Projekt nr. POIG.02 03. 00-00-028/08-01
www.platon.pionier.net.pl
PLATFORMA OBSŁUGI NAUKI PLATON

KOORDYNATOR: INSTYTUT CHEMII BIOORGANICZNEJ PAN
POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE
ul. Noskowskiego 12/14, 61-704 Poznań, (+48 61) 858 20 00, fax: (+48 61) 852 59 54, e-mail: office@man.poznan.pl, www: http://www.man.poznan.pl

Uwierzytelnianie 802.1X w usłudze eduroam

Maja Górecka-Wolniewicz, UCI UMK (mgw@umk.pl)
Tomasz Wolniewicz, UCI UMK (twoln@umk.pl)
dokument przygotowany w ramach projektu B-R eduroam-PIONIER,
zaktualizowany w ramach projektu PLATON
wersja 2.0

Spis treści

1. Wstęp

Usługa eduroam, umożliwiająca korzystanie z sieci bezprzewodowej na terenie instytucji uczestniczących w projekcie, wykorzystuje funkcjonalność standardu 802.1X, którą opisujemy w niniejszym dokumencie. Zastosowana technologia umożliwia identyfikację osób ubiegających się o dostęp do sieci i sprawdzenie uprawnień. Instytucje uczestniczące w usłudze eduroam ufają sobie wzajemnie i akceptują osoby pozytywnie uwierzytelnione w macierzystych instytucjach. Standard 802.1X jest obecnie implementowany w większości urządzeń sieciowych oraz systemów operacyjnych. Dzięki temu można w sposób wygodny, elastyczny i bezpieczny konfigurować środowisko sieciowe, z którego korzystają różnorodni użytkownicy. Poniżej omawiamy przede wszystkim zastosowanie 802.1X w sieciach bezprzewodowych. Dominującym standardem szyfrowania w sieciach bezprzewodowych jest 802.11i znany szerzej pod nazwą WPA2, który korzysta z 802.1X.

802.1X - podstawy

Standard IEEE 802.1X ([1]) definiuje mechanizm uwierzytelniania i kontroli ruchu użytkowników w obrębie chronionej sieci oraz dostarcza techniki służące do dynamicznej zmiany kluczy szyfrujących stosowanych w komunikacji sieciowej. 802.1X bazuje na protokole EAP *(Extensible Authentication Protocol)* zdefiniowanym w RFC 3748 ([2]). Wspiera wiele metod uwierzytelniania, które zo-

staną przedstawione w części 3.1. Może być stosowany zarówno do sieci bezprzewodowych, jak i przewodowych. 802.1X definiuje również sposób opakowywania komunikatów EAP, tak by mogły one zostać obsłużone bezpośrednio w danym środowisku sieciowym LAN. Taka opakowana postać ramki EAP zwana jest EAPOL. EAPOL to nie tylko pakiety i dane, również funkcje sterujące przebiegiem komunikacji, np. start, logoff oraz polecenia dystrybucji kluczy. Technologia EAPOL jest zdefiniowana dla ethernetowych sieci lokalnych oraz sieci bezprzewodowych.

2. 802.1X – opis działania

W komunikacji zgodnej ze standardem 802.1X uczestniczą:

- klient *(client, suplicant)* – urządzenie, które chce zostać uwierzytelnione,
- urządzenie dostępowe, przełączniki *(authenticator, Access Point – AP)* – urządzenie realizujące kontrolę dostępu zgodnie ze wymogami 802.1X,
- serwer uwierzytelniający RADIUS *(authentication server)* – oprogramowanie sprawdzające poprawność danych uwierzytelniania i decydujące o przyznaniu uprawnień; EAP wspiera różne serwery uwierzytelniania, najczęściej stosowany jest serwer RADIUS.

Stosowanym protokołem komunikacji jest EAP, który nie definiuje szczegółowych zasad bezpieczeństwa oraz sposobu realizacji procesów uwierzytelnienia, natomiast zezwala na używanie różnorodnych metod uwierzytelniania. Urządzenie dostępowe transparentnie przekazuje komunikaty 802.1X.

Główne zalety standardu 802.1X to:

- wsparcie przez większość obecnych dostawców sprzętu sieciowego;
- poprawa bezpieczeństwa dzięki zastosowaniu dynamicznych kluczy szyfrujących;
- komunikacja oparta na standardzie EAP;
- zastosowanie otwartej architektury bezpieczeństwa, możliwość dodawania nowych metod uwierzytelniania bez potrzeby aktualizacji urządzeń sieciowych;
- korzystanie z serwerów uwierzytelniania opartych na standardzie RADIUS.

