą jest używanie przenośnych kart magnetycznych lub elektronicznych. Są one trudne do podrobienia, ponieważ informacja w nich zawarta nie jest jawna, a ich małe rozmiary nie zmniejszają ich funkcjonalności. Koszt wdrożenia takiego systemu uwierzytelniania jest jednak większy niż przy metodzie wykorzystującej identyfikatory i hasła. Wadą kart jest niebezpieczeństwo wykradnięcia i bezprawnego ich użycia przez nieuprawnionego użytkownika.

Najbezpieczniejszą metodą uwierzytelniania użytkowników jest sprawdzanie ich cech biologicznych, takich jak: linie papilarne, analiza głosu czy struktura tęczówki oka. Metody te, mimo że bardzo bezpieczne, są rzadko stosowane w praktyce ze względu na wysokie koszty.

Szyfrowanie

Szyfrowanie jest przekształceniem poufnych danych do postaci nieczytelnej dla osób niepowołanych, a więc takich, które nie znają metody, jaka została użyta, lub nie posiadają odpowiedniego klucza koniecznego do odczytania ukrytej informacji.

Każdy szyfr zawierać musi trzy podstawowe składowe:

1) alfabet, za pomocą którego można reprezentować zakodowaną informację (kryptogram);
2) algorytm kodowania i algorytm dekodowania informacji;
3) klucze, za pomocą których dane są szyfrowane i odszyfrowywane.

Pierwsze dwie składowe są zwykle jawne, a wiedzę o nich posiadają zarówno użytkownicy systemów informatycznych, jak i intruzi pragnący odczytać poufną informację. W takim wypadku klucze zapewniają poufność zaszyfrowanej informacji – tylko osoba znająca klucz, za pomocą którego pewna informacja została utajniona, może tę informację odczytać.

Wśród współczesnych algorytmów można wyróżnić dwie duże grupy szyfrów:

1) symetryczną,
2) asymetryczną.

Szyfry symetryczne używają tego samego klucza zarówno do szyfrowania danych jak i do ich późniejszego odszyfrowywania. Ich zaletą jest wysoki poziom bezpieczeństwa i szybkość działania. Podstawową wadą szyfrów symetrycznych jest to, że w środowisku sieciowym wymagają, aby zarówno nadawca danych, jak i odbiorca znali klucz jeszcze przed transmisją danych.

Wady tej pozbawione są szyfry asymetryczne. Używają one dwóch kluczy:

1) publicznego,
2) prywatnego.

Aby odczytać tekst zaszyfrowany kluczem publicznym, należy użyć odpowiadającego mu klucza prywatnego. Jeżeli natomiast informację zaszyfrowano kluczem prywatnym, odszyfrować ją może każdy, kto zna klucz publiczny. Klucz prywatny jest poufny, a klucz publiczny powinien być powszechnie znany. Szyfry asymetryczne zwykle wykazują większą złożoność obliczeniową, więc są relatywnie wolniejsze w obliczaniu kryptogramów od szyfrów symetrycznych, a generowanie odpowiednich par kluczy jest kłopotliwe.

Najbardziej znane symetryczne algorytmy szyfrujące to stworzony w 1973 roku DES (*Data Encryption Standard*), IDEA (*International Data Encryption Algorithm*) oraz stosunkowo nowy AES (*Advanced Encryption*

Standard). Do najpopularniejszych algorytmów asymetrycznych można zaliczyć RSA, którego nazwa powstała od pierwszych liter nazwisk twórców: Rivest, Shamir i Adelman, i algorytm Rabina [6, 7].

