

Konceptcja uczelnianej sieci bezprzewodowej włączonej w strukturę eduroam

Tomasz Wolniewicz, UCI UMK (twoln@umk.pl)

Maja Górecka-Wolniewicz, UCI UMK (mgw@umk.pl)

Zbigniew Oltuszyk, PCSS (zbigniew.oltuszyk@man.poznan.pl)

dokument przygotowany w ramach projektu B-R eduroam-PIONIER

wersja 1.0

Spis treści

1. Wstęp.....	1
2. Funkcje sieci uczelnianej.....	1
3. WPA-Enterprise w użytkowaniu.....	2
4. Zarządzanie siecią uczelnianą.....	2
5. Ochrona bezprzewodowej sieci uczelnianej.....	3
6. Dwa modele sieci uczelnianej współpracującej z eduroam.....	4
6.1. Model I – eduroam jako główna sieć uczelni.....	4
6.2. Model II – eduroam jako sieć tylko dla gościnnego dostępu.....	4
7. Konceptcje wdrożenia sieci uczelnianej.....	5
7.1. System uwierzytelniający.....	5
7.1.1. TTLS/PAP.....	5
7.1.2. PEAP/MSCHAPv2.....	6
7.1.3. TLS.....	6
7.1.4. Identyfikowanie użytkowników przy pomocy atrybutu Chargeable-User-Identity.....	6
7.2. Implementacja modelu I.....	7
7.2.1. Sieć konferencyjna.....	7
7.2.2. Sieć eduroam.....	7
7.2.3. Problem nakładania się zasięgów.....	8
7.2.4. Stosowanie lokalnych VLAN-ów.....	8
7.3. Implementacja modelu II.....	8
7.3.1. Sieć konferencyjna.....	8
7.3.2. Sieć lokalna.....	8
7.3.3. Sieć eduroam.....	9
8. Organizacja gościnnego dostępu w ramach eduroam.....	9
9. Urządzenia na potrzeby sieci uczelnianej.....	9

1. Wstęp

Niniejszy dokument powstał na podstawie doświadczeń i przemyśleń związanych z wdrażaniem uczelnianych sieci bezprzewodowych włączonych w strukturę eduroam. Rezultatem są dwie koncepcje sieci, w których usługa eduroam pojawia się w różnych rolach. Obydwie koncepcje mają wady i zalety. To, na której z nich wzorować wdrożenie musi zależeć od lokalnych uwarunkowań.

2. Funkcje sieci uczelnianej

Sieć uczelniana na ogół spełnia dwie podstawowe funkcje:

- sieć dla pracowników i studentów uczelni musi być rozgłaszana, musi być zabezpieczona, nie może stosować wspólnych kluczy ani budowania reguł dostępu na podstawie adresu MAC; zazwyczaj stosowane rozwiązania to: portal dostępowy, ograniczenie wyjścia do VPN, WPA/WPA2-Enterprise;

- sieć gościnna na potrzeby konferencji – musi być rozgłaszana, może być nieszyfrowana, ale zabezpieczona portalem WWW lub szyfrowana i zabezpieczona wspólnym kluczem (WPA-PSK).

W niniejszym opracowaniu przedstawimy koncepcję sieci uczelnianej opartej o WPA-Enterprise, współpracującej z usługą eduroam i równocześnie realizującej potrzeby sieci konferencyjnej.

3. WPA-Enterprise w użytkowaniu

Panuje przekonanie, że wdrożenie i użytkowanie sieci w standardzie WPA-Enterprise jest trudne.

Najtrudniejszym elementem jest wsparcie użytkowników przy instalacji dostępu do sieci. Kilkuletnie doświadczenia z Uniwersytetu Mikołaja Kopernika wskazują, że nawet dobrze przygotowane pakiety instalacyjne i szczegółowe instrukcje nie są w stanie zastąpić bezpośredniego kontaktu z użytkownikiem, a w wielu przypadkach okazuje się niezbędne zainstalowanie sieci przez pracownika wsparcia informatycznego.

O ile etap pierwszego podłączenia do sieci jest bez wątpienia bardziej kłopotliwy niż w przypadku sieci zabezpieczonej portalem WWW, to użytkowanie takiej sieci na co dzień jest zdecydowanie łatwiejsze. Użytkownik uruchamia urządzenie i po chwili jest w sieci. To, że nie ma potrzeby logowania się do portalu jest szczególnie wygodne, jeżeli korzysta się z małych urządzeń, takich jak palmtopy, czy telefony dwusystemowe.

Ponieważ sieć korzystająca z WPA-Enterprise uwierzytelnia klienta przed dopuszczeniem go do sieci, to uważa się zazwyczaj, że administrator ma pełną kontrolę nad użytkownikami. Trzeba sobie jednak zdawać sprawę, że uwierzytelnienie dotyczy wyłącznie adresu MAC, a nie adresu IP. Jeżeli użytkownik korzysta z własnoręcznie ustawionego adresu IP, który należy do podsieci obsługiwanej przez dany punkt dostępowy i ten adres nie powoduje konfliktu z innym użytkownikiem, to system może nie odnotować, że użytkownik korzysta z tego adresu. W szczególności poleganie wyłącznie na logach serwera DHCP jest niewystarczające. (W opracowaniu [Zapobieganie samowolnej zmianie IP](#) [1] opisano jeden ze sposobów rozwiązania tego problemu.)