2.1. Zainicjowanie sesji

Jeśli klient nie został dotychczas uwierzytelniony, to między nim a urządzeniem dostępowym oraz serwerem uwierzytelniania mogą być przekazywane wyłącznie komunikaty EAP.

Praca w trybie 802.1X zaczyna się od momentu, gdy klient podłącza się do sieci i chce uzyskać informacje o możliwościach sieci. Na tym etapie klient nie dysponuje adresem IP, do komunikacji jest stosowany protokół EAPOL (EAP over LAN). Dalej komunikacja przebiega następująco:

1. urządzenie dostępowe widząc nowego klienta, transmituje do niego komunikat zawierający zapytanie o tożsamość `EAP-Request;`
2. klient, np. laptop, czy smartfon, wysyła do urządzenia dostępowego (AP) komunikat `EAP-start`;
3. AP odpowiada komunikatem `EAP-request/Identity`, mającym formę zapytania o tożsamość;
4. klient w odpowiedzi wysyła `EAP-response/Identity` – komunikat zawierający dane uwierzytelniania użytkownika;
5. AP przekazuje dane do serwera uwierzytelniającego RADIUS, który odsyła wynik uwierzytelnienia w postaci „zaakceptowany” lub „odrzucony”;
6. AP wysyła do klienta pakiet `EAP-Success` lub `EAP-Reject`;
7. jeśli RADIUS zaakceptował użytkownika, to AP ustawia port danego klienta w stan „uwierzytelniony”.

Czynności przedstawione w p. 5 i 6 wiążą się z kontaktem urządzenia dostępowego z serwerem uwierzytelniania. AP i serwer uwierzytelniania zazwyczaj stosują do komunikacji protokół RADIUS. W istocie nie jest to pojedyncza wymiana komunikatów, lecz kilka cykli zapytanie-odpowiedź. Po wymianie kompletu informacji serwer podejmuje decyzję o wyniku uwierzytelniania.

W przypadku pozytywnego wyniku procesu uwierzytelnienia, serwer może dodatkowo przekazywać parametry pozwalające na uszczegółowienie praw dostępu klienta poprzez umieszczenie go w konkretnym VLAN-ie.

2.2. Klucze sesyjne

Podstawowy protokół 802.1X umożliwia efektywną realizację procedury uwierzytelniania, niezależnie od stosowanych metod szyfrowania w sieci bezprzewodowej, również gdy korzystała ona ze słabych mechanizmów 802.11 WEP, a nawet gdy nie stosuje żadnego szyfrowania. Obecnie większość producentów sprzętu WiFi oferuje możliwość korzystania z mechanizmów dynamicznego zarządzania kluczami *(dynamic key exchange)*. Funkcjonalność ta pozwala na częste odświeżanie materiału kryptograficznego używanego do komunikacji. Zaakceptowany klient otrzymuje w fazie uwierzytelniania między innymi klucz sesyjny wygenerowany przez serwer RADIUS, przekazany wewnątrz komunikatów EAP. Ten sam klucz jest również przekazany do AP w pakiecie `Access-Accept` w postaci atrybutu `MS-MPPE-Recv-Key`. Znajomość klucza przez obie strony umożliwia nawiązanie szyfrowanej łączności, a jednocześnie wzajemnie uwierzytelnia obie strony. Zaraz po przekazaniu do klienta odpowiedzi EAP zawierającej informację `EAP-Success`, AP wysyła kolejny komunikat typu `EAP-Key`, zawierający klucz do komunikacji, zaszyfrowany i podpisany kluczem otrzymanym z serwera RADIUS. Klient po otrzymaniu tego komunikatu i odszyfrowaniu klucza definiuje używane przez siebie klucze transmisyjne. Standard 802.11i (WPA2) oraz jego poprzednik WPA implementują tzw. 4-stronny protokół potwierdzenia *(4-Way Handshake)*, służący do wygenerowania i wymiany kluczy szyfrowania między urządzeniem dostępowym oraz klientem. Protokół ten pozwala również potwierdzić, że obie strony znają główny klucz sesji (master session key). WPA/WPA2 korzysta z różnych kluczy, inicjujący materiał kryptograficzny odebrany z serwera uwierzytelniania jest wykorzystywany do utworzenia dwóch hierarchi kluczy: kluczy sparowanych *(pairwise key)* oraz grupowych *(group key)*. Pierwsza hierarchia powstaje na podstawie klucza PMK *(pairwise master key)* odebranego, gdy korzystamy z 802.1X, z serwera. Za pomocą generatora działającego na PMK i takich parametrach jak adresy fizyczne klienta, urządzenia dostępowego, liczb losowych dostarczonych przez obie strony powstaje klucz PTK *(pairwise transient key)*. PTK służy do utworzenia kolejnych trzech kluczy:

- klucza potwierdzającego *(EAPOL-key confirmation key, KCK)*, używanego w komunikatach pomocą EAPOL-key,
- klucza szyfrującego *(EAPOL-key encryption key, KEK)*, używanego do zapewnienia poufności komunikacji,
- klucza tymczasowego *(temporal key)*, używanego przez protokoły szyfrujące.

