Bezpieczeństwo 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
uaktualniony w ramach projketu PLATON
wersja 2.0

Spis treści

1. Wstęp

Podstawowym wymogiem projektowym eduroam było zagwarantowanie użytkownikom maksymalnego poziomu bezpieczeństwa. W niniejszym dokumencie przedstawiamy zagadnienia powiązane ze stosowanymi technologiami, mające wpływ na bezpieczeństwo usługi. Pomijamy natomiast aspekty formalne, czyli kwestie związane z obowiązującymi regulaminami oraz stosowanymi procedurami ([1], [2], [3]). Należy jednak pamiętać, że i one podnoszą znacząco stopień bezpieczeństwa usługi. Poruszone w tym dokumencie tematy dotyczące bezpieczeństwa eduroam są przede wszystkim kierowane do administratorów usługi eduroam, pokazują jak, włączając się w infrastrukturę eduroam, zadbać o to, by zagwarantować bezpieczeństwo oraz o czym powinni być informowani użytkownicy.

2. Bezpieczeństwo sieci

Sieć bezprzewodowa zawsze jest narażona na atak zarówno z zewnątrz, ze strony osób nieuprawnionych, starających się skorzystać z jej zasobów lub zaatakować jej elementy, jak i od wewnątrz albo ze strony użytkowników, którzy mogą starać się nadużyć swoich uprawnień, albo ze strony oprogramowania (malware) zainstalowanego na komputerach użytkowników.

2.1. Bezpieczne urządzenie dostępowe

Urządzenia dostępowe (Access Point, AP), z których korzysta eduroam muszą spełniać określone wymagania techniczne, przede wszystkim muszą wspierać standard 802.1X oraz odpowiednie technologie szyfrowania (WPA2). Zostało to szczegółowo omówione w dokumencie [4]. AP-y, czy w postaci 'cienkich' punktów dostępowych, czy kontrolerów są kluczowymi urządzeniami usługi, dlatego należy zadbać, by ich konfiguracja nie uległa zniszczeniu. Urządzenia te powinny funkcjonować w chronionej, dedykowanej podsieci (VLAN-ie) i muszą być na nich wdrożone mechanizmy ochrony przed nieuprawnionym dostępem. Zgodnie z przyjętą architekturą usługi eduroam, urządzenia do-

stępowe współpracują z serwerami RADIUS zlokalizowanymi w instytucjach. Współpraca AP z serwerem RADIUS jest możliwa pod warunkiem, że obie strony znają wspólne hasło stosowane w komunikacji. Zaleca się staranny dobór tych haseł i ich okresowe zmiany.

2.2. Bezpieczny serwer RADIUS

Serwery RADIUS w instytucjach włączonych w usługę eduroam działają zgodnie z ustalonymi regułami ([5, 7]). Akceptują zapytania nadchodzące od określonych klientów. W konfiguracji serwera są ustalane adresy IP oraz hasła wspólne urządzeń dostępowych, jak zostało to opisane w części 2.1 tego dokumentu. Klientami serwera RADIUS są nie tylko AP-y, ale również inne serwery RADIUS, występujące w roli serwerów proxy. Wszystkie serwery proxy, które mają prawo kontaktować się z serwerem RADIUS muszą zostać zarejestrowane w danym serwerze. Oznacza to dodanie pełnej nazwy domenowej lub adresu IP serwera do tablicy klientów oraz przydzielenie wspólnego hasła do komunikacji. Serwer RADIUS nasłuchuje domyślnie na portach UDP: 1812, 1813 i 1814. Dostęp do tych portów należy przydzielać wyłącznie zaufanym urządzeniom.

Procedury rejestracji serwerów zmienią się w kolejnych fazach projektu, gdy zacznie być wdrażany protokół RADIUS over TLS (powszechnie znany pod nazwą RadSec) [8]. RadSec realizuje transmisję komunikatów między serwerami w bezpiecznym kanale transmisji TLS w warstwie TCP, w tym przypadku do wdrożenia zabezpieczeń jest wykorzystywana funkcjonalność certyfikatów. Serwery kontaktujące się ze sobą korzystają z certyfikatów identyfikowanych jako wspólne dzięki wbudowanym w nie rozszerzeniom. Nie jest wówczas realizowana ochrona portów serwera, gdyż nie są z góry znani potencjalni klienci. Serwer odrzuca zlecenia od nieuprawnionych klientów RadSec, czyli tych, którzy posługują się niewłaściwym certyfikatem. Ponieważ takie podejście może wnieść dodatkowe zagrożenie związane z atakami typu Denial od Service, zaleca się na tym etapie położenie nacisku na ochronę poprzez mechanizmy firewallowe, m.in. limitowanie liczby połączeń z danego IP na adres serwera.

