

Zasady obsługi incydentów sieciowych w usłudze eduroam

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

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

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

dokument przygotowany w ramach projektu B-R eduroam-PIONIER

wersja 1.0

Spis treści

1. Wstęp.....	1
2. Incydent sieciowy	2
2.1. Definicja.....	2
2.2. Obsługa.....	2
2.2.1. Adres sieciowy i fizyczny klienta eduroam.....	2
2.2.2. Sesja uwierzytelnienia.....	2
2.2.3. Przekazanie zgłoszenia do dalszej obsługi.....	3
3. Przechowywanie informacji dotyczącej usługi eduroam.....	3
3.1. Logi DHCP.....	4
3.2. Zapisy uwierzytelniania serwera RADIUS.....	4
3.3. Narzędzia wspomagające.....	4
4. Informacja o użytkowniku.....	4
4.1. Tożsamość zewnętrzna i wewnętrzna (inner and outer identity).....	4
4.2. Atrybuty User-Name i Chargeable-User-Identity.....	5
5. Przykład rozwiązania wspomagającej obsługę incydentów.....	5
5.1. Ochrona przed zmianą adresu IP przez użytkownika.....	5
5.2. Utrzymywanie logów DHCP.....	6
5.3. Zapisy uwierzytelniania.....	6

1. Wstęp

Zgodnie z definicją europejskiej usługi eduroam [1] oraz z dokumentem *Koncepcja wdrożenia usługi eduroam w sieci PIONIER* [3], usługa ta opiera się w znacznym stopniu na wzajemnym zaufaniu instytucji współuczestniczących jej budowaniu. Kluczowym ogniwem zaufania jest gwarancja, że każda nieprawidłowość w zakresie funkcjonowania usługi zostanie szybko wyjaśniona. Dodatkowo, obsługiwane incydenty sieciowe mają służyć poprawie ogólnego bezpieczeństwa, dlatego duży nacisk kładzie się na współpracę ośrodków korzystających z usługi i na propagowanie zdobytych doświadczeń.

W niniejszym dokumencie opisujemy sposób reakcji na incydenty sieciowe. Podstawowym wymogiem działania przedstawionych procedur jest przechowywanie przez wszystkie jednostki uczestniczące w usłudze eduroam zapisów dotyczących uwierzytelniania oraz przypisywania adresów IP klientom eduroam.

Administratorzy eduroam muszą pamiętać, że funkcjonowanie mechanizmów udostępniania sieci bezprzewodowej w ich instytucji wpływa znacząco na obraz ogólnoeuropejskiej usługi eduroam. Dlatego, aby usługa funkcjonowała zgodnie z zaprojektowanym modelem, wszędzie muszą być stosowane zalecane zabezpieczenia.

2. Incydent sieciowy

2.1. Definicja

Incydentem sieciowym nazywamy zdarzenie w sieci, które nastąpiło w określonym czasie i wiązało się z dostępem do zasobów sieciowych przez klienta o konkretnym adresie IP. Zazwyczaj takie zdarzenie polega na niewłaściwym korzystaniu z sieci, np. naruszeniu jej regulaminu, rozsyłaniu spamów, rozpowszechnianiu poprzez sieć materiałów chronionych prawem autorskim, skanowaniu hostów w Internecie, próbach włamań itp. Często o incydencie sieciowym dowiadujemy się z powodu skargi innych użytkowników sieci, albo przez zgłoszenie nadużyć pochodzące z innych instytucji lub od właścicieli chronionych zasobów.

2.2. Obsługa

Incydent sieciowy dotyczy usługi eduroam, jeśli wiąże się z pulą adresów IP wykorzystywanych w eduroam. Wyjaśnienie incydentu sieciowego polega na powiązaniu zdarzenia z konkretnym użytkownikiem, a następnie w zależności od oceny stopnia stworzonego zagrożenia, pouczeniu użytkownika, lub zablokowaniu możliwości korzystania z usługi eduroam przez danego użytkownika lub przez wszystkich użytkowników danej domeny. Incydent związany ze złamaniem prawa może mieć konsekwencje w postaci dochodzenia prowadzonego przez organy ścigania i to do nich należy podjąć odpowiednie kroki formalnych.