Druga hierarchia kluczy bazuje na kluczu GMK *(Group Master Key)*, będącym liczbą losową. Generator tworzy na podstawie GMK oraz innych parametrów klucz GTK *(group temporal key)*.

W czasie sesji *4-Way hanshake* klient i AP negocjują sposób kodowania danych, poprzez ustalenie kluczy w obu opisanych hierarchiach. Do transmisji danych typu unicast jest stosowane klucze parowania, klucze grupy są używane w pakietach typu broadcast/unicast.

2.3. Standardy szyfrowania

Standardy WPA oraz WPA2 zostały opracowane przez Wi-Fi Alliance w celu ochrony bezprzewodowych sieci komputerowych. Powstały w odpowiedzi na wykryte słabości poprzedniego systemu szyfrowania - WEP *(Wired Equivalent Privacy)*. WPA implementuje znaczną część standardu IEEE 802.11i, natomiast WPA2 to pełna implementacja IEEE 802.11i. WPA używa szyfrowania RC4 z dłuższym niż używany w WEP, 48-bitowym wektorem inicjującym. Drugą ważną zmianą w stosunku do WEP jest zastosowanie protokołu TKIP *(Temporal Key Integrity)*, który w trakcie użycia systemu dynamicznie zmienia klucze. WPA2 korzysta z szyfrowania AES *(Advanced Encryption Standard)* oraz CCMP *(Counter-Mode/CBC-MAC Protocol)*, charakteryzujących się dużą efektywnością – jest ono stosunkowo łatwe w implementacji, zajmuje mało pamięci, jest szybkie. WPA automatycznie generuje nowy unikatowy klucz szyfrowania dla każdego klienta, a nawet każdej ramki danych. Dzięki tym własnościom systemy WPA/WPA2 są znacząco bardziej odporne na popularne ataki polegające na przejęciu klucza transmisji. Protokoły WPA/WPA2 zapewniają znacznie lepszą niż w WEP kontrolę integralności danych, dzięki zastosowaniu bezpiecznej metody MIC *(Message Integrity Check)* zamiast CRC *(Cvclic Redundancy Check)*. MIC umieszcza w ramkach liczniki, co

dodatkowo zabezpiecza przed atakami polegającymi na ponownym wysyłaniu tych samych danych *(replay attacks)*.

WPA i WPA2 są zazwyczaj wiązane z standardem 802.1X, jednak dla urządzeń domowych i małych sieci, w których nie ma potrzeby wprowadzania specjalnych zabezpieczeń zaprojektowano tryb PSK *(Pre-Shared Key)*, zwany również osobistym (personal). Tego typu sieci dostępne są najczęściej pod synonimami WPA-PSK, WPA2-PSK, WPA-Personal, WPA2-Personal i wymagają wprowadzenia wspólnego hasła. Sieci pracujące w standardzie 802.1X i korzystające z protokołów WPA/WPA2 określane są terminami WPA-Enterprise, WPA2-Enterprise.

WPA/TKIP nigdy nie był prawdziwym standardem, był raczej czasowym rozwiązaniem wprowadzonym by szybko uporać się z zagrożeniami, jakie tworzyło używanie szyfrowania WEP. TKIP był metodą narażoną na ataki i aby nim zapobiec wprowadzono zabezpieczenie polegające na czasowym wyłączaniu aktywności radiowej po wykryciu potencjalnego zagrożenia. To zabezpieczenie było jednak samo w sobie zagrożeniem, ponieważ umożliwiało ataki typu DOS. W TKIP odkryto również inne słabości, które umożliwiały przejecie części szyfrowanej komunikacji.

WPA2/AES jest (jak na razie) wolny od wad. Wprowadza również dodatkowe mechanizmy, które znacząco poprawiają komfort pracy w sieci bezprzewodowej. Uwierzytelnianie „na zapas" oraz przechowywanie w pamięci urządzeń i klienta danych z wcześniejszego uwierzytelnienia, poprawia płynność przekazywania klienta bezprzewodowego między punktami dostepu.

