GDPR e applicazioni

“ Casi d'uso: network access, wi-fi e eduroam „

Daniele Albrizio
albrizio@units.it

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Nota sul deployment

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Gestisco radius server e rete wireless e 802.1x cablata
- DB locale con account temporanei e banning di utenti e dispositivi
- Directory di backend e backup dei server gestiti da **altri** sistemisti

Strumenti

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- FreeRADIUS 3
- Postgresql
- php scripts, bash, munin
- ISC dhcp
- Controller Wireless HPE Aruba e Cisco

Obiettivi

- Minimizzazione dei dati trasferiti (GDPR/Privacy)
- Garantire integrità dei log
- Garantire cancellazione dei log dopo il periodo di retention

Obiettivi

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Minimizzazione dei dati trasferiti (GDPR/Privacy)
  - Filtri sugli attributi
  - Pseudonimizzazione dello username
  - Disabilitare l’auth_log in quanto conserva gli attributi non richiesti e sovrabbondanti in ingresso (disabilitato per default)

Obiettivi

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Garantire integrità dei log
  - Firma e marca temporale di una TSA non sotto il mio controllo
  - Accesso autonomo dell'utente ai propri log
    - Solo utenti del proprio IdP

Obiettivi

- Garantire cancellazione dei log dopo il periodo di retention
  - Stabilire i tempi di retention
    - Incident response
    - Troubleshooting problemi utente
      - Ticket escalation
    - Troubleshooting problemi dei sistemi
    - Tempi di federazione (attualmente 6 mesi)
  - Aggiungere (o ridurre) i tempi di retention del backup
  - Cron jobs di cancellazione

Difficoltà di analisi

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Analizzare a fondo le procedure in essere
- Discernere sulle motivazioni, sugli interessi e sulla reale utilità per i vari soggetti coinvolti
  - Sistemisti
  - Utenti
  - Titolare (interessi istituzionali)
- Analizzare bene tutti i flussi dei dati

Registro trattamento

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Può venirci in aiuto fra le altre cose per
  - ...
  - Individuazione dei diversi tipi di trattamento
  - Individuazione di quali dati vengono trattati (natura dei dati)
  - Individuazione dell'utenza interessata
  - Individuazione di trattamenti transnazionali e extra UE
  - ...

Linee guida CODAU

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Linee guida CODAU
  - Username, MAC, IP, timestamp
- Caso reale
  - Username, MAC, IP, timestamp
  - AP collegato (geolocalizzazione), application profiling, quantità di dati scambiati,
  - Nome della rete a cui ci si collega
  - Causa della disconnessione

Attributi passati

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Caso reale
  - Istituzione di appartenenza (Operator-Name)
  - Nazione di collegamento (eduroam-SP-Country)
  - Tipo di dispositivo usato (Aruba-Device-Type)
  - ...

Esempio di registro

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Esempio imperfetto pubblicato su

https://github.com/speedj/Registro-Trattamento-eduroam

- Sono benvenute domande, correzioni e considerazioni **da casa o in pausa caffè**

Anonimizzare lo user

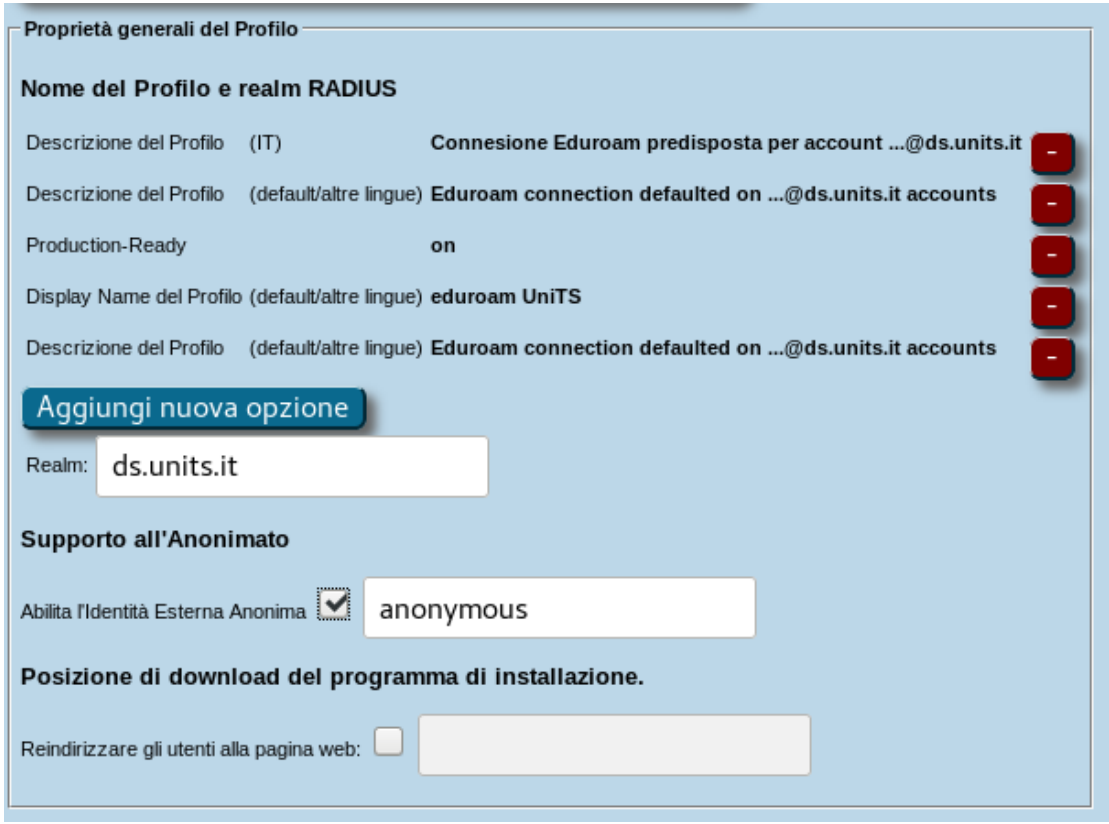
UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Anonimizzare lo User-Name senza perdere la tracciabilità della sessione fra IdP e RP
  - Configurare l'**Anonymous outer identity**
  - Rilasciare l'**Operator-Name**
  - Supportare e valorizzare **Chargeable-User-Identity**