Serwery RADIUS w instytucjach realizują proces uwierzytelniania użytkowników z danej instytucji. Najczęściej RADIUS współpracuje w tym zakresie z dedykowanym systemem uwierzytelniania, jak np. baza LDAP, ActiveDirectory, czy relacyjna baza danych. Należy zapewnić bezpieczny przepływ informacji związanej z uwierzytelnianiem, umożliwia to m.in. korzystanie z protokołu TLS do komunikacji z bazą danych, lub zapewnić, by serwery RADIUS oraz serwery systemu uwierzytelniającego znajdowały się w strefie zdemilitaryzowanej.

2.3. Standard 802.1X i metody uwierzytelniania

W dokumencie [10] zostały przedstawione korzyści, jakie daje technologia 802.1X. Do jej podstawowych zalet, również z punktu widzenia usługi eduroam, należy możliwość kontrolowania ruchu oraz identyfikacji osób korzystających z sieci bezprzewodowej poprzez eduroam.

Dostęp do sieci bezprzewodowej w eduroam wymaga uwierzytelnienia. Dzięki istnieniu zaufanej struktury serwerów RADIUS nie jest możliwe korzystanie z sieci przez nieuprawnione osoby. Każdy użytkownik, który uzyskuje dostęp do sieci musi zostać zaakceptowany przez serwer RADIUS macierzystej instytucji.

Komunikacja realizowana między urządzeniem klienckim, urządzeniem dostępowym i serwerem RADIUS odbywa się za pomocą protokołu EAP. W pierwszym etapie konwersacji ustalane są zasady uwierzytelnienia, klient przekazuje dane uwierzytelnienia oraz informację, z jakiej metody uwierzytelniania chce skorzystać. Protokół EAP dostarcza wyłącznie infrastrukturę komunikacji, tzn. określa postać komunikatów i sposób ich przekazywania. EAP nie definiuje mechanizmu uwierzytelniania. Poszczególne implementacje EAP zawierają w sobie konkretne metody uwierzytelniania.

Metoda uwierzytelniania to element narażony na zagrożenia w środowisku sieciowym. Niektóre metody, jak EAP-MD5, czy LEAP są bardzo mało wytrzymałe na ataki. Najbezpieczniejszą metodą jest EAP-TLS, który korzysta ze środowiska PKI i wymaga prezentacji poprawnych certyfikatów przez obie strony komunikacji. Metody EAP-TTLS, PEAP, EAP-FAST, przekazują dane uwierzytelniania w postaci identyfikatora użytkownika oraz hasła w tunelu TLS, dedykowanym do komunikacji klient-serwer - gwarantują więc dobry poziom bezpieczeństwa, a jednocześnie zapewniają

możliwość lepszej ochrony rzeczywistej tożsamości użytkownika (patrz część 3.3.1). Nowa metoda EAP-PWD realizuje zabezpieczenia w bardzo specyficzny sposób; jest uważana za szybką i bezpieczną, ale z uwagi na znikomy stan wróżenia, nie można mieć pewności, że została dokładnie przetestowana.

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. 802.1X dzięki stosowaniu dynamicznych kluczy sesyjnych w istotny sposób zmniejsza się prawdopodobieństwo takiej sytuacji, gdyż czas życia konkretnych kluczy jest krótki. W szyfrowaniu TKIP występuje możliwość przejęcia kluczy grupowych i w konsekwencji przechwycenia niewielkiej części transmisji, nie jest to jednak znaczące zagrożenie, a TKIP i tak jest już wycofywany.
3. **Atak typu „man-in-the-middle”**: atakujący czyta i modyfikuje komunikację pomiędzy dwoma stronami, bez ich wiedzy. Podobnie jak w p. 2, dynamiczne klucze szyfrujące, stosowane w standardzie 802.1X minimalizują możliwość wykorzystania informacji zawartej w pakiecie. dodatkowo szyfrowanie komunikacji uniemożliwia podejrzenie i modyfikację jej treści.