4. Zarządzanie sieciami uczelnianymi

Tradycyjnie, ośrodki obsługi informatycznej na uczelniach zatrudniały bardzo kompetentnych pracowników, którzy często preferowali tworzenie własnego oprogramowania zarządzającego, zamiast stosowania gotowych (często drogich) zakupionych rozwiązań. Ta sytuacja ostatnio się zmienia, utrzymanie kadry informatycznej staje się coraz trudniejsze i coraz droższe, a zmiany pracowników są coraz częstsze. Dlatego stosowanie gotowych rozwiązań jest dużo prostsze, a często również tańsze.

Sieci bezprzewodowe można budować albo w technologii tzw. grubego punktu dostępowego, czyli autonomicznych urządzeń dostępowych o stosunkowo dużej funkcjonalności, albo kontrolera i cienkiego punktu dostępowego. W tym drugim przypadku, punkt dostępowy nie jest w stanie pracować samodzielnie, praktycznie cała obsługa połączenia jest realizowana na kontrolerze.

Kontroler jest stosunkowo drogim urządzeniem o bardzo rozbudowanej funkcjonalności (z reguły znacznie większej niż dostępna w autonomicznych punktach dostępowych). Niektóre funkcje, takie jak automatyczna konfiguracja całej sieci, automatyczne uzupełnianie braków (popsutych punktów dostępowych), czy geograficzna lokalizacja użytkowników, są użyteczne tylko w sieciach, w których liczba punktów radiowych została zaplanowana z dużym zapasem. Należy przypuszczać, że sieci uczelniane nie będą na razie budowane z takim zapasem, więc nie można oczekiwać, że te rozbudowane możliwości kontrolerów będą przydatne.

Wiele funkcji kontrolera, związanych ze scentralizowanym zarządzaniem siecią daje się realizować również w technologii grubego punktu dostępowego stosując odpowiednie skrypty automatyzujące podstawowe zadania. Nakład pracy na przygotowanie takich skryptów jest dosyć duży, ale osiągnięty efekt może być zupełnie satysfakcjonujący.

Bardzo mocno nagłaśnianą przewagą systemów kontrolerowych nad systemami grubych punktów dostępowych jest możliwość płynnego przekazywania użytkowników od jednego punktu dostępowego do kolejnego. W przypadku grubego punktu dostępowego takie przejście wymaga ponownego uwierzytelnienia. Taki proces trwa zazwyczaj pod 2 do 3 sekund. Przechodzenie pomiędzy punktami dostępowymi może następować samoczynnie, nawet w sytuacji, kiedy użytkownik nie prze-

mieszczą się – zmieniające się warunki, np. zwiększająca się liczba użytkowników jednego z punktów, a niekiedy po prostu wadliwe oprogramowanie karty, mogą wymusić zmianę punktu dostępowego przez kartę sieciową użytkownika. Niekiedy zmiany są na tyle częste, że powodują wyraźną degradację jakości dostępu do sieci. W przypadku technologii cienkiego punktu dostępowego, kontroler ma wszystkie informacje dotyczące powiązania klienta i, zgodnie z zapewnieniami producentów, jest w stanie obsłużyć przełączenie bez ponownego uwierzytelnienia. Przeprowadzane testy wskazują, że kwestia przełączania jest zazwyczaj znacznie bardziej skomplikowana niż jest to opisywane w dokumentacji urządzeń. Więcej na ten temat piszemy w części 9.

Standard WPA2 wprowadził rozszerzenia ułatwiające przełączanie klientów, np. uwierzytelnienie wstępne, kiedy komputer użytkownika rejestruje się we wszystkich widzianych punktach dostępowych, tak by późniejsze przejście nie powodowało przerwy w transmisji. Na razie WPA2 nie jest jednak jeszcze dostatecznie powszechnie stosowany, a ponadto możliwość stosowania uwierzytelnienia wstępnego zależy od oprogramowania po stronie użytkownika. Z tych powodów płynność przejścia powinna być w miarę możliwości realizowana po stronie urządzeń dostępowych, co jest możliwe tylko przy systemach zarządzanych kontrolerem. Przed zakupieniem systemu należy się jednak upewnić, czy deklarowana płynność przełączania jest rzeczywiście realizowana przy takich ustawieniach sieci, z jakich zamierzamy korzystać.

Rozważając systemy kontrolerowe należy zdawać sobie sprawę z tego, że cały ruch generowany za pośrednictwem punktów dostępowych przechodzi przez interfejs kontrolera. Projektując taką sieć należy rozważyć, jaka liczba kontrolerów będzie optymalna.

Trudno przesądzić, jaki model jest właściwszy, podejmując decyzję trzeba wziąć pod uwagę m. in. poziom kompetencji administratorów, wielkości sieci, oszacować proporcje kosztów między zakupem bardziej zaawansowanego rozwiązania a wydatkami na czas pracy potrzebny do zbudowania oprogramowania obsługującego prostszy system itd. Sugerujemy jednak, aby przy składaniu wniosków inwestycyjnych na budowę sieci ogólnouczelnianych brać pod uwagę przede wszystkim systemy zarządzane przez kontroler.