3. EAP

Protokół EAP *(Extensible Authentication Protocol)* został zdefiniowany w dokumencie RFC 3748 ([2]) jako mechanizm uwierzytelniania wspierający różne metody uwierzytelniania, bez konieczności wstępnej negocjacji stosowanej metody. EAP ustala, w jaki sposób mają być wymieniane komunikaty pomiędzy klientem i urządzeniem dostępowym. Typowo EAP działa w warstwie łącza danych, nie wymaga więc adresacji IP, np. PPP *(Point-to-Point Protocol)*, IEEE 802. EAP implementuje własne techniki eliminacji powielania oraz retransmisji danych, ale opiera się na kolejności danych gwarantowanej przez niższe warstwy. Sam EAP nie wspiera fragmentacji, jest ona jednak możliwa w ramach konkretnych metod uwierzytelniania EAP. EAP jest często stosowany w sieciach bazujących na serwerze DHCP do pobierania adresów IP – w tej sytuacji klient nie może uzyskać adresu do czasu udanego uwierzytelnienia w danej sieci. Poziom bezpieczeństwa w sieciach stosujących EAP jest determinowany w dużym stopniu przez stosowany protokół uwierzytelniania. EAP pozwala, by serwer uwierzytelniania kontrolował konkretne metody uwierzytelniania, urządzenie dostępowe zajmuje się tylko opakowywaniem przesyłanych danych. Urządzenie dostępowe 802.1X może część klientów uwierzytelniać lokalnie, a pozostałych przekazywać do serwera uwierzytelniania. Jeżeli urządzenie dostępowe działa w formie pośrednika między klientem a serwerem uwierzytelniania, to jest dla niego istotny jedynie wynik uwierzytelnienia: zaakceptowany lub odrzucony (`Access-Accept` / `Access-Reject`) otrzymany z serwera uwierzytelniającego.

3.1. Metody uwierzytelniania EAP

Podstawowe metody uwierzytelniania wspierane przez EAP to:

- EAP-MD5 (Message-Digest 5)
- EAP-TLS (Transport Level Security)
- EAP-TTLS (Tunneled TLS)
- EAP-PEAP (Protected EAP)

Nowszymi i jeszcze stosunkowo mało rozpowszechnionymi metodami są:

- EAP-FAST
- EAP-PWD

3.1.1. EAP-MD5

Metoda ten został zdefiniowany w dokumencie [2] i [3]. Jest to najprostsza i najszybsza metoda EAP, dająca minimalny poziom zabezpieczenia. Danymi uwierzytelniania są nazwa użytkownika oraz hasło. EAP-MD5 chroni komunikację za pomocą tzw. odcisku palca *(fingerprint)*, napisu wygenerowanego w celu cyfrowego podpisywania pakietów, dla zapewnienia ich autentyczności. Protokół ten nie korzysta z certyfikatów PKI i z technik szyfrowania przekazywanych danych. Z powodu słabego bezpieczeństwa, jego stosowanie nie jest zalecane. Dopuszcza się używanie EAP-MD5 w sieciach przewodowych, gdzie klient jest podłączony bezpośrednio do urządzenia dostępowego i prawdopodobieństwo podsłuchu jest niewielkie.

3.1.2. EAP-TLS

Metoda ta gwarantuje silny poziom bezpieczeństwa, gdyż wymaga, by obie strony komunikacji – klient i serwer zostały zidentyfikowane za pomocą certyfikatów PKI. Sposób komunikacji definiuje RFC 5216 ([6]). Dane przekazywane w pakietach są szyfrowane. Protokół EAP-TLS jest traktowany jako skomplikowany i wymagający, ponieważ bazuje na infrastrukturze kluczy publicznych. Jednocześnie jest najczęściej implementowany. Wszyscy producenci sprzętu bezprzewodowego oraz systemów operacyjnych wspierają EAP-TLS.

3.1.3. EAP-TTLS

Metoda EAP-TTLS jest w dużym stopniu oparta na EAP-TLS. Oferuje technikę charakteryzującą się poziomem bezpieczeństwa EAP-TLS, nie wymagając jednocześnie dwustronnego uwierzytelnienia poprzez certyfikaty PKI. Jedynie serwer musi potwierdzić swoją tożsamość za pomocą certyfikatu, co znacząco zmniejsza trudności konfiguracyjne. Klient uwierzytelnia się za pomocą tradycyjnych technik, tj. poprzez podanie nazwy użytkownika i hasła. Po uwierzytelnieniu serwera za pomocą certyfikatu między serwerem a klientem jest ustanawiany bezpieczny tunel, w którym jest przeprowadzana procedura uwierzytelnienia klienta. Dane są przekazywane w szyfrowanym tunelu TLS, dlatego metoda ta gwarantuje pełne bezpieczeństwo. EAP-TTLS został opracowany przez Funk Software oraz Certicom i opisany dokumencie [7]. Jest szeroko wspierany, jednak w systemach Microsoft Windows pojawia się dopiero w najnowszej wersji – MS Windows 8. Jego stosowanie we wcześniejszych wersjach wymaga instalacji specjalnego programu klienckiego, np. SecureW2.