2.4. Bezpieczna sieć bezprzewodowa

Po pozytywnym uwierzytelnieniu za pomocą infrastruktury eduroam, otwierany jest dla danego użytkownika dostęp do sieci. Sieć bezprzewodowa powinna korzystać adresów należących do danej instytucji, nie jest zalecane stosowanie prywatnej puli adresów, gdyż w ten sposób ograniczamy możliwość analizy incydentów sieciowych [2].

Jeżeli z powodu bezpieczeństwa jest wskazane oddzielenie bezprzewodowej sieci pracowników od sieci studentów, czy gości, to zaleca się stosowanie technologii VLAN. Serwer RADIUS może decydować o umieszczeniu użytkownika w określonym VLAN-ie na podstawie atrybutów w bazie danych, czy domeny logowania. Obecność atrybutu VLAN w odpowiedzi Access-Accept na zlecenie uwierzytelniania, pozwala na właściwą kwalifikację użytkownika. Należy zwrócić szczególną uwagę, aby prawidłowo obsługiwać atrybuty VLAN pojawiające się w pakietach Access-Accept przychodzących z obcych serwerów RADIUS. Bezwzględnie należy pilnować zasady, aby wartości takich atrybutów były zastępowane wartościami właściwymi dla VLAN-u gości.

Zlecenie przydzielenia numeru IP uwierzytelnionemu klientowi kierowane jest do serwera DHCP w danej sieci, czy danym VLAN-ie. Sieć bezprzewodowa nie powinna pozwalać na samowolną zmianę adresu IP przez użytkowników. Jednym ze sposobów obrony przed tego typu incydentem jest domyślne blokowanie dostępu do sieci i jawne otwieranie dostępu na podstawie adresu MAC i IP, mechanizm ten został opisany w dokumencie [9].

Nie ma potrzeby wprowadzania ochrony sieci bezprzewodowej na wejściu, gdyż nie ma w ramach tej sieci żadnych usług. Dokumenty [1] i [4] zawierają rekomendacje dotyczące ochrony sieci bezprzewodowej. Jednym z zaleceń jest uniemożliwienie rozsyłania spamów oraz wirusów poprzez stosowanie transparentnego pośredniego serwera SMTP (np. oprogramowania smtp-proxy http://smtp-proxy.klolik.org/, czy Anti-Spam SMTP Proxy (ASSP) http://sourceforge.net/projects/assp/

3. Bezpieczeństwo użytkownika sieci eduroam

Każdy użytkownik Internetu powinien sobie zdawać sprawę, że jeżeli nie stosuje szyfrowania transmisji, to dane które wysyła są narażone na podsłuch. Jeżeli podsłuchem zagrożony jest kanał prowadzący bezpośrednio do użytkownika, to niebezpieczeństwo jest zdecydowanie wyższe, ponieważ przejęcie wszystkich wysyłanych danych pozwala na zgromadzenie dużo bardziej kompletnej informacji o konkretnym użytkowniku, niż gdy atakujący stara się analizować strumień danych w szkielecie sieci. Stąd łatwo wyciągnąć wniosek, że kanał użytkownika powinien być szczególnie chroniony. W przypadku sieci bezprzewodowej na ten kanał składa się transmisja radiowa między komputerem użytkownika a punktem dostępowym, sam punkt dostępowy i jego połączenie do reszty sieci. W tej części przeanalizujemy występujące zagrożenia i metody, przy pomocy których eduroam sobie z nimi radzi.

Drugim, bardzo istotnym zagadnieniem, jest sposób, w jaki użytkownik uwierzytelnia się w sieci. Jeżeli do uwierzytelnienia korzysta się z identyfikatora i hasła, to konieczne jest zabezpieczenie tych danych nie tylko w kanale podłączeniowym, ale na całej trasie przez Internet.

Trzecią sprawą, którą się zajmiemy jest ochrona prywatności użytkownika, a dokładniej informacji o tym w jakiej lokalizacji i w jakim czasie korzystał z sieci.