5. Ochrona bezprzewodowej sieci uczelnianej

Kontrolerowe systemy zarządzania urządzeniami bezprzewodowymi często są wyposażone w rozbudowane systemy zabezpieczeń – firewalle, systemy IPS itp. Coraz częściej mówi się również o technologii NAC (Network Access Control), dzięki której, przed dołączeniem do sieci, komputer może być sprawdzany pod kątem aktualności systemu, oprogramowania antywirusowego itp. Projektując sieć uczelnianą warto rozważyć sensowność stosowania rozbudowanych (i często drogich) zabezpieczeń, wobec specyfiki użytkowników, dla których sieć jest przeznaczona. Sieć uczelniana nie jest typową siecią korporacyjną, do której łączą się tylko komputery służbowe skonfigurowane i monitorowane przez działy IT. W sieciach uczelnianych przeważają prywatne komputery użytkowników, nad którymi administratorzy nie mają żadnej władzy i, do których zazwyczaj nie stosują się posiadane przez uczelnię licencje na oprogramowanie.

W sieci bezprzewodowej nie umieszcza się żadnych usług, a zatem ochrona tej sieci na wejściu służy tylko ochronie przenośnych komputerów użytkowników. Komputery przenośne są podłączane nie tylko do sieci uczelni, ale również w wielu innych, zazwyczaj zupełnie nie zabezpieczonych lokalizacjach. Komputer użytkownika jest narażony na tyle ataków, że chronienie go akurat w sieci uczelnianej mija się z celem.

Ochrona sieci na wejściu jest i tak niewystarczająca, bo wewnątrz sieci działają potencjalnie niebezpieczne komputery użytkowników. Urządzenia sieci bezprzewodowej mają wprawdzie opcje blokowania ruchu pomiędzy użytkownikami tej sieci, ale włączenie takiej ochrony zablokuje np. telefonię internetową między użytkownikami lokalnej sieci bezprzewodowej.

Ponieważ użytkownicy sieci bezprzewodowej korzystają z adresów należących do uczelni, to uzasadnione jest wprowadzanie filtrów na wyjściu z sieci np. uniemożliwiających rozsyłanie spamu. W przypadku podsieci udostępnianej użytkownikom lokalnym zabezpieczenia mogą być bardziej restrykcyjne niż w przypadku gości, ponieważ użytkownik lokalny powinien korzystać z większości usług wewnątrz własnej sieci, podczas gdy dla gościa kluczowy jest dostęp do usług w jego sieci macierzystej. Z tego powodu *Polska Polityka eduroam* [2] sugeruje, by w sieci przeznaczonej dla gości nie stosować żadnych blokad oraz specyfikuje listę portów, które MUSZĄ pozostawać otwarte. Su-

gerujemy, aby stosować serwer proxy dla protokołu SMTP, który nie blokując możliwości łączenia się z dowolnym serwerem SMTP, potrafi odfiltrować ruch generowany przez robaki internetowe.

6. Dwa modele sieci uczelnianej współpracującej z eduroam

6.1. Model I – eduroam jako główna sieć uczelni

W tym rozwiązaniu wszyscy użytkownicy korzystają z sieci o SSID eduroam. Podstawową zaletą takiego podejścia jest to, że daje ono stosunkowo wysoką gwarancję, że użytkownik będzie gotowy do korzystania z sieci we wszystkich lokalizacjach eduroam na świecie.

To podejście jest jednak obciążone również wadami, które należy brać pod uwagę:

1. Sieć powinna korzystać z szyfrowania WPA/TKIP, tak by zapewnić najwyższą możliwą kompatybilność z innymi lokalizacjami eduroam na świecie, WPA2/AES w ogóle nie powinno być włączane, gdyż w takiej sytuacji pierwsze połączenie klienta do sieci zazwyczaj konfiguruje właśnie ten bardziej zaawansowany sposób szyfrowania, utrudniając dostęp do innej sieci eduroam. Wynika z tego że, późniejsze przejście na standard WPA2 będzie mocno utrudnione.
2. Użytkownik sieci na terenie macierzystej instytucji zazwyczaj czuje się bardziej bezpieczny niż w czasie, gdy jest gościem. Jeżeli kilka instytucji w jednym mieście korzysta z SSID-a eduroam, to w niektórych obszarach użytkownik może nie wiedzieć, czy podłączył się do sieci swojej instytucji macierzystej, czy jakiejś sieci gościnnej.
3. W sytuacji, kiedy zasięgi sieci dwóch instytucji zachodzą na siebie może występować przełączanie użytkownika między sieciami i związana z tym konieczność zmiany adresu IP – jeżeli takie przełączenia występują często, to mogą całkowicie uniemożliwić płynne korzystanie z sieci.
4. Oddzielenie ruchu gości od ruchu własnych użytkowników wymaga stosowania urządzeń, które przydzielają użytkownika do VLAN-u w sposób dynamiczny (na podstawie informacji przesłanej przez serwer RADIUS).

Przedstawione problemy (1), (2) w przyszłości mogą zostać rozwiązane poprzez odpowiednie oprogramowanie klienckie. Z najbardziej uciążliwym problemem (1) oprogramowanie wpa_supplicant radzi sobie już teraz, podobnie jest z oprogramowaniem na telefonach firmy Nokia, bardzo obiecujący jest projekt OpenSea (<http://www.openseaalliance.org/>). Pomimo niewygodny jaką sprawia instalowanie dodatkowego oprogramowania, na razie będzie to przypuszczalnie niezbędne. Problem (2) mógłby zostać obsłużony przez odpowiedni system sygnalizacji, to zagadnienie było omawiane w ramach projektu JRA5¹, ale konkretne rozwiązanie nie zostało zaproponowane. Problem (3) jest prosty do rozwiązania przy odpowiedniej współpracy instytucji i będzie omówiony poniżej. (4) nie jest właściwie problemem, tylko wymogiem w stosunku do urządzeń, który w bardziej zaawansowanych rozwiązaniach jest zawsze spełniony.