Bezpieczna wymiana kluczy

Aby przeprowadzić szyfrowanie informacji za pomocą algorytmów symetrycznych, konieczne jest wcześniejsze uzgodnienie klucza pomiędzy użytkownikami. W środowisku sieciowym klucze to ciągi binarne, które zgodnie z pewnym algorytmem, modyfikują szyfrowaną informację binarną. W praktyce ich długość waha się od 54 do 1024 bitów. Długość klucza ma istotne znaczenie dla bezpieczeństwa utajnianej wiadomości. Klucze krótkie można złamać atakiem brutalnym – próbując kolejno wszystkie możliwe wartości klucza. Standardową długością staje się dziś 128, a nawet 256 bitów.

Klucz należy przesyłać w bezpieczny sposób, ponieważ jego odczytanie przez osobę nieuprawnioną może spowodować naruszenie poufności danych. Ustalanie nowych kluczy może być spowodowane potrzebą zestawienia połączenia lub wymianą używanego klucza na nowy. Zbyt długie stosowanie tego samego klucza obniża bezpieczeństwo całego systemu.

Automatyczna wymiana kluczy za pomocą specjalnie w tym celu skonstruowanych algorytmów jest koniecznością, szczególnie w przypadku terminali połączonych w dużą sieć, gdzie uciążliwa byłaby ich wymiana metodami bezpośrednimi. Obecnie sposoby bezpiecznego ustalania kluczy stały się powszechne, a ich różnorodność pozwala na wybór najbardziej odpowiedniej techniki w danym środowisku.

Algorytmy bezpiecznej wymiany kluczy można podzielić na:

- sposoby wymiany typu punkt-punkt,
- algorytmy wymiany za pośrednictwem Centrum Dystrybucji Kluczy (KDC – *Key Distribution Center*).

Jako przykład algorytmu wymiany kluczy typu punkt-punkt można podać prostą metodę opartą na szyfrowaniu wymienianego klucza. Szyfrowanie odbywa się przy wykorzystaniu znanego obu osobom asymetrycznego algorytmu szyfrującego. Po wymianie klucza, użytkownicy zaczynają stosować szyfr symetryczny. Innym przykładem może być algorytm Diffie-Hellmana. Wśród rozwiązań wykorzystujących Centrum Dystrybucji Kluczy, najbardziej znanymi metodami wymiany są: Kerberos i algorytm Needhama-Schroedera [11, 12].

Skrót wiadomości

Jednokierunkowa funkcja skrótu, zwana również funkcją hashującą, od angielskiego słowa *hash* – mieszać, jest przekształceniem, które z ciągu binarnego o dowolnej długości bitów generuje krótką wartość binarną (skrót), unikalną i charakterystyczną dla tego ciągu [1].

Podstawową cechą, którą muszą charakteryzować się funkcje skrótu, jest wrażliwość wyniku na zmiany w oryginalnym tekście. Jeden zmieniony bit wiadomości powinien spowodować zmianę około połowy bitów skrótu. Ważną cechą funkcji skrótu jest małe prawdopodobieństwo kolizji, które oznacza, że prawdopodobieństwo istnienia dwóch wiadomości o identycznych skrótach musi być bardzo małe. Mimo że obliczenie skrótu wiadomości powinno być łatwym zadaniem, funkcja skrótu musi być nieodwracalna – silnie jednokierunkowa, to znaczy, że niemożliwe jest obliczenie oryginalnego tekstu wiadomości na podstawie jej skrótu.

Funkcje skrótu znajdują powszechne zastosowanie w ochronie integralności. W najprostszym wariancie obliczany jest skrót tekstu jawnego i dołączany do kryptogramu, odbiorca po odszyfrowaniu wiadomości oblicza jej skrót i porównuje z otrzymanym. Jeżeli skróty są identyczne, to można mieć pewność, że dane nie zostały zmodyfikowane w trakcie transmisji. Innym przykładem zastosowania funkcji skrótu są techniki uwierzytelniania wiadomości przesyłanych pocztą elektroniczną. Treść wiadomości lub dokumentu poddawana jest wówczas działaniu funkcji skrótu, a otrzymany w rezultacie ciąg znaków, będący znacznie krótszy od tekstu wejściowego, jest szyfrowany przy użyciu asymetrycznych algorytmów kryptograficznych. Jeśli skrót wiadomości zaszyfrowany zostanie kluczem prywatnym, staje się rodzajem elektronicznego podpisu, który po dołączeniu do oryginalnego listu pozwala adresatowi upewnić się o autentyczności przesyłki.