Bardzo ważna jest więc właściwa, pierwotna konfiguracja sieci na urządzeniu klienckim użytkownika – laptopie, czy telefonie. Szczegółowe instrukcje konfiguracji są umieszczane na stronach WWW dostawców usługi eduroam w macierzystej instytucji. Jednym z najbardziej istotnych elementów konfiguracji jest honorowanie certyfikatów stosowanych do komunikacji w tunelu SSL. Serwery RADIUS instytucji korzystają z certyfikatów poświadczonych przez urząd certyfikacyjny znany użytkownikowi. Jakiekolwiek błędy związane z certyfikatami powinny zostać zgłoszone przez użytkownika administratorowi usługi eduroam w macierzystej instytucji. Zabronione jest wyłączanie sprawdzania certyfikatów po stronie użytkownika. W projekcie GN3 prowadzone są prace nad stworzeniem uniwersalnego konfiguratora eduroam. System będzie generował gotowe, instalatory dopasowane do ustawień konkretnej instytucji. Instalatory będą ograniczały do minimum kłopotliwość konfiguracji po stronie użytkownika, a jednocześnie będą gwarantowały maksymalne bezpieczeństwo.

Użytkownik musi zostać poinformowany, że administratorzy nie ponoszą konsekwencji samowolnych zmian konfiguracji eduroam na jego urządzeniu klienckim. Nie zaleca się modyfikacji ustawień w przypadku braku połączenia z siecią w nowej lokalizacji. Ewentualnie administrator może przedstawić listę akceptowalnych zmian po stronie użytkownika (np. przełączenie typu szyfrowania z WPA na WPA2).

3.1. Zagrożenia i ochrona transmisji bezprzewodowej

3.1.1. Odczytanie transmisji bezprzewodowej

Dane wysyłane w sieci bezprzewodowej są bardzo łatwe do podsłuchania, dlatego niezbędne jest zabezpieczanie ich poprzez szyfrowanie. W eduroam zawsze stosuje się szyfrowanie danych przy pomocy często zmieniających się indywidualnych kluczy zapewnianych przez standard 802.1X. Sieci zgodne z tzw. WPA-Enterprise (a zatem takie jakie się stosuje w eduroam) są wystarczająco bezpieczne, aby móc uznać, że odczytanie danych jest niewykonalne. Ostatnio pojawiły się doniesienia o wykryciu pewnych słabości WPA-Enterprise pozwalających na zdeszyfrowanie niewielkich pakietów danych. Tych słabości nie ma WPA2 (802.11i) i aktualny regulamin eduroam nakazuje stosowanie właśnie tego rozwiązania.

3.1.2. Nakłonienie użytkownika by podłączył się do niezaufanego urządzenia

Użytkownik usługi eduroam korzysta z sieci bezprzewodowej widocznej pod identyfikatorem `eduroam`. Zazwyczaj raz konfiguruje dostęp do sieci eduroam i następnie łączy się z nią automatycznie wszędzie tam, gdzie taki identyfikator sieci jest widoczny. Podstawowym założeniem usługi eduroam jest zagwarantowanie użytkownikowi, że korzystając w dowolnym miejscu z sieci o nazwie `eduroam` może uważać, że ma do czynienia z bezpieczną siecią.

Uruchomienie urządzenia dostępowego jest bardzo proste, można do tego użyć komputera z kartą bezprzewodową. Osoba uruchamiająca punkt dostępu może wybrać dowolną nazwę sieci, w szczególności może próbować podszyć się pod sieć eduroam. Użytkownik widząc sieć o znanej nazwie podejmie próbę połączenia. Jeżeli system użytkownika jest poprawnie skonfigurowany, to przed przesłaniem jakichkolwiek danych uwierzytelniających zostanie sprawdzone, czy sieć przedstawia się certyfikatem serwera domowego użytkownika. Ta weryfikacja przypomina dostęp do bezpiecznej strony WWW, chociaż w przypadku eduroam klient łączy się zawsze z tym samym serwerem, więc zabezpieczenia mogą być naprawdę skuteczne. Prawidłowo skonfigurowane urządzenie użytkownika nigdy się nie połączy z fałszywą siecią.

Drugi rodzaj ataku to tzw. man-in-the middle, polegający na uruchomieniu urządzenia rozgłaszającego nazwę sieci eduroam, a jednocześnie podłączonego do rzeczywistej sieci eduroam (np. za pośrednictwem anteny kierunkowej skierowanej na uczelniany punkt dostępu). Taki fałszywy punkt dostępu mógłby przejmować transmisję użytkownika i przekazywać ją dalej. Atak tego typu jest nieskuteczny dzięki metodzie szyfrowania transmisji bezprzewodowej stosowanej w rozwiązaniach eduroam. Do nawiązania połączenia obie strony – komputer użytkownika i punkt dostępu – muszą dysponować tym samym kluczem szyfrującym, który jest przekazywany przez serwer RADIUS każdej ze stron oddzielnie, w sposób niewidoczny dla drugiej strony. Jeżeli urządzenie dostępowe nie jest uwierzytelnione w serwerze RADIUS włączonym w strukturę eduroam, to nie otrzyma właściwego klucza szyfrującego i transmisja nie zostanie nawiązana.