6.2. Model II – eduroam jako sieć tylko dla gościnnego dostępu

W tej sytuacji SSID eduroam jest uruchamiany tylko na potrzeby dostępu gościnnego, w szczególności separacja ruchu gości od ruchu własnych użytkowników może być zrobiona poprzez statyczne przypisanie VLAN-u do SSID-a. Dodatkową zaletą tego rozwiązania jest wyeliminowanie wszystkich wad rozwiązania poprzedniego. Trzeba jednak zdawać sobie sprawę, że użytkownik, który korzysta z dostępu lokalnego poprzez lokalny SSID, a w innych lokalizacjach z dostępu gościnnego poprzez SSID eduroam musi używać dwóch profili sieciowych. Na terenie instytucji macierzystej obydwa profile będą aktywne i to, jaki zostanie użyty będzie zależał od ustawienia priorytetów. Ponieważ, np. w oprogramowaniu MS-Windows, priorytety zmieniają się dynamicznie, to użytkownik może nie zauważyć, że będąc na terenie instytucji macierzystej w istocie korzysta z dostępu gościnnego, a zatem jest w sieci niezauwanej, bez dostępu do części usług. Poprawne korzystanie z tego rozwiązania wymaga zatem pewnej kontroli ze strony użytkownika.

Najważniejszą wadą modelu II są kłopoty przy korzystaniu z dostępu gościnnego – profil dla eduroam musi być skonfigurowany oddzielnie, a użytkownik, który zazwyczaj korzysta z sieci na

1 JRA5 – Joint Research Activity 5 – jedno z zadań badawczo-rozwojowych projektu GEANT2.

terenie swojej instytucji, z pewnością nie zadba o to, by konfigurację eduroam przygotować z góry, kiedy ma prosty dostęp do wsparcia. W efekcie, znajdując się na terenie obcej instytucji, gdzie eduroam jest dostępny, nie będzie potrafił z niego skorzystać.

7. Koncepcje wdrożenia sieci uczelnianej

Najprostszym modelem jest jednolita sieć dla całej uczelni zarządzana przez jeden serwer RADIUS, w której użytkownicy są umieszczani w tym samym VLAN-ie niezależnie od miejsca, w którym się łączą. Wskażemy jednak również przypadki, kiedy konfiguracja powinna być bardziej złożona.

Decyzja czy projektowana sieć będzie budowana w technologii grubego, czy cienkiego punktu dostępowego ma stosunkowo niewielki wpływ na projekt. Istotnym kryterium przy wyborze typu rozwiązania powinien być planowany sposób propagacji VLAN-ów w sieci uczelnianej. W technologii cienkiego punktu dostępowego VLAN-y muszą łączyć kontrolery, w przypadku grubego punktu dostępowego, VLAN-y trzeba doprowadzić bezpośrednio do punktów dostępu. W technologii cienkiego punktu dostępowego łączność między kontrolerem i punktem dostępowym może zazwyczaj być realizowana w trzeciej warstwie, co pozwala na implementację sieci bez żadnej ingerencji w strukturę sieci lokalnych.

Zakładamy, że ruch gości musi się odbywać w innym VLAN-ie niż ruch użytkowników lokalnych. Separowanie ruchu pracowników od ruchu studentów może być przydatne, ale nie jest przez nas przyjmowane jako niezbędne.

Rozważymy również rozwiązanie, w którym planuje się przypisywanie części użytkowników w niektórych miejscach do specjalnych VLAN-ów.

7.1. System uwierzytelniający

W sieciach WPA-Enterprise niezbędny jest serwer RADIUS². Z powodu dostępności i kosztów najczęściej używane oprogramowanie to: FreeRADIUS (na licencji GPL) oraz Microsoft IAS (składnik systemów Windows Server 2003 i nowszych). W sieciach opartych o systemy Microsoft i korzystających z Active Directory najbardziej naturalnym jest zastosowanie IAS, w sieciach unixowych stosuje się zazwyczaj oprogramowanie FreeRADIUS.

Serwer RADIUS zazwyczaj współpracuje z zewnętrzną bazą użytkowników. FreeRADIUS bardzo łatwo daje się skonfigurować do współpracy zarówno z bazą relacyjną, LDAP-em, czy też szczególną jego odmianą Active Directory³.

Serwer RADIUS powinien być zdublowany.

Proces uwierzytelnienia jest realizowany przy pomocy protokołu EAP. Sam EAP jest w zasadzie tylko protokołem ramowym, a właściwe uwierzytelnienie korzysta z jednej z metod EAP. Poniżej omówimy trzy, które są najczęściej stosowane.