3.1.4. PEAP

Jest to protokół bardzo podobnej funkcjonalności do EAP-TTLS. Został zaproponowany przez firmy Microsoft, CISCO oraz RSA Security jako alternatywa EAP-TTLS. Mimo że standard powstał już po ukazaniu się EAP-TTLS, zyskał dużą popularność i jest szeroko implementowany, oczywiście również w systemach Microsoft Windows. Możliwe są dwa podtypy PEAP:

- PEAPv0/EAP-MSCHAPv2;
- PEAPv1/EAP-GTC.

PEAPv0/EAP-MSCHAPv2 to metoda popularnie zwana PEAP-em, gdyż większość użytkowników nie zdaje sobie sprawy, że istnieją dwie odmiany PEAP-a. Definicje można znaleźć w dokumencie Internet-Draft [8]. Określenie PEAPv0 dotyczy metody związanej z tożsamością zewnętrzną (widoczną na zewnątrz tunelu TLS), natomiast metoda EAP-MSCHAPv2 wiąże się z tożsamością wewnętrzną (wewnątrz tunelu). CISCO dopuszcza do obsługi wewnętrznej tożsamości oprócz EAP-MSCHAPv2 metodę EAP-SIM *(EAP for GSM Subscriber Identity)*.
PEAPv1/EAP-GTC to standard zdefiniowany przez CISCO. EAP-GTC *(Generic Token Card)* został zdefiniowany w [2]. Protokół ten przenosi tzw. wezwanie w postaci tekstu wygenerowanego przez serwer uwierzytelniania oraz odpowiedź, która powstaje na podstawie tzw. tokenu bezpieczeństwa. EAP-GTC nie chroni danych uwierzytelniania. PEAPv1 nie ma wsparcia w systemach Microsoft Windows. Protokół definiuje dokument [6].

3.1.5. EAP-FAST i TEAP

EAP-FAST jest metodą EAP zdefiniowaną w RFC-4851. Metoda jest pod wieloma względami podobna do PAEP i TTLS. Istotna różnicą jest jednak możliwość zapisania stanu bezpiecznego tunelu TLS w celu późniejszego odtworzenia. Przygotowaniem do odtworzenia stanu jest dystrybucja plików PAC (Protected Access Credentials). Takie pliki muszą być przygotowane indywidualnie dla użytkownika i ich dystrybucja jest jednym z głównych problemów EAP-FAST. Jedna z metod na dystrybucję PAC jest dystrybucja automatyczna odbywająca się w ramach pierwszego połączenia, kiedy to klient bezprzewodowy nawiązuje połączenie z użyciem identyfikatora i hasła (podobnie jak w TTLS czy PEAP), po zweryfikowaniu tożsamości klient otrzymuje plik PAC i od tego momentu może już pracować w oparciu o niego. Ogromną zaletą EAP-FAST, zwłaszcza w scenariuszach eduroam, jest fakt, że w czasie uwierzytelnienia użytkownika jest wymieniana mniejsza liczba pakietów, co znacznie skraca czas uwierzytelnienia.

Brak systemowej implementacji w systemach Microsoft oraz brak darmowego klienta, którego można by doinstalować, powoduje, ze popularnośc tej metody jest stosunkowo niewielka.

3.1.6. EAP-PWD

EAP-PWD jest zdefiniowany w RFC i wnosi do metod EAP prawdziwie nową jakość. Wszystkie inne, bezpieczne metody EAP wymagają stosowania technik kryptografii klucza publicznego. Metody tunelowe korzystają z PKI w celu zestawienia bezpiecznego tunelu, w którym transmituje się następnie dane uwierzytelniające. Proces zestawiania tunelu jest ważnym elementem bezpieczeństwa, ponieważ pozwala klientowi bezprzewodowemu na potwierdzenie, że komunikuje się z właściwym serwerem, zanim dojdzie do transmisji poufnych danych. W EAP-PWD nie ma tunelu, zamiast tego stosuje się złożone metody kryptograficzne i komunikację hasło-odzew. Obie strony muszą mieć dostęp do identycznego tokena uwierzytelniającego (np. hasła w postaci niezaszyfrowanej lub zaszyfrowanej jakąś typową metodą skrótu). W czasie komunikacji, żadna ze stron nie ujawnia informacji, która pozwoliłaby na odtworzenie tokena, ale to co przekazuje wystarcza na potwierdzenie, że dysponuje tym samym tokenem co strona przeciwna. W EAP-PWD nie ma potrzeby wstępnej weryfikacji serwera, ponieważ sam proces uwierzytelnienia klienta jest bezpieczny.