Próba podłączenia urządzenia dostępowego bezpośrednia do któregoś z serwerów RADIUS również nie może się powieść, bo do tego niezbędny jest klucz dostępu ustawiany przez administratora.

3.2. Wpływ trybu i wyboru narzędzia logowania do sieci na bezpieczeństwo

Do uwierzytelnienia się w sieci eduroam użytkownik może korzystać albo z indywidualnego certyfikatu, albo z identyfikatora i hasła. W pierwszym przypadku użytkownik jest całkowicie bezpieczny, bo krytyczne dane nigdy nie opuszczają jego komputera. Drugi przypadek wymaga dokładniejszego wyjaśnienia, ponieważ przechwycenie danych byłoby bardzo niebezpieczne.

W stosowanych w eduroam, metodach uwierzytelnienia przesłanie danych krytycznych jest zawsze poprzedzone sprawdzeniem certyfikatu uwierzytelniającego serwera RADIUS. Po potwierdzeniu prawidłowości certyfikatu, między macierzystym serwerem RADIUS a stacją użytkownika zestawia się szyfrowany kanał i w nim przesyła dane uwierzytelniające. Jeżeli użytkownik zwraca uwagę na komunikaty ostrzegawcze, to jego dane są bezpieczne. System może być również skonfigurowany w sposób nie pozwalający na połączenie z fałszywym serwerem i wówczas użytkownik może nawet nie otrzymać o tym komunikatu.

Należy zwrócić uwagę, że stosując na serwerze RADIUS certyfikat podpisany przez lokalny urząd certyfikacyjny, np. uczelniany, podnosimy bezpieczeństwo usługi. Wprawdzie użytkownik musi instalować na swoim komputerze certyfikat danego urzędu, jednak w ten sposób znacząco minimalizujemy niebezpieczeństwo łączenia się z obcymi serwerami, używającymi certyfikatów wystawionych przez zaufane urzędy. Jeżeli stosuje się certyfikat pochodzący z CA ogólnego użytku, to niezbędne jest, aby dodatkowo zapisać listę nazw domenowych uprawnionych serwerów. Oprogramowanie klienckie sprawdza wówczas czy w certyfikacie, którym przedstawia się serwer znajduje się dozwolona nazwa.

Do połączenia z siecią użytkownik musi skorzystać ze specjalizowanego oprogramowania obsługującego protokół 802.1X. Dobre narzędzie powinno mieć następujące cechy:

1. Zapewniać prostotę i pełny automatyzm logowania – sieci korzystające z uwierzytelniania 802.1X cechują się stosunkowo często ponawianą akcją uwierzytelniania, dlatego dane użytkownika powinny być wprowadzanie maksimum jeden raz przy połączeniu – większość użytkowników akceptuje jednak trwałe zapisanie hasła w programie logującym, jeżeli z komputera korzysta tylko jedna osoba.
2. Chronić użytkownika przed wysłaniem danych uwierzytelniających do niezaufanej sieci – sieć włączona w usługę eduroam „przedstawia" użytkownikowi certyfikat jego domowego serwera RADIUS; w programie logującym użytkownika powinien być zapisany certyfikat urzędu, który wystawił certyfikat dla serwera RADIUS oraz końcówka nazwy domenowej, której serwer korzysta (ten drugi warunek musi być spełniony tylko w przypadkach, gdy zachodzi możliwość, że urząd certyfikacyjny potwierdza tożsamość również obcych serwerów

RADIUS); program logujący powinien odrzucać próby połączenia z siecią, która przedstawia niepoprawny certyfikat.

3. Chronić tożsamość użytkownika – tam, gdzie to możliwe powinny być stosowane anonimowe identyfikatory zewnętrzne.
4. Dawać się wstępnie konfigurować, tak by minimalizować ilość danych, które użytkownik musi wprowadzać samodzielnie i eliminować ew. błędy.
5. Poprawnie współpracować z różnymi typami szyfrowania sieci – jest to jeden z głównych problemów eduroam – sieci różnych instytucji stosują różne rodzaje szyfrowania (zazwyczaj WPA/TKIP lub WPA2/AES). Oprogramowanie klienckie powinno się przełączać pomiędzy tymi typami nie wymagając od użytkownika ręcznej rekonfiguracji.