7.1.1. TTLS/PAP

Ten typ uwierzytelniania wymaga podania przez użytkownika identyfikatora oraz hasła. Hasło jest przesyłane stworzonym wcześniej tunelem TLS. Na etapie zestawiania połączenia TLS oprogramowanie użytkownika ma możliwość sprawdzenia certyfikatu, którym przedstawia się serwer. Oprogramowanie na komputerze użytkownika powinno zablokować możliwość przesłania danych do niewłaściwego serwera. EAP-TTLS pozwala na ustawienie dwóch identyfikatorów użytkownika: *zewnętrznego*, widocznego dla wszystkich serwerów pośredniczących oraz *wewnętrznego*, przesyłanego w tunelu TLS i widocznego tylko dla końcowego serwera RADIUS. Dzięki tej metodzie użytkownik może pozostać anonimowy dla wszystkich instancji pośredniczących. Ponieważ hasło jest przysyłane w swojej oryginalnej wersji, to TTLS/PAP nadaje się do uwierzytelniania w systemach przechowujących hasła użytkownika w postaci skrótów Crypt lub MD5 (systemy Uniksowe). Wada

² Niektóre systemy kontrolerowe nie wymagają zewnętrznego serwera RADIUS, łącząc się od razu z odpowiednią bazą użytkowników, nie będziemy tego przykładu rozważać oddzielnie, ponieważ koncepcyjnie odpowiada on serwerowi RADIUS wbudowanemu w kontroler.

³ Szczegółowe instrukcje konfigurowania serwera FreeRADIUS zostały przygotowane w opracowaniu [3]

EAP-TTLS jest to, że nie jest powszechnie wspierany (brakuje go w oprogramowaniu Windows, a również w systemie Symbian dla telefonów komórkowych). W systemach Windows można zainstalować bardzo dobry, darmowy dodatek SecureW2 (<http://www.securew2.com>), który zapewnia pełną obsługę EAP-TTLS. SecureW2 można wstępnie skonfigurować i przez to bardzo ułatwić instalację i konfigurację sieci.

7.1.2. PEAP/MSCHAPv2

Jest to najbardziej powszechna metoda EAP wspierana w praktycznie wszystkich systemach operacyjnych. PEAP jest bardzo podobny do TTLS, z tym, że w tunelu TLS zazwyczaj stosuje się metodę uwierzytelnienia MSCHAPv2. MSCHAP wymaga, aby po stronie serwera dostępne było albo hasło w postaci otwartej, albo tzw. NT-hash. PEAP dopuszcza stosowanie odrębnego identyfikatora zewnętrznego, ale systemowa implementacja dostarczana w MS-Windows (zarówno XP jak i Vista) nie daje takiej możliwości. Stosowanie PEAP jest najbardziej naturalne w sytuacji, gdy system kont stosowany w instytucji uwierzytelniającej jest oparty o MS-Windows i Active Directory, ale PEAP można również stosować w systemach Linux przechowując kopie haseł w postaci NT-hash. Należy pamiętać, że PEAP w wydaniu MS-Windows naraża prywatność użytkownika poprzez ujawnianie jego właściwego identyfikatora. Bardzo dużą wadą PEAP jest to, że pod Windows XP uruchomienie tej metody wymaga dosyć skomplikowanych czynności. W Windows Vista PEAP jest domyślną metodą EAP i dla użytkownika jest z całą pewnością najprostszy. Ta prostota ma jednak wadę – stosunkowo łatwo można zmylić użytkownika podstawiając fałszywą sieć i spowodować, aby się w niej uwierzytelniał.

7.1.3. TLS

Ta metoda EAP korzysta z indywidualnego certyfikatu użytkownika. Jest wspierana we wszystkich testowanych systemach operacyjnych, chociaż zainstalowanie certyfikatu indywidualnego w Windows Mobile wymaga dodatkowego oprogramowania. W Windows XP TLS jest domyślną metodą EAP i przy odpowiednio skonstruowanym certyfikacie korzystanie z sieci nie wymaga od użytkownika praktycznie żadnego działania. W Windows Vista używanie TLS-a jest niemal tak samo proste. Warunkiem bezproblemowej konfiguracji EAP-TLS jest to, by certyfikat użytkownika był wystawiony dla podmiotu, którego nazwa zawiera atrybut CN o wartości identycznej, jak nazwa użytkownika w połączeniu. Stosowanie certyfikatów wystawionych dla inaczej skonstruowanych podmiotów jest możliwe, ale wymaga pewnych dodatkowych czynności zarówno po stronie użytkownika, jak i administratora serwera.

Decydując się na wdrożenie metody EAP-TLS należy wziąć pod uwagę trzy dodatkowe aspekty.

1. Ta metoda wymaga wysyłania stosunkowo dużych pakietów ze strony klienta, które przechodząc przez kilka serwerów pośredniczących jeszcze się powiększają i mogą przekroczyć MTU dla sieci. Konsekwencją jest fragmentacja pakietu, co w niektórych przypadkach może zablokować dalszą transmisję, a w efekcie brak uwierzytelnienia. Takie problemy były obserwowane w eduroam.
2. Dystrybucja indywidualnych certyfikatów jest organizacyjnie bardziej skomplikowana od stosowania identyfikatorów i haseł.
3. Niektórzy użytkownicy nie przejmują się faktem, że inne osoby mogą korzystać z sieci w ich imieniu i, jeżeli certyfikaty stosowane są wyłącznie na potrzeby połączenia z siecią, mogą uważać, że przekazywanie certyfikatu innym osobom nie stanowi zagrożenia. Stosowanie metod, w których używa się hasła użytkownika dającego dostęp do wielu innych, prywatnych usług, może dawać wyższą gwarancję, że z połączenia sieciowego będzie korzystała wyłącznie upoważniona osoba. Z tego powodu należy rozważyć, czy metody TLS nie należy ograniczyć do grupy bardziej zaufanych użytkowników.