Największą zaletą EAP-PWD jest to, że proces przyłączenia do sieci nie wymaga żadnej wstępnej konfiguracji. Użytkownik wprowadza tylko identyfikator i hasło. Od strony użytkownika wygląda to zatem identycznie jak, przyłączanie do nowej sieci np. przez PEAP, przy pomocy urządzenia, które nie alarmuje o braku możliwości weryfikacji serwera. Tyle, że w przypadku PEAP-a, użytkownik naraża się na wykradzenie hasła logowania, a w przypadku EAP-PWD, nie.

Kolejną przewagą EAP-PWD jest niewielka liczba pakietów niezbędnych do dokonania uwierzytelnienia, do jest szczególnie istotne w eduroam, gdzie pakiety muszą często przebywać daleką drogę.

W przypadku typowych metod EAP klient weryfikuje tożsamość serwera na podstawie przedstawionego certyfikatu, natomiast w EAP -PWD tylko poprzez identyczność tokena. W szczególności klient nie może odróżnić serwerów, o ile na wszystkich ma takie samo hasło. Można to uważać za wadę, ale wydaje się, aby w środowisku eduroam mógł to być istotny problem.

Drugą wadą EAP-PWD jest brak odpowiednika tożsamości anonimowej. Identyfikator użytkownika musi być przekazywany w sposób jawny. W eduroam zwraca się dużą uwagę na ochronę prywatności użytkowników, a zatem ta cecha EAP-PWD może być uznana za istotniejszą wadę.

4. Serwer RADIUS

Serwery uwierzytelniania, z którymi kontaktują się urządzenia dostępowe zazwyczaj korzystają z protokołu RADIUS *(Remote Authentication Dial In User Service)*, zdefiniowanego w RFC 2865 ([3]). RADIUS realizuje funkcje uwierzytelniania, autoryzacji i rozliczania *(authentication, autorization, accounting)*. Wprowadzenie standardu 802.1X wpłynęło na rozszerzenie specyfikacji RADIUS, tak by był wspierany protokół EAP (RFC 3579, [4]). Komunikaty RADIUS są przenoszone w datagramach UDP. Składają się z typu komunikatu (`Access-Reqeust`, `Access-Challenge`, `Access-Response`), numeru sekwencyjnego, rozmiaru danych, pola `Authenticator` oraz serii par typ atrybutu – wartość. Pole `Authenticator` gwarantuje integralność komunikacji między urządzeniem do-

stępowym a serwerem RADIUS oraz pozwala ukryć przed urządzeniem dostępowym hasło użytkownika. Dostęp do hasła uzyskuje wyłącznie serwer przeprowadzający procedurę uwierzytelniania. Istotną funkcjonalnością serwerów RADIUS jest możliwość przekazywania otrzymanych danych do kolejnego serwera. W tej sytuacji serwer RADIUS, z którym kontaktuje się urządzenie dostępowe występuje w roli pośrednika *(proxy)*. Właściwe uwierzytelnienie jest realizowane poprzez inny serwer, do którego dotrze dane zlecenie. Między urządzeniem dostępowym a serwerem RADIUS, który realizuje właściwą funkcję uwierzytelnienia może znajdować się wiele serwerów RADIUS.

Serwery RADIUS realizują uwierzytelnienie użytkowników tylko wówczas, jeżeli domena, do której należy dany użytkownik jest obsługiwana przez ten serwer. Pozostałe zlecenia są albo odrzucane, albo przekazywane do innych serwerów.

5. Identyfikator użytkownika

W procesie uwierzytelnienia klienta wykorzystywane są dostarczone przez klienta dane uwierzytelniania. Jest to przede wszystkim identyfikator użytkownika, przekazany przez klienta w odpowiedzi na wezwanie AP do zaprezentowania danych uwierzytelniania. Towarzyszy mu, w zależności od stosowanej metody EAP, albo hasło użytkownika, albo certyfikat kliencki.

Identyfikator użytkownika, zgodnie z RFC 2865 ma postać identyfikatora sieciowego *(network access identifier)*, zdefiniowanego w dokumencie RFC 4282 ([11]), czyli jest to nazwa użytkownika (username) lub nazwa użytkownika połączona znakiem @ z nazwą domeny (`user@realm`) – w tym drugim przypadku, nazwa użytkownika może być pustym ciagiem.

Serwer uwierzytelniający, po odbiorze z urządzenia dostępowego pakietu zawierającego identyfikator użytkownika, podejmuje decyzję, czy jest w stanie sam obsłużyć zlecenie, czy musi przekazać pakiet dalej, do kolejnego serwera RADIUS.