Oprogramowanie klienckie w ciągu ostatnich lat uległo dużej poprawie. Niestety pojawiające się nowe urządzenia – smartfony, tablety niekiedy maja oprogramowanie mocno niedoskonałe.

Systemy Microsoft Windows, począwszy od Windows Vista, pozwalają na poprawna i automatyczną konfigurację. Podobnie jest z systemami Apple Mac OS X oraz iOS.

Oprogramowanie wpa_supplicant stosowane w systemach Linux można skonfigurować, tak by spełniało wszystkie wymienione cechy. Prekonfiguracja jest stosunkowo skomplikowanym zagadnieniem, ale eduroam CAT będzie wkrótce udostępniał mechanizm, który to zadanie bardzo ułatwi.

Bardzo obiecującym projektem jest eduroam CAT – system generowania instalatorów na podstawie danych wprowadzonych przez administratorów instytucji. System jest obecnie w fazie testów i będzie na początku udostępniał automatyczne instalatory dla systemów Microsoft Windows, MAC OS X, iOS, Linux. Zainstalowanie eduroam przy pomocy tych instalatorów nie tylko ułatwia życie użytkownikowi, ale również chroni go przed wszystkimi potencjalnymi atakami.

3.3. Ochrona prywatności użytkownika

3.3.1. Ochrona tożsamości

Standard 802.1X pozwala kontrolować, kto korzysta z sieci bezprzewodowej. Przekazywanie identyfikatorów użytkownika w otwartej postaci pomiędzy zdalnymi serwerami budzi sporo kontrowersji, gdyż przechwycenie takich danych może narazić użytkownika na większą liczbę spamów, czy umożliwić dotarcie do właściciela identyfikatora niepożądanych osób. O ile w jednostce macierzystej ujawnianie takich danych jest łatwe do zaakceptowania, w ruchu zewnętrznym użytkownicy wolą pozostać anonimowi. Naprzeciw temu problemowi wychodzi funkcjonalność zewnętrznej tożsamości, stosowania w protokole RADIUS. Zewnętrzna tożsamość (*outer identity*), to identyfikator, który pojawia się w pakietach RADIUS w atrybucie `User-Name`. Niektóre programy klienckie, jak SecureW2, czy klient `wpa_supplicant` w systemach linuxowych pozwalają zdefiniować identyfikator używany na zewnątrz tunelu. Ma on najczęściej postać `anonymous@domena`, albo po prostu `@domena`. Właściwy identyfikator, używany do uwierzytelnienia, zwany tożsamością wewnętrzną, albo identyfikatorem wewnętrznym, jest przekazywany w zaszyfrowanej postaci w atrybucie `EAP-Message` komunikatu protokołu RADIUS. Wewnętrzny identyfikator jest widoczny wyłącznie przez macierzysty serwer RADIUS.

Korzystanie z zewnętrznej tożsamości stanowi istotne utrudnienie przy rozwikływaniu incydentów sieciowych. Administrator usługi eduroam reagując na incydent w sieci, dotyczącego użytkownika spoza danej instytucji, nie może jednoznacznie wskazać winnego na podstawie identyfikatora osoby podejrzanej o niewłaściwe korzystanie z sieci. Nawet jeśli identyfikator nie wskazuje swoją postacią na to, że jest inny niż identyfikator wewnętrzny, nie można traktować go jako wiarygodnego źródła danych. W usłudze eduroam zaleca się stosowanie atrybutu Chargeable-User-Identity (CUI), zdefiniowanego w RFC 4372 ([6]). W tym atrybucie serwer RADIUS powinien umieścić unikatowy identyfikator, jednoznacznie wskazujący konkretnego użytkownika. Atrybut ten ma się pojawiać w pakiecie akceptującym użytkownika (`Access-Accept`). W celu maksymalnej ochrony prywatności użytkownika zaleca się, aby taki identyfikator był zmieniany w zależności od instytucji, w której znajduje się użytkownik, tak by uniemożliwić korelowanie informacji na jego temat przez instytucje, które odwiedza. Jedną z możliwości jest wprowadzenie zasady, że wartość CUI jest generowana poprzez zastosowanie funkcji skrótu (np. MD5) do ciągu znaków powstałego z połączenia identyfikatora przesłanego przez instytucję w atrybucie NAS-Identifier z rzeczywistym identyfika-

torem użytkownika. Taka informacja jest dla osób postronnych całkowicie nieprzydatna, jej publikowanie nie stanowi więc dla użytkownika żadnego zagrożenia.