7.1.4. Identyfikowanie użytkowników przy pomocy atrybutu Chargeable-User-Identity

Ponieważ prawdziwy identyfikator użytkownika może być ukryty w tunelu TLS, to identyfikacja użytkownika na terenie obcej instytucji może być stosunkowo trudna. Znaczącym ułatwieniem dla instytucji udzielających dostępu gościnnego, jest przesyłanie w pakietach Access-Accept atrybutu Chargeable-User-Identity, w którym podaje się unikatowy (ale nie zdradzający danych osobowych)

identyfikator użytkownika. Stosowanie tego atrybutu jest szczególnie przydatne w czasie reagowania na nadużycia w korzystaniu z sieci i dlatego dokładniejsze informacje zawarliśmy w dokumencie [4]. Tutaj chcemy jedynie podkreślić, że stosowanie tej metody będzie docelowo uważane za obowiązkowe w eduroam.

7.2. Implementacja modelu I

W celu poprawnego wdrożenia modelu I niezbędne jest dysponowanie urządzeniami, które są w stanie przypisać użytkownika do VLAN-u zgodnie z informacją przesłaną przez serwer RADIUS.

Należy zaplanować jeden VLAN dla gości i jeden lub więcej VLAN-ów na potrzeby lokalne. Sugerujemy, aby zaplanować odrębny VLAN dla pracowników i odrębny dla studentów⁴. Kolejny VLAN będzie potrzebny do obsługi dedykowanej sieci na potrzeby konferencji itp. Przyjmijmy nazewnictwo VLAN-ów: prac, stud, gość, konf.

Na urządzeniach dostępowych należy uruchomić dwa rozgłaszane SSID-y: eduroam i np. konferencja.

7.2.1. Sieć konferencyjna

SSID konferencja jest statycznie przypisany do VLAN-u konf, nie jest zabezpieczony żadnym szyfrowaniem. W sieci pracuje serwer DHCP, a na domyślnej bramie jest zainstalowany typowy portal dostępowy, tj. system, który wstępnie blokuje wyjście, a jednocześnie przechwytuje wszystkie pakiety protokołu HTTP i przekazuje je do serwera lokalnego. Serwer wyświetla stronę logowania, na której użytkownik wprowadza dane uwierzytelniające dostarczone mu przez organizatora konferencji. Po uwierzytelnieniu portal otwiera dostęp do internetu dla danego adresu MAC.

Tego typu rozwiązanie wymaga wcześniejszej interakcji gościa z administratorem lokalnym lub organizatorem konferencji, potrzebne jest bowiem i przekazanie danych uwierzytelniających.

Zamiast rozwiązania portalowego można zastosować również WPA-PSK, a hasło dostępu przekazać wszystkim uczestnikom. Wadą takiego rozwiązania jest brak możliwości związania konkretnego użytkownika z adresem IP.

7.2.2. Sieć eduroam

SSID eduroam powinien być domyślnie przypisany do VLAN-u, który nie ma żadnego dostępu do sieci; użytkownicy korzystający z tego SSID-a, po uwierzytelnieniu są przypisywani do jednego z VLAN-ów prac, stud lub gość⁵.

Użytkownicy muszą korzystać z identyfikatorów w postaci `id@realm`, przy czym `realm` musi zawierać się w oficjalnej domenie instytucji.

Przypisanie użytkowników do określonego VLAN-u następuje w wyniku przesłania przez serwer RADIUS odpowiednich atrybutów w pakiecie Access-Accept. W sytuacji, kiedy użytkownik eduroam korzysta z sieci poza swoją instytucją macierzystą, pakiet Access-Accept jest przesyłany z jego serwera macierzystego do serwera instytucji udostępniającej sieć i jest następnie przekazywany do punktu dostępowego. Pakiety Access-Accept przekazywane z jednej instytucji do drugiej nie powinny zawierać atrybutów zawierających VLAN-y. Gdyby numer VLAN-u przypisany przez instytucję macierzystą został nadany użytkownikowi w instytucji, w której w danym momencie jest, to albo znajdzie się on w istniejącym VLAN-ie (ale prawdopodobnie nie w tym, w którym powinien), albo przypisany numer nie będzie odpowiadał istniejącym VLAN-om i wówczas użytkownik nie otrzyma połączenia z siecią⁶. W pierwszym przypadku błędne ustawienie stanowi zagrożenie dla instytucji, na terenie której użytkownik korzysta z sieci, w drugim jest to niewygodą dla użytkownika, a za-

4 Uczelnia może docelowo wprowadzić dodatkowe systemy kontroli dostępu – np. sprawdzenie stanu oprogramowania antywirusowego; wdrożenie takiego systemu w odniesieniu do pracowników jest z pewnością dużo prostsze niż w przypadku studentów.

5 Ustawienie domyślnego VLAN-u, który nie daje żadnej łączności, jest dodatkowym zabezpieczeniem na wypadek błędu w konfiguracji serwera RADIUS – jeżeli serwer nie ustali żadnego VLAN-u, to użytkownik, pomimo uwierzytelnienia nie powinien uzyskać dostępu do sieci. Więcej o ustawianiu VLAN-ów można znaleźć w dokumencie [3]

6 Opisana sytuacja była stosunkowo często obserwowana we wczesnej fazie projektu eduroam.

tem stanowi problem dla instytucji macierzystej. Z tych powodów kładziemy bardzo silny nacisk na to, aby atrybuty odpowiadające za ustawianie VLAN-ów kasować zarówno przy wysyłaniu, jak i przy przyjmowaniu pakietów. Trzeba zdawać sobie sprawę, że samo dopisanie VLAN-u gościnnego do pakietu przychodzącego z zewnątrz może być niewystarczające, jeżeli ten pakiet już VLAN zawierał. Urządzenie dostępowe widząc dwa ustawienia VLAN-u może zareagować w różny sposób.