Na tej funkcjonalności standardu 802.1X bazuje usługa eduroam. Jeśli w obrębie sieci eduroam pojawia się obcy użytkownik, dysponujący uprawnieniami w instytucji stowarzyszonej w eduroam, urządzenie dostępowe, jak zwykle przekazuje zlecenie identyfikacji do lokalnego serwera RADIUS. Ten, po analizie identyfikatora użytkownika, uzna, że nie może sam przeprowadzić procesu potwierdzenia tożsamości, dlatego przekaże zlecenie do innego serwera RADIUS. Sposób przekazywania zleceń wynika z definicji obsługi domen na danym serwerze. Obecnie większość konfiguracji eduroam opiera się na hierarchicznym układzie serwerów RADIUS. Jeśli, np. lokalny serwer obsługuje domenę `man.poznan.pl`, to w swojej konfiguracji musi określać, gdzie mają być kierowane zapytania dotyczące innych domen.

Należy pamiętać, że w przypadku takich protokołów uwierzytelniania jak EAP-TTLS oraz PEAP, na zewnątrz bezpiecznego tunelu jest przenoszona tzw. tożsamość zewnętrzna (outer identity), która nie musi być taka sama, jak tożsamość wewnętrzna. Wymagane jest, by tożsamość zewnętrzna reprezentowała użytkownika w tej samej domenie, w przeciwnym razie zlecenie nie może dotrzeć do właściwego serwera. Tożsamość zewnętrzna decyduje, który serwer RADIUS będzie realizował uwierzytelnienie klienta.

6. Bezpieczeństwo w standardzie 802.1X

Standard 802.1X może wyeliminować podstawowe zagrożenia w sieciach komputerowych. Stopień bezpieczeństwa zależy od stosowanych konkretnych metod uwierzytelniania, działających w oparciu o protokół EAP. Następujące zagrożenia mogą być eliminowane lub minimalizowane w tego typu konfiguracjach:

1. **Atak słownikowy**: polegający na próbie złamania haseł na podstawie obserwacji wymiany komunikatów pomiędzy klientem a urządzeniem dostępowym. Jeśli razem ze standardem 802.1X używamy tunelu TLS, to dane uwierzytelniania użytkownika (np. nazwa użytkownika i hasło) są chronione, gdyż ich przekazywanie odbywa się w postaci zaszyfrowanej.
2. **Atak przejęcia sesji**: atakujący przejmując pakiety wymieniane w komunikacji klient – urządzenie dostępowe, pobiera dane o tożsamości klienta, następnie podszywa się pod niego i kontynuuje komunikację. Mechanizm wymiany kluczy stosowany w opisanych w p. meto-

dach szyfrowania gwarantuje wystarczająco częstą ich modyfikację, by niebezpieczeństwo zostało zminimalizowane.

3. **Atak typu „man-in-the-middle”**: atakujący czyta i modyfikuje komunikację pomiędzy dwoma stronami, bez ich wiedzy. Podobnie jak w p. 2, stosowane metody szyfrowania minimalizują możliwość wykorzystania informacji zawartej w pakiecie. dodatkowo szyfrowanie komunikacji uniemożliwia podejrzenie i modyfikację jej treści.

Ataki wykorzystujące brak techniki Channel Binding w metodach EAP. Problemy opisane w drafcie internetowym [] dotyczą praktycznie wszystkich stosowanych rozwiązań. Standardowo wykorzystywane metody EAP, powiązane z 802.1X dają użytkownikowi pewność, że dane logowania nie zostaną ujawnione, pozwalają również potwierdzić, że łączy się do sieci, która jest uwierzytelniana przez jego serwer macierzysty. Brak Channel-Binding nie pozwala jednak na uzyskanie pewności, że sieć do której łączy się użytkownik jest obsługiwana przez konkretnego operatora.

W kontekście eduroam, zagrożenia wynikające z braku Channel-Binding, pojawijają się głównie w sytuacjach, kiedy eduroam jest stosowany jako sieć tylko dla gości, niejako „obok” głównej sieci bezprzewodowej danej instytucji. Przyjmijmy dosyć typowy scenariusz, w którym instytucja **A** zdefiniuje dwie sieci o SSID: **eduroam** oraz **siec_wewnetrzna_A** i będzie korzystała w obu z nich z tych samych parametrów łączności (tzn. w obu przypadkach użytkownik będzie korzystał z tego samego serwera RADIUS i tych samych danych uwierzytelniających). Przyjmijmy również, że administratorzy poinformowali użytkowników, że połączenie do sieci **siec_wewnetrzna_A** gwarantuje, że ich ruch jest ruchem wewnętrznym instytucji **A**, a zatem nie może zostać podsłuchany. Jeżeli w innej instytucji podłączonej do eduroam ktoś uruchomi SSID **siec_wewnetrzna_A** i przekieruje uwierzytelnienia zwykła droga eduroam, to użytkownik instytucji **A** uzyska połaczenie do tej sieci i może błędnie uważać, że jego ruch jest bezpieczny. Technika Channel-Binding pozwoliłaby na zweryfikowanie, faktu, że użytkownik łączy się z niewłaściwą siecią.