Współcześnie wykorzystywane funkcje skrótu dają wynik o długości minimum 128 bitów. Do algorytmów tych zaliczyć można funkcję MD-4 (*Message Digest*) oraz ulepszoną i bezpieczniejszą od niej funkcję MD5. Skrót dłuższy (160 bitów) generują funkcje SHA-1 (*Secure Hash Algorithm*) oraz RIPEMD-160 (*RACE Integrity Primitives Evaluation Message Digest*). Działanie wspomnianych algorytmów opiera się na obliczaniu szeregu funkcji nieliniowych na wszystkich bitach wiadomości. Dzięki temu zapewniona jest jednokierunkowość funkcji skrótu.

Znakowanie czasem

Istnieje szereg sytuacji, w których obok potwierdzenia tożsamości użytkownika, zapewnienia poufności oraz weryfikacji integralności przesyłanych danych, istotną kwestią jest jednoznaczne określenie momentu, w którym dane zostały utworzone. Aby zrealizować ten cel, przesyłana wiadomość powinna zostać zaopatrzona w tak zwany znacznik czasu (*digital timestamp*), który jednoznacznie określa czas, w którym zbiór danych został oznakowany. Znakowanie czasem można dokonać indywidualnie lub za pośrednictwem zaufanej jednostki trzeciej. W pierwszym przypadku, aktualny czas pobrany zostaje z lokalnego systemu użytkownika, w przypadku drugim, wyspecjalizowana

jednostka pobiera czas z własnego, bardzo dokładnego zegara, a następnie oznacza dane znacznikiem czasu i odsyła je użytkownikom. System wykonujący znakowanie czasem musi uniemożliwiać manipulację czasem oraz zapewnić, iż osoba podpisująca pewne dane nie będzie mogła twierdzić, iż dokonała ich podpisania przed momentem oznakowania czasem.

Zwykle znacznik czasu tworzy się w dwóch fazach. Najpierw przekształca się dane za pomocą funkcji skrótu, a następnie skrót wiąże się kryptograficznie z parametrem, który określa aktualne wskazanie zegara.

4. Przykłady architektur bezpieczeństwa

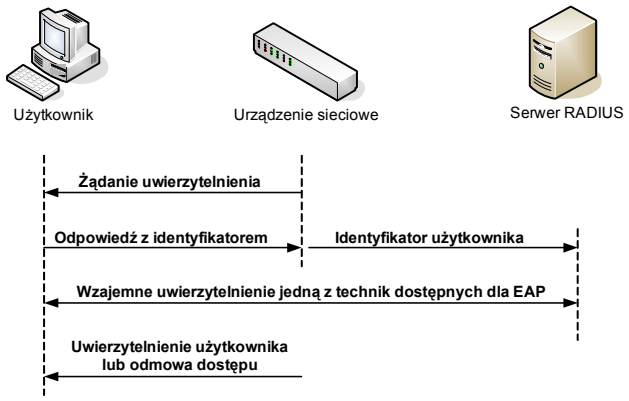
Wybór odpowiednich technik bezpieczeństwa jest istotnym krokiem w procesie projektowania bezpiecznego systemu komunikacji w sieci komputerowej. Ważną kwestią staje się tutaj dobór odpowiednich algorytmów. Istotna jest także wydajność bezpiecznego systemu. Należy pamiętać, że wydajność systemu maleje wraz ze wzrostem bezpieczeństwa.