7.2.3. Problem nakładania się zasięgów

W przypadku, kiedy dwie instytucje korzystające z eduroam znajdują się bardzo blisko siebie (np. współdzielą jeden budynek) ich sieci bezprzewodowe mogą się nakładać. Jeżeli obie sieci stosują tę samą nazwę (SSID), to użytkownik będzie losowo przełączany pomiędzy punktami dostępu różnych sieci. Przełączenie do innej sieci będzie wymagało ustawienia nowego adresu IP, co nie dzieje się automatycznie przy każdym uwierzytelnieniu. W efekcie użytkownik będzie tracił łączność na dłuższy czas, a dodatkowo może tracić dostęp do pewnych usług lokalnych (będąc raz traktowany jako użytkownik lokalny własnej sieci, a za chwilę jako gość w sieci sąsiedniej instytucji).

Opisany problem można rozwiązać na dwa sposoby. Można zastosować różne SSID-y (tak jak to jest przewidziane w założeniach eduroam, czyli np. eduroam-ins1, eduroam-inst2) lub uzgodnić wspólną politykę propagacji i ustawiania VLAN-ów, tak by użytkownicy każdej z instytucji oraz goście zawsze trafiali do takiego samego VLAN-u i jednej klasy adresowej. Uzgodnienie takiej wspólnej polityki będzie wymagało współpracy z operatorem regionalnym, ponieważ będzie on musiał zapewnić propagację VLAN-ów oraz umożliwić przesyłanie atrybutów VLAN-owych poprzez serwer regionalny.

7.2.4. Stosowanie lokalnych VLAN-ów

W niektórych sytuacjach może zachodzić potrzeba zastosowania dodatkowych VLAN-ów i przydzielania do nich konkretnych użytkowników, pod warunkiem, że znajdują się na określonym obszarze. Np. pracownicy wydziału powinni być przydzielani do VLAN-u, z którego będą mieli dostęp do usług lokalnych, na przykład drukowania. Pomimo zastosowania jednego uczelnianego serwera RADIUS, możliwe jest ustawienie wartości VLAN-u na podstawie grupy, do której należy użytkownik oraz adresu punktu dostępowego, do którego jest dowiązany. Adres MAC punktu dostępu jest zazwyczaj dostępny w atrybucie RADIUS Called-Station-Id i to wystarczy, aby zbudować odpowiednie reguły.

7.3. Implementacja modelu II

W modelu tym stosujemy trzy SSID-y: eduroam, konferencja, lokalna. Sieci eduroam i lokalna stosują jakiś z typów WPA-Enterprise.

Łatwość implementacji tego modelu zależy od rodzaju urządzeń, jakimi dysponujemy. Jeżeli nasze urządzenia pozwalają na ustawienie oddzielnych serwerów RADIUS dla każdego SSID-a, to można z tego skorzystać stosując odrębny serwer RADIUS dla sieci lokalna i konfigurując go tak, by odrzucał próby uwierzytelnienia z nieznanym identyfikatorem użytkownika. Inną metodą jest korzystanie z dodatkowej informacji przesyłanej w pakietach Access-Request np. w postaci atrybutów Called-Station-Id (jako wartość przesyłany jest zazwyczaj BSSID, czyli adres MAC wirtualnego urządzenia dostępowego). Możliwe są inne scenariusze, ale właściwie wszystkie sprowadzają się do interpretacji informacji przesyłanej w pakietach RADIUS, tak by ograniczyć dostęp do sieci lokalna. Począwszy od wersji 2.0 oprogramowanie FreeRADIUS daje możliwość definiowania wirtualnych serwerów, dedykowanych na przykład dla określonej puli BSSID. Takie podejście może być wygodniejsze niż konfigurowanie wielu serwerów RADIUS powiązanych z tą samą bazą użytkowników.

7.3.1. Sieć konferencyjna

Konfiguracja identyczna jak w 7.2.1.

7.3.2. Sieć lokalna

Sieć z SSID-em lokana (oczywiście tę nazwę przyjmujemy tylko na potrzeby niniejszego dokumentu), zabezpieczona przez WPA ew. WPA+WPA2. Może być statycznie przypisana do jednego VLAN-u (bez rozdziału użytkowników lokalnych na podgrupy), bądź stosować atrybuty ustawiające VLAN. Taka sieć nie nakłada ograniczeń odnośnie postaci identyfikatorów użytkowników dowolne identyfikatory użytkowników, ale radzimy, by dla uproszczenia używać identyfikatorów, które będą mogły być również zastosowane w sieci eduroam, tzn. by budować je w postaci `id@realm`. Należy wprowadzić jakiś mechanizm ochronny przed osobami spoza instytucji, tak jak to opisano powyżej.

7.3.3. Sieć eduroam

Sieć z SSID-em eduroam. Najprościej użyć statycznego powiązania SSID-u z VLAN-em. Oczywiście z siecią eduroam mogą się połączyć również użytkownicy lokalni, ale ponieważ w tym modelu eduroam służy tylko dostępowi gościnnemu, to użytkownicy lokalni, łączący się z tą siecią, powinni być traktowani tak samo jak goście.