2.2.1. Adres sieciowy i fizyczny klienta eduroam

Punktem wyjścia jest źródłowy adres IP incydentu. Na jego podstawie powinno być możliwe ustalenie, np. w oparciu o logi serwera DHCP, adresu fizycznego (MAC) klienta. Aby pierwsza faza obsługi incydentu funkcjonowała poprawnie, zalecane jest zapewnienie przez dostawcę eduroam w instytucji, by:

1. adres IP jednoznacznie identyfikował użytkownika w danym czasie – w tym celu *Polska Polityka eduroam* ([2]), w ślad za europejską, sugeruje, by instytucja udostępniająca sieć poprzez eduroam nie stosowała technologii NAT, która uniemożliwia właściwą obsługę incydentów sieciowych – dostawca nie jest wówczas w stanie powiązać zdarzenia z konkretnym użytkownikiem;
2. klient eduroam nie miał możliwości, po otrzymaniu dostępu do sieci, zmiany adresu IP i kontynuowania pracy w sieci z obcym adresem.

Pierwsze zalecenie jest stosunkowo łatwe w realizacji, trzeba jedynie dysponować odpowiednimi zapasami adresów sieciowych. Serwer DHCP odpowiedzialny za przydzielanie adresów internetowych korzysta wówczas ze wskazanej puli adresów publicznych.

Drugi element wymaga nieco większego wkładu pracy. Należy zagwarantować, by uprawnienia do korzystania z sieci wiązały się z parą (adres IP, MAC), a nie wyłącznie z adresem fizycznym. W tym celu należy domyślnie wyłączyć prawo korzystania z sieci, a w chwili przydzielania adresowego przez serwer DHCP otwierać dostęp sieciowy dla konkretnej pary IP i MAC.

Jeśli użytkownik samodzielnie zmieni sobie adres sieciowy na statyczny, to utraci dostęp do sieci. Gdyby nie był zaimplementowany powyżej opisany mechanizm, klient mógłby po takiej zmianie kontynuować pracę w sieci z nadanym sobie samodzielnie adresem IP. W takiej sytuacji w przypadku incydentu sieciowego administrator nie byłby w stanie wskazać winnego, lub wina spadłaby na niewłaściwego użytkownika.

2.2.2. Sesja uwierzytelnienia

Gdy są już znane adresy IP i MAC klienta, kolejną fazą identyfikacji incydentu jest powiązanie tych danych z konkretną sesją uwierzytelnienia. W tym celu należy znaleźć właściwą sesję uwierzytelniania na podstawie daty i czasu zdarzenia oraz adresu MAC. Z lokalnej konfiguracji eduroam wynika, na jakim serwerze mogło nastąpić uwierzytelnienie. Efektem tej fazy analizy incydentu jest identyfikator związany z uwierzytelnieniem konkretnego użytkownika. Należy tu wyróżnić dwie możliwe sytuacje dotyczące znalezionej sesji uwierzytelnienia:

1. wskazuje użytkownika lokalnego i w logach serwera widzimy pełny zapis sesji uwierzytelnienia – identyfikator dotyczy domeny obsługiwanej przez serwer RADIUS danej instytucji;
2. dotyczy użytkownika zewnętrznego – identyfikator zawiera domenę nie obsługiwaną lokalnie.

Gdy źródłem incydentu sieciowego jest użytkownik lokalny, to nie mamy do czynienia z naruszeniem dotyczącym gościnnego dostępu do usługi eduroam i dalsze postępowanie jest podobne jak w przypadku każdego innego nadużycia związanego z lokalną siecią. Istnieje wówczas możliwość samodzielnej, szczegółowej dalszej analizy źródła incydentu, gdyż znamy lokalne metody uwierzytelniania i potrafimy powiązać identyfikator uwierzytelnienia z konkretną osobą. O tym, że naruszenie zasad korzystania z sieci wiąże się z aktywnością użytkownika lokalnego można już świadczyć sam numer IP zdarzenia – jest tak, gdy użytkownicy eduroam są umieszczani w odpowiednich VLAN-ach.

W drugim przypadku możemy jedynie stwierdzić, że użytkownik posługujący się danym identyfikatorem uzyskał dostęp do sieci dzięki usłudze eduroam. W dalsze dochodzenie w sprawie incydentu sieciowego musi zostać włączony administrator serwera uwierzytelniania w domenie występującej w identyfikatorze.