W procesie projektowania architektury bezpieczeństwa, należy tak dobierać techniki ochrony oraz stosowane algorytmy, aby wydajność nie zmalała w istotny sposób [2]. Częstym wymogiem jest, aby wydajność nie zmalała w sposób zauważalny dla użytkownika systemu. Dlatego działanie algorytmów szyfrujących, funkcji skrótu i innych rozwiązań powinno zajmować tak mało czasu, aby użytkownik miał wrażenie, że dzieje się to natychmiastowo. Kwestia wydajności staje się szczególnie ważna dla takich rozwiązań, jak np. wymiana danych sygnalizacyjnych. Wtedy przy doborze odpowiednich algorytmów należy zwrócić szczególną uwagę na ich złożoność obliczeniową, aby komunikacja między użytkownikami systemu mogła być zbudowana i aby nie została przerwana w późniejszym czasie.

EAP/IPsec

We współczesnej telekomunikacji stosuje się wiele różnych rozwiązań, które zabezpieczają informację przesyłaną w sieciach komputerowych. Wśród tych, które ze względu na swoje dobre własności ochrony stosowane są powszechnie, na szczególną uwagę zasługują: IPsec (*IP security*) oraz protokół uwierzytelniania EAP (*Extensible Authentication Protocol*).

Identyfikacja użytkowników w sieciach bezprzewodowych typu 802.11 oraz sieciach przewodowych Ethernet bardzo często dokonywana jest za pomocą standardu IEEE 802.1x, który oparty jest na protokole EAP [8]. Sam 802.1x pracuje w warstwie dostępu do medium, blokując porty logiczne urządzeń dostępowych, aż do czasu uwierzytelnienia jednostek przez EAP. Protokół EAP pozwala zbierać dane identyfikacyjne użytkowników i na ich podstawie weryfikować poprawnie ich tożsamość. Protokół ten nie określa sposobu, w jaki użytkownicy przedstawiają się w sieci, zaś samo uwierzytelnianie opiera się na wymianie pakietów EAP, tzw. żądań i odpowiedzi. Dzięki temu jest on protokołem bardzo uniwersalnym, który pozwala na implementację różnych technik uwierzytelniania. Schemat ideowy uwierzytelniania przeprowadzonego przy wykorzystaniu protokołu EAP przedstawiony został na rysunku 2.



Rys. 2. Schemat uwierzytelniania protokołem EAP

Jedną z najczęściej stosowanych technik jest uwierzytelnianie przez certyfikaty, realizowane przez protokół EAP-TLS (*EAP Transport Level Security*) [10]. Certyfikaty to dane, podpisane cyfrowo przez pewną jednostkę (urząd certyfikacji), której można zaufać, służące do uwierzytelnienia nadawcy. Ich działanie opiera się na asymetrycznych algorytmach szyfrujących, a więc na istnieniu dwóch kluczy: publicznego i prywatnego. Działanie protokołu zaczyna się od wysłania do nowego użytkownika wiadomości zawierającej żądanie podania identyfikatora. Użytkownik, który chce potwierdzić swoją tożsamość, zwraca wiadomość, w której zawarty jest jego identyfikator. Następnie identyfikator jest wysyłany do serwera uwierzytelniającego (RADIUS – *Remote Authentication Dial In User Service*). Następuje wymiana certyfikatów i jeśli obie jednostki potwierdzą swoją tożsamość, wtedy uwierzytelnianie kończy się sukcesem. W przeciwnym wypadku użytkownik nie będzie obsługiwany.

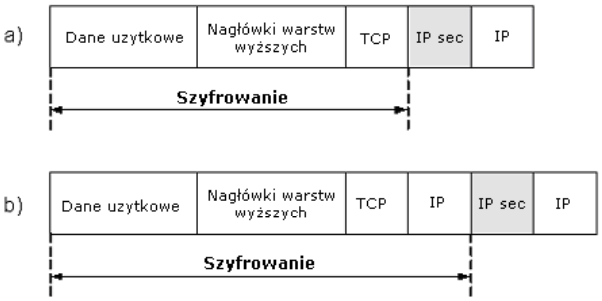
Protokół IPsec [9], ma na celu ochronę informacji przesyłanych w sieciach komputerowych. Jest on związany z protokołem IP. Zapewnia zarówno poufność, jak i integralność danych.