8. Organizacja gościnnego dostępu w ramach eduroam

Podstawowym założeniem eduroam jest to, że dostęp do sieci nie jest anonimowy, tzn. że istnieją środki pozwalające na wskazanie użytkownika, który w danym momencie korzystał z sieci. W przypadku, gdy zaistnieje jakieś nadużycie związane z korzystaniem z sieci, instytucja powinna zgłosić ten fakt Operatorowi Regionalnemu lub Koordynatorowi eduroam w Polsce zgodnie z procedurami opisanymi w dokumencie [4]. Należy być przygotowanym na to, że do właściwego powiązania incydentu z konkretną osobą niezbędne jest skojarzenie adresu IP z jego użytkownikiem w konkretnym momencie. Chcemy podkreślić, że stosowanie NAT w sieci gościnniej praktycznie uniemożliwi skuteczne reagowanie na incydenty. Projektując sieć należy przemyśleć procedury i przykłady rozwiązań opisane w [4], tak by dopasować do nich właściwe rozwiązania lokalne.

9. Urządzenia na potrzeby sieci uczelnianej

W ramach przygotowań do wdrożenia eduroam przeprowadzono szereg testów sprzętu bezprzewodowego. Testowano systemy oparte o centralne kontrolery. Wyniki testów są dostępne w postaci oddzielnych raportów. Należy podkreślić, że raporty mogą jeszcze ulec modyfikacji, ponieważ niektórzy producenci nadal pracują nad poprawą parametrów działania swojego sprzętu.

Testowane przez nas systemy można podzielić na cztery grupy:

1. klasyczne systemy centralizujące zarządzanie punktami dostępu, nie korzystające z żadnych rozszerzeń standardu 802.11;
2. systemy dodatkowo wspomagające się rozszerzeniami implementowanymi po stronie klienta;
3. systemy przedstawiające całą sieć bezprzewodową w postaci jednego, wirtualnego punktu dostępu.

Do grupy 1 zaliczyliśmy systemy producentów: 3COM (seria WX), Alcatel/Aruba, Siemens, Trapeze Networks.

Grupa 2, to urządzenia Cisco, w których implementowane są rozszerzenia, które po stronie klienta wymagają wsparcia dla tzw. Cisco Client Extensions.

Grupa 3 to bardzo specyficzne i nieco kontrowersyjne rozwiązanie firmy Meru Networks.

W czasie testów stwierdzono, że systemy z grup 1-2, od strony użytkownika, zachowują się bardzo podobnie. Płynne przejście między AP (tzn. bez uwierzytelnienia) było praktycznie nie do osiągnięcia. Czasy przełączenia zależały od typu systemu, od stosowanych metod EAP, od stosowanego serwera RADIUS oraz od tego, czy uwierzytelnienie odbywało się lokalnie, czy też wymagało przekazywania zleceń poprzez strukturę eduroam.

W Grupie 3 symulacja pojedynczego punktu dostępu sprawia, że problem przełączania klienta jest w całości realizowany po stronie kontrolera. Jest to jedyny z testowanych systemów, który w płynny sposób przełącza klientów niezależnie od ich oprogramowania i sprzętu.

Jednoznaczne zarekomendowanie sprzętu jest niemożliwe. W każdej sytuacji trzeba wziąć pod uwagę warunki lokalne. Płynne przełączanie użytkowników może być ważne w sieciach, gdzie użytkowników jest wielu, często są w ruchu, a dodatkowo nasycenie punktami dostępu jest wysokie. Prowadzone testy miały maksymalnie odzwierciedlać warunki rzeczywiste, ale nie są w stanie wykryć stosunkowo rzadko występujących problemów. Na wyniki testów duży wpływ może mieć przyjęte założenie, że stosuje się tylko szyfrowanie WPA/TKIP. Standard WPA2 z nowszą i lepszą metodą dystrybucji kluczy oraz mechanizmami wstępnego uwierzytelnienia jest w stanie poprawić rezultaty przełączania użytkowników. Z tych powodów testy należy traktować jako zbiór wskazań, które mogą być przydatne przy sporządzaniu specyfikacji, a nie jako rekomendację konkretnych rozwiązań.

System wydzielony jako Grupa 3 jest niewątpliwie bardzo interesującym rozwiązaniem, trzeba jednak pamiętać o tym, że specjaliści od standardów WiFi podnoszą zastrzeżenia co do „czystości” tego rozwiązania. Może się również zdarzyć, że pewne karty, lub sterowniki nie będą się tak łatwo podporządkowywały reżimowi transmisji narzucanym przez to rozwiązanie.

Bibliografia

- [1] A. Angowski; Zapobieganie samowolnej zmianie IP, http://www.eduroam.pl/Dokumentacja/eduroam_zapobieganie_zmianie_IP.pdf
- [2] eduroam-PIONIER; Polska Polityka eduroam (regulamin usługi eduroam), <http://www.eduroam.pl/polityka>
- [3] M. Górecka-Wolniewicz; Instalacja i konfiguracja serwera FreeRADIUS, <http://www.eduroam.pl/Dokumentacja/freeradius2-1.0.pdf>
- [4] M. Górecka-Wolniewicz, Z. Ołtuszyk, T. Wolniewicz; Zasady obsługi incydentów sieciowych w usłudze eduroam, <http://www.eduroam.pl/Dokumentacja/incydenty-1.0.pdf>