2.2.3. Przekazanie zgłoszenia do dalszej obsługi

Jeśli analizowany incydent, dotyczący usługi eduroam, wiąże się z użytkownikiem z domeny zewnętrznej, należy przekazać informację o zdarzeniu:

- swojemu operatorowi regionalnemu, gdy dotyczy domeny polskiej,
- Koordynatorowi eduroam w Polsce, gdy dotyczy domeny zagranicznej.

Operator regionalny, w przypadku, gdy incydent wiąże się z domeną przekierowywaną na serwerze regionalnym do serwera instytucji podległej danemu operatorowi, dostarcza dane zdarzenia do administratora właściwej instytucji. W przeciwnym razie informacje o incydencie otrzymuje Koordynator eduroam w Polsce.

Koordynator przekazuje dane związane z incydem do właściwego administratora w instytucji, lub w przypadku incydentów zagranicznych, uruchamia kanały europejskiej usługi eduroam.

Administrator eduroam w macierzystej jednostce lokalizuje sesję uwierzytelnienia danego użytkownika, na podstawie otrzymanych danych: daty i godziny, adresu MAC oraz identyfikatora uwierzytelnienia.

Jeżeli incydent dotyczy złamania regulaminu lokalnego, etykiety sieciowej lub innego wykroczenia nie powodującego rozpoczęcia dochodzenia przez organy ścigania, to jednostka macierzysta powinna podjąć stosowne działania, tak by zapobiec powtórzeniu się tego typu sytuacji. Nagminne powodowanie incydentów przez osoby związane z daną instytucją może doprowadzić do zablokowania możliwości korzystania z usługi eduroam przez całą instytucję.

W przypadku poważnych incydentów, w sprawie których prowadzone jest dochodzenie, inicjatywę należy pozostawić właściwym organom ścigania, przekazując im stosowne informacje i opis procedur usługi eduroam. Operatorzy regionalni oraz Koordynator usługi eduroam w Polsce będą wspomagać instytucję w wyjaśnieniu sprawy.

Kontakt z operatorem regionalnym, Koordynatorem eduroam oraz administratorem eduroam w instytucji powinien odbywać się w sposób bezpieczny, zaleca się wsparcie komunikacji poprzez pocztę elektroniczną technologiami PGP lub S/MIME. Najwłaściwszym rozwiązaniem będzie zastosowanie mechanizmów wdrażanych przez projekt PKI Konsorcjum PIONIER.

Instytucja, na której terenie doszło do incydentu ma prawo tak zmodyfikować konfigurację usługi eduroam na swoim terenie, by dany użytkownik, lub wszyscy użytkownicy w danej domenie (jeśli nie jest możliwa jednoznaczna identyfikacja użytkownika, patrz p. 4) nie mieli dostępu do usługi do czasu wyjaśnienia problemu.

3. Przechowywanie informacji dotyczącej usługi eduroam

Zgodnie z *Polską Polityką eduroam* zapisy dotyczące korzystania z usługi eduroam muszą być przechowywane przez co najmniej sześć miesięcy. Aby była możliwa analiza incydentów sieciowych, według procedury opisanej w części 2, niezbędne jest przechowywanie zarówno danych dotyczących

przydzielania adresu IP w eduroam (zadanie serwera DHCP), jak i realizacji sesji uwierzytelnienia (rola serwera RADIUS). Administrator usługi eduroam w instytucji powinien być przygotowany, by szybko zidentyfikować incydent, dlatego zaleca się zbudowanie odpowiedniej infrastruktury zapisu zdarzeń DHCP i uwierzytelniania RADIUS. Najlepiej, by oba źródła miały wspólne miejsce logowania, np. plik, czy bazę danych. W przypadku uwierzytelniania trzeba również wziąć pod uwagę, że zapisy mogą się pojawić na jednym ze zdefiniowanych serwerów – podstawowym lub zapasowym.

Należy zadbać o to, by zegary wszystkich serwerów i urządzeń biorących udział w tworzeniu logów były synchronizowane przy pomocy usługi NTP.

3.1. Logi DHCP

Zapisy w logach DHCP są niezbędne do analizy zgłoszonych incydentów. Dlatego należy zagwarantować, by po pierwsze w logach znalazły się informacje dotyczące przydzielenia adresu IP adresowi MAC, po drugie, by logi były archiwizowane przez zalecany czas sześciu miesięcy.