W celu ich realizacji, zdefiniowano dwa podprotokoły i odpowiadające im nagłówki rozszerzające:

- AH (*Authentication Header*),
- ESP (*Encapsulation Security Payload*).

Protokół AH zapewnia ochronę integralności zarówno dla przesyłanych danych, jak i części nagłówka IP. Ochroną obejmowane są te pola nagłówka, które nie ulegają zmianie podczas wędrówki przez sieć (np. adresy, identyfikator). Aby zapewnić integralność informacji wykorzystywane są takie funkcje skrótu, jak MD-5, SHA-1 lub RIPEMD-160.

Protokół ESP, obok ochrony integralności danych, zapewnia także ich szyfrowanie. Integralność sprawdzana jest tylko dla danych użytkowych. Szyfrowanie może odbywać się przy wykorzystaniu algorytmów, takich jak: DES, 3DES (*Triple DES*) czy AES. Algorytmy funkcji skrótu są takie same jak w przypadku AH.



Rys. 3. Tryby pracy protokołu IPsec: a) transportowy; b) tunelowy

Protokół IPsec może pracować w dwóch trybach. Oba z nich przedstawione zostały na rysunku 3. Pierwszym, najprostszym jest tzw. tryb transportowy. Pomiędzy nagłówkiem IP a protokołem wyższej warstwy (transportowej) dodaje się nagłówek IPsec. Chroni on zarówno dane użytkowe, jak i nagłówki wyższych warstw. Tak skonstruowany pakiet może poruszać się po globalnej sieci, chociaż tryb transportowy stosuje się zwykle w sieciach lokalnych z powodu wymagań dotyczących kolejności dostarczanych pakietów. Drugi tryb zapewnia tunelowanie protokołu IP. Dane użyteczne wraz ze wszystkimi nagłówkami są szyfrowane, a protokół IPsec buduje nowy nagłówek IP, w którym umieszcza adresy pośrednich ruterów, na trasie między nadawcą a odbiorcą, stanowiących końce tunelu IP. Dzięki temu, że wewnętrzny pakiet jest szyfrowany w całości, bierny obserwator nie ma możliwości stwierdzenia, między jakimi jednostkami zachodzi wymiana danych.

Propozycja własnej architektury

Aby chronić dane w systemie można rozważyć rozwiązanie, które będzie integrować szczególnie pożądane cechy dostępnych technik bezpieczeństwa. Świadomie dobierając odpowiednie techniki ochrony i algorytmy jesteśmy w stanie stworzyć bezpieczny i wydajny system ochrony danych.

Jeśli za wymóg postawimy sobie stworzenie wydajnego systemu, jako pierwszą technikę ochrony wprowadzić możemy uwierzytelnianie procedurą Lamporta. Metoda ta bazuje na obliczaniu funkcji skrótu z ciągu binarnego, który służy do poprawnej weryfikacji tożsamości użytkownika [11]. Protokół Lamporta jest rozwiązaniem o wiele prostszym od uwierzytelniania za pomocą EAP i dzięki temu bardziej wydajnym. Już po wysłaniu dwóch wiadomości, użytkownik jest w stanie potwierdzić swoją tożsamość. W protokole EAP takich wiadomości może być nawet kilkanaście [10]. Inną różnicą jest konieczność zastosowania dodatkowej jednostki w strukturze sieci: serwera uwierzytelniającego. Zwiększa on opóźnienie wynikające z procesu weryfikacji tożsamości danych jednostek i powiększa koszty sieci. Jednak zaletą EAP jest uniwersalność stosowania technik uwierzytelniających. Oprócz certyfikatów mogą to być np. hasła lub karty SIM.