Innym potencjalnym zagrożeniem jest niepoprawna metoda konfigurowania tuneli w metodach takich jak TTLS, czy PEAP. W tym przypadku, identyfikator zewnętrzny, służący do prawidłowego kierowania pakietu do instytucji macierzystej może być inny od wewnętrznego. może się zdarzyć (i takie efekty były obserwowane w eduroam), że część domenowa (realm) identyfikatora wewnętrznego, może wskazywać na inny serwer macierzysty i w takiej sytuacji może dojść do przekierowania niezaszyfrowanych danych identyfikacyjnych użytkownika przez sieć zewnętrzną. pomimo że taki problem wpada w grupę zagadnień Channel Binding, to da mu się prosto zaradzić odpowiednia konfiguracją serwera RADIUS.

Niestety Channel Binding jest stosunkową nowością. prawdopodobnie nie zostanie wprowadzone do powszechnych obecnie metod EAP i trzeba będzie poczekać na opracowanie i spopularyzowanie się nowej metody TEAP.

7. Implementacje

Systemy Windows począwszy od XP domyślnie obsługują standard 802.1X w odniesieniu do dowolnych połączeń sieciowych. Windows 2000 wymagał instalacji poprawki *(service pack)*. Producenci kart bezprzewodowych dawniej bardzo często dostarczali własne oprogramowanie 802.1X. Obecnie, obsługa systemowa jest już na tyle dobra, że producenci zazwyczaj ograniczają się do przygotowania sterowników.

Przez jakiś czas prowadzone były prace nad wielosystemowym klientem 802.1X o nazwie Open1X. Oprogramowanie było rozwijane jako Open Source, ale prace zostały zarzucone.

Systemy Mac OS od wersji 10.3 implementują 802.1X. iPhone oraz iPod Touch wymagają oprogramowania w wersji 2.0, udostępnionego w czerwcu 2008. W aktualnych wersjach systemów Mac OS i iOS wsparcie dla 802.1X jest bardzo dobre.

W aktualnych dystrybucjach systemu Linux, jedynym klientem bezprzewodowym jest `wpa_supplicant` wspierający bardzo wiele metod metod EAP. `wpa_supplicant` na ogół pracuje w tle, a dostęp do niego zapewnia oprogramowania konfiguracyjne takie jak Network Manager czy WiCd.

System Android wspiera 802.1X, chociaż można zgłaszać pewne zastrzeżenia odnośnie systemu zabezpieczeń.

Telefony komórkowe pracujące pod systemem operacyjnym Symbian wspierają WPA i WPA2.

W ramach projektu GN3 przygotowywane jest narzędzie wspomagające konfigurację 802.1X na urządzeniach klienckich. Uruchomienie tego systemu w europejskim projekcie eduroam będzie niewątpliwie dużym ułatwieniem przy wdrażaniu nowych sieci i wsparciu dla już istniejących.

Materiały towarzyszące

[1] *802.1X-2004 – Port Based Network Access Control*, http://www.ieee802.org/1/pages/802.1x-2004.html

[2] *Extensible Authentication Protocol*, RFC 3748, http://tools.ietf.org/html/rfc3748

[3] *The Remote Authentication Dial In User Service (RADIUS)*, RFC 2865, http://tools.ietf.org/html/rfc2865

[4] *RADIUS (Remote Authentication Dial In User Service Support For Extensible Authentication Protocol (EAP)*, RFC 3579, http://tools.ietf.org/html/rfc3579

[5] *PPP Challenge Handshake Authentication Protocol (CHAP)*, RFC 1994, http://tools.ietf.org/html/rfc1994

[6] *The EAP-TLS Authentication Protocol*, RFC 5216, http://tools.ietf.org/html/rfc5216

[7] *EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0)*, Internet-Draft, http://tools.ietf.org/html/draft-funk-eap-ttls-v0-04

[8] *Microsoft's PEAP version 0 (Implementation in Windows XP SP1)*, http://tools.ietf.org/id/draft-kamath-pppext-peapv0-00.txt

[9] *Protected EAP protocol (PEAP) Version 2*, http://tools.ietf.org/id/draft-josefsson-pppext-eap-tls-eap-10.txt

[10] *Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)*, http://tools.ietf.org/html/rfc3079

[11] Network Access Identifier, RFC 2486, http://tools.ietf.org/html/rfc2486