3.2. Zapisy uwierzytelniania serwera RADIUS

Każde udane uwierzytelnienie dokonane przez serwer RADIUS musi zostać odnotowane i przechowane przez sześć miesięcy, analogicznie jak w przypadku zapisów DHCP. Serwer instytucji, na którym jest realizowana obsługa uwierzytelniania w konkretnej domenie musi po udanej weryfikacji danych uwierzytelniania zapisać w logu informację dotyczącą uwierzytelnienia. Powinna ona zawierać: datę i czas, identyfikator użytkownika, adres fizyczny karty. Typowo serwer FreeRADIUS zapisuje również nazwę lub adres IP urządzenia sieciowego (Access Point, kontroler lub serwer pośredniczący), za pośrednictwem którego zostało przekazane zlecenie uwierzytelnienia. Zazwyczaj w instytucji działają dwa serwery, podstawowy i zapasowy – oba serwery muszą identycznie zapisywać informacje o uwierzytelnieniach. Należy rozważyć możliwość utrzymywania zapisów uwierzytelnień w relacyjnej bazie danych, w ten sposób dane będą dostępne w jednym miejscu, co ułatwi lokalizację potrzebnej informacji. W 5.3 opisujemy, jak można taką funkcjonalność zrealizować w oprogramowaniu FreeRADIUS.

3.3. Narzędzia wspomagające

Jeśli zostały wdrożone procedury opisane w 3.1. i 3.2, to dysponując pełną, łatwo dostępną informacją dotyczącą pracy DHCP oraz serwerów RADIUS w usłudze eduroam, można przygotować proste skrypty operujące na tych danych. Będzie to duże udogodnienie pracy, nie tylko przy rozwikływaniu incydentów sieciowych, również przy zbieraniu statystyk.

4. Informacja o użytkowniku

Jeżeli mamy do czynienia z incydentem sieciowym, w którym uczestniczył użytkownik zewnętrzny, to po dokonaniu powiązania adres IP → adres MAC → identyfikator użytkownika, uzyskany napis użytkownik@domena najczęściej nie wskazuje jeszcze konkretnego użytkownika. Możemy mieć jedynie pewność, że chodzi o użytkownika w danej domenie. Nie oznacza to, że identyfikator logowania nie jest istotny dla administratora serwera tej domeny.

4.1. Tożsamość zewnętrzna i wewnętrzna (*inner and outer identity*)

Popularne metody uwierzytelnienia, z których korzysta większość instytucji uwierzytelniających, to PEAP i EAP-TTLS. Cechą wspólną tych metod jest przekazywanie właściwych danych uwierzytelniania w tunelu SSL, w zaszyfrowanym atrybucie EAP-Message. Dane te są przekazywane w typowym pakiecie RADIUS, zawierającym atrybut User-Name, na podstawie którego jest dedukowany sposób obsługi zlecenia. W tym przypadku atrybut User-Name przynosi nazwę tzw. tożsamości zewnętrznej użytkownika, często ma wartość anonymous@domena, lub @domena. Nazwa ta nie jest unikatową nazwą użytkownika. Unikatowy identyfikator użytkownika jest dostępny dopiero po rozszyfrowaniu komunikatu z atrybutu EAP-Message. Rozszyfrowanie jest realizowane na serwerze macierzystym użytkownika, więc tylko tam, w zapisach pracy serwera RADIUS, można znaleźć pełną informację dotyczącą uwierzytelnienia.

Dysponując informacją związaną wyłącznie z pośrednictwem w realizacji zlecenia uwierzytelnienia, nie jesteśmy w stanie jednoznacznie wskazać użytkownika. Nawet jeśli identyfikator nie ma postaci `anonymous@domena`, czy `@domena`, lecz np. `stud1357@domena`, nie można traktować go jako wiążącego wskazania konkretnego użytkownika – za chwilę inny użytkownik może użyć takiego samego identyfikatora w polu zewnętrznej tożsamości, albo użytkownik, który spowodował problemy, będzie ubiegał się o dostęp do sieci wysyłając inną nazwę w polu `User-Name`. Należy zdawać sobie z tego sprawę, gdy reakcją na incydent jest chęć odcięcia dostępu do sieci poprzez odrzucanie zleceń zawierających określoną nazwę użytkownika.