Kolejną techniką ochrony może być szyfrowanie. Dobrym rozwiązaniem z punktu widzenia wydajności jest stosowanie symetrycznych szyfrów do zapewnienia poufności danych. Nie jest koniecznością stosowanie znanych algorytmów szyfrujących, tj. DES czy AES. Dobrym pomysłem jest stworzenie własnego algorytmu, np. skonstruowanie bezpiecznej sieci podstawieniowo-permutacyjnej [11]. Obok szybkości działania niewątpliwą jej zaletą jest wysoki poziom bezpieczeństwa. Mimo iż szyfry podstawieniowo-permutacyjne korzystają z niezbyt silnych kryptograficznie funkcji składowych: podstawień i permutacji, to wspólnie tworzą bezpieczny algorytm kryptograficzny. Skrzynki podstawieniowe połączone z permutacją bitów na ich wyjściach powodują, że wszystkie bity wyjściowe szyfru są skomplikowanymi funkcjami bitów wejścia. Mała zmiana na wejściu sieci spowoduje lawinę zmian na jej wyjściu.

Jako algorytm służący do ustalenia klucza szyfrującego między użytkownikami posłużyć może algorytm Diffie–Hellmana. Jest to prosty algorytm z grupy, która nie wymaga szyfrowania za pomocą wcześniej ustalonego klucza nadrzędnego (takiego, który istniał przed rozpoczęciem wymiany klucza służącego do szyfrowania bieżącej sesji). Jego bezpieczeństwo polega na trudności obliczenia dyskretnego logarytmu. Wymaga jedynie wymiany dwóch wiadomości.

Do bezpiecznej wymiany danych pomiędzy użytkownikami możemy wyspecyfikować własny protokół. Podstawowa jednostka takiego protokołu (pakiet) powinna zawierać wszystkie niezbędne pola zapewniające ochronę danych, jak również powinna być prosta, tak aby zapewnić jak najlepszą wydajność. Oprócz pola z zaszyfrowanymi danymi, powinno być w niej miejsce na znacznik czasu, gdzie zapisywane byłoby aktualne wskazanie zegara oraz pole przechowujące skrót całej wiadomości. Jako algorytmu skrótu można użyć jednego ze standardowych rozwiązań (np. SHA-1, MD-5) lub zaprojektować własny algorytm. Tak zaprojektowany protokół pracować będzie ponad warstwą transportową wg modelu ISO-OSI (*International Standards*

Organization – Open Systems Interconnection). Dane wraz z dodatkową informacją (np. znacznik czasu, liczba bitów danych) będą szyfrowane, np. za pomocą sieci podstawieniowo-permutacyjnej, natomiast skrót wiadomości dodawany będzie do zaszyfrowanej informacji. Następnie dołożone zostaną nagłówki warstwy transportowej oraz sieciowej i pakiety zostaną przesłane do odbiorcy za pośrednictwem protokołu IP [5]. Struktura tak wyspecyfikowanego pakietu została przedstawiona na rysunku 4.

Rys. 4. Przykładowa struktura jednostki protokołu

Podsumowując przedstawioną propozycję architektury bezpieczeństwa, należy podkreślić, że może ona działać przede wszystkim w warstwie aplikacji według zalecenia X.805, na płaszczyźnie użytkownika. Należy pamiętać o tym, że aby zapewnić wysoki poziom bezpieczeństwa systemu, ochrona danych powinna odbywać się we wszystkich warstwach i płaszczyznach modelu X.805.