Możliwość ukrycia tożsamości użytkownika może być ważna w kontekście przepisów chroniących dane osobowe. Warto zdawać sobie sprawę, że użytkownik stosujący EAP-TLS przesyła swój certyfikat indywidualny bez ochrony, a zatem dane w nim zapisane są widoczne. Wprawdzie EAP-TLS przewiduje mechanizmy ochrony certyfikatu, to jednak na razie nie są one implementowane. Na potrzeby eduroam nie powinno się zatem stosować certyfikatów, z których można odczytać dane osobowe użytkownika.

3.3.2. Ochrona danych związanych z miejscem pobytu

Usługa eduroam zaleca stosowanie atrybutu Operator-Name, zawierającego domenę instytucji, w której użytkownik korzysta z sieci. Przekazanie tej informacji jest ważne z kilku powodów, również dla ochrony prywatności użytkownika. Atrybut Chargeable-User-Identity jest generowany na podstawie rzeczywistego identyfikatora użytkownika oraz wartości Operator-Name i dlatego może być różny dla różnych lokalizacji.

W procesie uwierzytelnienia przekazywane są dane użytkownika i urządzenia dostępowego. Podobnie adres IP urządzenia dostępowego (AP lub kontrolera) jest zazwyczaj wysyłany w atrybucie RADIUS NAS-IP-Address zlecenia Access-Request. To zlecenie trafia do serwera macierzystego użytkownika, a zatem, jeżeli dla AP stosujemy publiczne adresy IP, to „zdradzamy" lokalizacje użytkownika.

Wdrożenie protokołu RadSec i bezpośrednich połączeń między serwerami instytucji spowoduje, że lokalizacja użytkownika będzie znana instytucji uwierzytelniającej.

Użytkownik powinien sobie zdawać sprawę, że informacji o jego lokalizacji mogą docierać do instytucji macierzystej i, że jest to nieusuwalny skutek korzystania z eduroam. Lokalne regulaminy eduroam powinny uwzględniać ten fakt i np. nakazywać, by informacje mogące określić położenie użytkownika nie były zapisywane w logach systemowych.

Materiały towarzyszące

[1] *Regulamin dostępu do eduroam,* http://www.eduroam.pl/regulamin/

[2] *Koncepcja wdrożenia usługi eduroam w sieci Pionier*, T. Wolniewicz, M. Górecka-Wolniewicz, Z. Ołtuszyk

[3] *Zasady obsługi incydentów sieciowych w usłudze eduroam*, M. Górecka-Wolniewicz, T. Wolniewicz, Z. Ołtuszyk

[4] *Koncepcja uczelnianej sieci bezprzewodowej włączonej w strukturę eduroam,* T. Wolniewicz, M. Górecka-Wolniewicz, Z. Ołtuszyk, http://www.eduroam.pl/Dokumentacja/incydenty-2.0.pdf

[5] *Koncepcja uczelnianej sieci bezprzewodowej włączonej w strukturę eduroam,* T. Wolniewicz, M. Górecka-Wolniewicz, Z. Ołtuszyk, http://www.eduroam.pl/Dokumentacja/koncepcja_sieci_uczelnianej-2_0.pdf

[6] *Chargeable User Identity*, F. Adrangi, A. Lior, J. Korhonen, J. Loughney, RFC 4372

[7] *Instalacja i konfiguracja serwera FreeRADIUS*, http://www.eduroam.pl/Dokumentacja/freeradiusv2-09-2012.pdf

[8] *Wykorzystywane technologii RadSec w usłudze eduroam*, Maja Górecka-Wolniewicz, http://eduroam.pl/Dokumentcja/radsec.pdf

[9] *Zabezpieczenie przez zmianą adresu IP przez Użytkownika,* A. Angowski, http://www.eduroam.pl/Dokumentacja/eduroam_zapobieganie_zmianie_IP.pdf

[10] Uwierzytelnianie 802.1X w usłudze eduroam, M. Górecka-Wolniewicz, T. Wolniewicz, http://www.eduroam.pl/Dokumentacja/802_1X_02.pdf