4.2. Atrybuty `User-Name` i `Chargeable-User-Identity`

Na spotkaniach operatorów europejskiej usługi eduroam było dyskutowane wykorzystanie atrybutu `Chargeable-User-Identity` (RFC 4372, [5]). Wartość tego atrybutu, zgodnie z definicją we wskazanym RFC ma przenosić informację, pozwalającą na jednoznaczną identyfikację użytkownika, przy jednoczesnym zachowaniu jego anonimowości wobec osób spoza instytucji macierzystej. Oznacza to, że w atrybucie można umieścić napis typu lokalny identyfikator (np. identyfikator w bazie kadrowej, czy studenckiej) – taka informacja nie ma żadnego praktycznego znaczenia dla osób z zewnątrz. Jeśli w pakiecie `Access-Accept` pojawi się atrybut `Chargeable-User-Identity` (CUI), to administrator zdalnego serwera RADIUS, pośredniczącego w obsłudze zlecenia może mieć pewność, że ma do czynienia z konkretnym użytkownikiem po ustaleniu łańcucha adres IP, MAC, identyfikator CUI. RFC 4372 ustala, że atrybut CUI może zostać zwrócony w odpowiedzi `Access-Accept` tylko wówczas, gdy atrybut ten pojawił się w odpowiednim zapytaniu (`Access-Request`). Na ogół oznacza to, że w zleceniach jest wysyłany atrybut CUI z pustą wartością.

Korzystanie z atrybutu CUI jest zalecane w polskiej usłudze eduroam. Jeśli chcemy wprowadzić funkcjonalność CUI musimy uwzględnić w konfiguracji serwera FreeRADIUS dwie rzeczy:

1. podczas uwierzytelniania serwer RADIUS musi zakładać, że atrybut CUI będzie wysyłany, dlatego należy na etapie sesji uwierzytelnienia pobrać jego wartość, np. odczytać wartość lokalnego identyfikatora użytkownika podczas współpracy z bazą danych;
2. po pozytywnym uwierzytelnieniu, należy sprawdzić, czy w zleceniu pojawił się atrybut CUI, jeśli tak, to w odpowiedzi jest umieszczana właściwa wartość atrybutu CUI, na podstawie ustaleń z p. 1 (odbywa się to w sekcji `post-auth` konfiguracji FreeRADIUS-a).

Jeżeli przewidujemy wysyłanie atrybutu CUI, to wskazana jest usunięcie atrybutu `User-Name` z odpowiedzi.

5. Przykład rozwiązania wspomagającej obsługę incydentów

Poniżej opisujemy, jak można przygotować się do realizacji zadań związanych z rozwikłaniem incydentów sieciowych.

Przedstawione mechanizmy przechowywania danych usługi eduroam zostały oparte na usłudze `syslog-ng` i na bazie `MySQL`.

5.1. Ochrona przed zmianą adresu IP przez użytkownika

Gdy chcemy zagwarantować, by adres IP, po jego nadaniu konkretnemu adresowi MAC, nie został zmieniony samodzielnie przez zaradnego użytkownika, to należy przede wszystkim zapewnić ochronę dostępu do sieci w określonych przestrzeniach adresowych. Uzyskanie adresu IP przez klienta nie może dawać od razu prawa korzystania z otwartej sieci. Jeśli np. filtrujemy pakiety sieciowe za pomocą mechanizmu `iptables` i domyślnie klienci w VLAN-ie 11 nie mają otwartej sieci, to użytkownik o MAC-u `aa:bb:cc:dd`, który otrzymał adres `11.22.33.44` w tym VLAN-ie uzyska dostęp do sieci po dodaniu reguł:

```
-A FORWARD -s 11.22.33.44 -i vlan11 -o eth0 -m mac --mac-source aa:bb:cc:dd
-j ACCEPT
-A FORWARD -d 11.22.33.44 -i eth0 -o vlan11 -j ACCEPT
```

Przykładowa implementacja rozwiązania pozwalającego na ochronie przed samodzielną zmianą adresu IP przez użytkowników eduroam została opisana w dokumencie [4]. W przedstawionym podejściu zasto-

sowano pakiet `dnsmasq`, realizujący funkcję serwera DHCP oraz przekierowującego DNS-a. Specyfiką serwera `dnsmasq` jest możliwość powiązania zdarzenia przydzielenia adresu sieciowego z wywołaniem wskazanego skryptu. Zadaniem tego skryptu jest otwarcie połączenia sieciowego dla danego klienta.