Porównując architekturę EAP/IPsec z architekturą zaproponowaną przez autorów, znaleźć można wiele różnic pomiędzy tymi rozwiązaniami. Przykładowo, protokół Lamporta jest rozwiązaniem o wiele prostszym od EAP i dzięki temu bardziej wydajnym. Już po wysłaniu dwóch wiadomości, użytkownik jest w stanie potwierdzić swoją tożsamość. W protokole EAP takich wiadomości jest znacznie więcej. Następną różnicą jest konieczność zastosowania dodatkowej jednostki w strukturze sieci: serwera uwierzytelniającego. Zwiększa on opóźnienie wynikające z procesu weryfikacji tożsamości danych jednostek i powiększa koszty sieci. Jednak zaletą protokołu EAP jest uniwersalność stosowania technik uwierzytelniających. Mogą to być np.: hasła, certyfikaty lub karty SIM. Inną różnicą pomiędzy porównywanymi rozwiązaniami jest brak szyfrowania dla nagłówka warstwy transportowej – w zaprojektowanej architekturze nagłówek ten przesyłany jest w formie jawnej.

Bezpieczeństwo obu protokołów opiera się przede wszystkim na bezpieczeństwie zastosowanych algorytmów. Przy założeniu, że zastosowane szyfry i funkcje skrótu będą algorytmami odpornymi na różnego rodzaju ataki, można stwierdzić, że oba porównywane rozwiązania zapewniają wysoki poziom ochrony danych.

Obie przedstawione architektury bezpieczeństwa realizują większość z metod ochrony opisanych w zaleceniu X.805. Przede wszystkim zapewniają bezpieczny przepływ informacji pomiędzy dwoma użytkownikami sieci, zapewniają poufność przesyłanych danych oraz ich integralność. Zapewniają także uwierzytelnianie, dzięki czemu jedynie uprawnione jednostki mogą uczestniczyć w komunikacji. Z przeprowadzonej analizy działania rozwiązania EAP/IPsec, stworzonego przez organizację IETF (Internet Engineering Task Force) wynika, że jest ono zgodne z architekturą zalecaną przez ITU-T w dokumencie X.805.

5. Podsumowanie

W niniejszym artykule został omówiony problem bezpieczeństwa danych przesyłanych w sieciach komputerowych. Szczególną uwagę zwrócono na zalecenie X.805, w którym międzynarodowa organizacja standaryzacyjna ITU-T proponuje model bezpiecznej komunikacji między użytkownikami końcowymi. Omówione zostały pojęcia związane z tym modelem, tj. wrażliwość, zagrożenie i atak, warstwy i płaszczyzny ochrony oraz metody ochrony systemu. Następnie opisano przykładowe techniki ochrony oraz zgodnie z zaleceniem zaproponowano przykładową architekturę bezpieczeństwa, a następnie porównano ją z rozwiązaniem EAP/IPsec.

W trakcie projektowania architektury zwrócono szczególną uwagę na kwestię wydajności zabezpieczonego systemu: starano się zapewnić jak najmniejsze opóźnienia przesyłanych wiadomości, stosowano proste mechanizmy ochrony, a przy dobieraniu algorytmów szczególną uwagę zwracano na ich małą złożoność obliczeniową. Dzięki temu, rozwiązanie jest dobrym kompromisem pomiędzy stopniem bezpieczeństwem danych a wydajnością systemu ochrony. Zwrócono również uwagę, aby opracowana architektura bezpieczeństwa nie była jedynie luźnym połączeniem różnych technik bezpieczeństwa, a stanowiła w pełni działający system, skutecznie zabezpieczający przesyłane dane.

Literatura

[1] Buchmann J.S.: *Introduction to cryptography*. New York, Springer 2001

[2] Hardy D.W., Walker C.L.: *Applied algebra: codes, ciphers and discrete algorithms*. New Jersey, Pearson Education 2003

[3] ITU-T Recommendation X.805: *Security architecture for systems providing end-to-end communications*. 2003

[4] ITU-T Publication: *Security in Telecommunications and Information Technology*. 12/2003

[5] Nowicki K., Woźniak J.: *Sieci LAN, MAN i WAN – protokoły komunikacyjne*. Kraków. Wydawnictwo FPT 1998