Można również korzystać z funkcji wiązania adresów IP i MAC dostępnych w niektórych urządzeniach sieciowych takich jak przełączniki lub kontrolery bezprzewodowe.

5.2. Utrzymywanie logów DHCP

Serwer DHCP można skonfigurować tak, by zapis aktywności systemu był realizowany poprzez usługę `syslog`. Na ogół najwygodniej jest, by serwer DHCP logował do zdalnego serwera, dedykowanego do obsługi zapisów pracy zarówno DHCP, jaki i serwerów RADIUS. Jeśli obsługa logowania na takim serwerze jest realizowana w oparciu o system `syslog-ng`, to możemy zastosować odpowiednie filtry oraz skrypty, by zgodnie z potrzebą przetworzyć zapisy. Np.

```
source s_net_udp { udp(); };
filter f_eduroam { netmask( "11.22.33.44/255.255.255.255" ); };
destination d_eduroam { program("/opt/local/scripts/eduroamlogger.pl"); };
log { source(s_net_udp); filter(f_eduroam); destination(d_eduroam); };
```

ustala, że jeśli źródłem logów jest serwer 11.22.33.44, to zostaje uruchomiony skrypt `/opt/local/scripts/eduroamlogger.pl`. Skrypt ten może dodatkowo zinterpretować dane wejściowe i na ich podstawie przygotować instrukcje SQL by załadować dane do bazy MySQL. W ten sposób dane dotyczące powiązania MAC – IP mogą być zapisywane w specjalnej tabeli bazy danych przeznaczonej do gromadzenia informacji o usłudze eduroam.

5.3. Zapisy uwierzytelniania

Jeśli w konfiguracji oprogramowania FreeRADIUS zdefiniowano blok `detail auth_log {...}`, to należy jedynie zadbać, by w sekcji `post_auth { ... }` znalazło się wskazanie `auth_log` (najlepiej blisko końca bloku, po instrukcjach modyfikujących zawartość pakietu odpowiedzi, by zapis logowania miał zawartość zgodną z przekazywaną klientowi).

FreeRADIUS pozwala również zdefiniować logowanie poprzez bazę SQL. Służy do tego sekcja `sql_log`, ustalająca konfigurację dla modułu `rlm_sql_log`. Zasada działania jest następująca:

1. moduł dopisuje instrukcje SQL do wskazanego pliku,
2. plik jest źródłem danych dla specjalnego programu pakietu FreeRADIUS – `radsqrelay`.

Przykładowo kod:

```
sql_log {
  path = "${radacctdir}/sql-relay"
  postauth_table = "freeradiusauth"
  Post-Auth = "INSERT INTO ${postauth_table} \
    (user,reply,nasip,cliip,called,calling,date,radius,vlan) VALUES \
    ('${User-Name}', \
    '${reply:Packet-Type}', \
    '${NAS-IP-Address}', \
    '${Client-IP-Address}', \
    left(ucase(replace(replace(replace(replace('${Called-Station-Id}','-', ''),'.',''),':',' ')), 12), \
    left(ucase(replace(replace(replace('${Calling-Station-Id}','-', ''),'.',''),':',' ')), 12), '%S', \
    'radius1.umk.pl', '${reply:Tunnel-Private-Group-Id}');"
}
```

powoduje, że do tablicy `freeradiusauth` zostanie zapisany rekord dotyczący danej sesji uwierzytelnienia. Rekord ten będzie zawierał informację, na jakim serwerze nastąpiło uwierzytelnienie. Zapasowy serwer powinien tak samo zapisywać informację do bazy SQL.

Materiały towarzyszące

- [1] *eduroam Service Definition*, <http://www.eduroam.org/downloads/docs/GN2-07-328-eduroam-policy-for-signing-Final2-2.pdf>
- [2] *Polska Polityka eduroam (regulamin usługi eduroam)*, <http://www.eduroam.pl/polityka>
- [3] *Koncepcja wdrożenia usługi eduroam w sieci Pionier*, T. Wolniewicz, M. Górecka-Wolniewicz, Z. Oltuszyk
- [4] *Zapobieganie samowolnej zmianie IP*, http://www.eduroam.pl/Dokumentacja/eduroam_zapobieganie_zmianie_IP.pdf
- [5] *Chargeable User Identity*, RFC 4372