[6] Ogiela M.R.: *Podstawy kryptografii*. Kraków, UWND AGH 2000

[7] Ogiela M.R.: *Systemy utajniania informacji*. Kraków, UWND AGH 2003

[8] Blunk L., Vollbrecht J.: *PPP Extensible Authentication Protocol (EAP)*. RFC 2284, 03/1998

[9] Kent S., Atkinson R.: *Security Architecture for the Internet Protocol*. RFC 2401, 11/1998

[10] Aboba B., Simon D.: *PPP EAP TLS Authentication Protocol*. RFC 2716, 10/1999

[11] Sadowski A.: *Wybrane zagadnienia kryptologii i ochrony informacji*. Wydawnictwo Helion, 1999

[12] Schroeder M., Needham R.: *Using encryption for authentication in large networks of computers. Communications of the ACM*, 12/1978

Marcin Niemiec urodził się w Tuchowie 11 października 1981 roku. Tytuł magistra inżyniera otrzymał na Wydziale Elektrotechniki, Automatyki i Elektroniki AGH w Krakowie. W trakcie studiów przebywał na półrocznym stypendium na Uniwersytecie Karola III w Madrycie. Studia magisterskie ukończył z wyróżnieniem. Obecnie uczestniczy w studium doktoranckim na Wydziale Elektrotechniki, Automatyki, Informatyki i Elektroniki AGH. Do jego zainteresowań naukowych należą: bezpieczeństwo sieci komputerowych, protokoły komunikacyjne, łączność bezprzewodowa i telefonia VoIP.

Andrzej Ryszard Pach ukończył Wydział Elektrotechniki, Automatyki i Elektroniki AGH w roku 1975, w r. 1977 doktoryzował się na AGH, a w roku 1990 uzyskał stopień doktora habilitowanego na Wydziale Elektroniki Politechniki Warszawskiej. Zatrudniony jest obecnie na stanowisku profesora zwyczajnego w Katedrze Telekomunikacji AGH, w której pełni funkcję kierownika. Wcześniej był prodziekanem Wydziału EAiE.

Główne zainteresowania naukowe związane są z sieciami telekomunikacyjnymi oraz systemami informacyjnymi. Autor ponad stu publikacji naukowych z zakresu protokołów komunikacyjnych, modelowania i analizy sieci komputerowych, sieci szerokopasmowych z integracją usług. Aktywnie uczestniczy w projektach europejskich IST, ACTS, COST i COPERNICUS. Członek komitetów programowych konferencji międzynarodowych. Konsultant firm państwowych i prywatnych w zakresie nowoczesnej telekomunikacji.

Współzałożyciel i wiceprezydent Fundacji Postępu Telekomunikacji, przewodniczący IEEE Communications Society Chapter.

Piotr Pacyna ukończył Informatykę na Wydziale Elektrotechniki, Automatyki i Elektroniki Akademii Górniczo-Hutniczej w Krakowie. w 2005 roku uzyskał stopien doktora nauk w dziedzinie Telekomunikacja. Obecnie pracuje w Katedrze Telekomunikacji AGH, gdzie prowadzi prace naukowe oraz zajęcia z przedmiotu Nowoczesne Sieci IP. Przebywał na stażach naukowych, m.in. w Loracom we Francji oraz w CNET France Telecom. Zainteresowania naukowe obejmują problematykę projektowania i użytkowania sieci IP: routing w sieciach stałych i w sieciach ad-hoc, wsparcie mobilności terminali ruchomych w sieci IP, bezpieczeństwo i sygnalizację. Jest aktywnie zaangażowany w międzynarodowe programy naukowo-badawcze ACTS oraz IST. Brał udział w pracach badawczych na zlecenie operatorów i firm telekomunikacyjnych. Organizował konferencję Protocols for Multimedia Systems PROMS2000. Jest współautorem czterech książek i autorem kilkunastu publikacji naukowych.