Outer Identity anonima

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Impostare su eduroamCAT



- Eliminare eventuali riscritture della outer con la inner sul proprio IdP

Usare il CUI

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Chargeable-User-Identity
- Pseudonimo dello User-Name alla stregua di ComputedID o Stored PersistentID di tipo targeted di Shibboleth

```
%{sha1:
    ${policy.cui_hash_key}
    %{tolower:%{User-Name}
    %{%{outer.request:Operator-Name}}
}
```

Implementare il CUI


```
server default {
    authorize {
        filter_username
        operator-name
        cui
    }
```

Implementare il CUI


```
post-auth {
    cui
    eduroam_log
     Post-Auth-Type REJECT {
        eduroam_log
        attr_filter.access_reject
    }
}
```

Implementare il CUI


```
pre-proxy {
   update proxy-request {
      #Operator-Name := "1units.it"
   }
   operator-name
   cui
   attr_filter.pre-proxy
}
} # end default virtual server
```

Implementare il CUI


```
server inner-tunnel {
   post-auth {
      cui-inner
      eduroam_inner_log
      Post-Auth-Type REJECT {
         eduroam_inner_log
         attr_filter.access_reject
      }
   } # end post-auth
} # end server inner-tunnel
```

Implementare il CUI

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

clients.conf

```
client ap-1 {
    ipaddr                  = 172.16.199.1
    netmask                 = 32
    secret                  = yoursecret12345
    nas_type                = other
    #virtual_server         = eduroam
    Operator-Name           = 1units.it
    add_cui                 = yes
}
```

Implementare il CUI

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

File policy.d/cui

```
cui_hash_key = "exampleString1234-CHANGE-ME"
cui_require_operator_name = "yes"

#nella sezione cui.post-auth commentare
#       if (&reply:Chargeable-User-Identity) {
#               # Force User-Name to be the User-Name from
#               # the request
#               update {
#                       &reply:User-Name := &request:User-Name
#               }
#               cuisql
#       }
```

Implementare il CUI

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

/var/log/freeradius/eduroam-log

2018-05-22 12:22:29 eduroam-auth
USER=555@ujep.cz ORG=DEFAULT
CSI=aa-bb-cc-dd-ee-ff
NAS=lapB1p4:eduroam
CUI=0x396139326538346565636…
RESULT=OK
...
MSG=Request Denied RESULT=FAIL

Utente straniero presso la propria infrastruttura

Implementare il CUI

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

/var/log/freeradius/eduroam-log-inner

2018-04-10 17:21:46 user-auth
USER=s555@ds.units.it VISINST=1units.it
CSI=CC-DD-EE-FF-AA-BB
NAS=lapH3-3A:eduroam
CUI=0x396139326538346565636374422346…
RESULT=OK

Autenticazione di un proprio utente

Implementare il CUI

- eduroam-log e eduroam-inner-log sono due istanze di linelog

```
linelog eduroam_log {
    filename = ${logdir}/eduroam-log
    format = ""
    reference = "eduroam_log.%{%{reply:Packet-Type}:-format}"
    eduroam_log {
        Access-Accept = "%S eduroam-auth USER=%{User-Name}
          ORG=%{request:Realm} CSI=%{%{Calling-Station-Id}:-Unknown Caller Id}
          NAS=%{%{Called-Station-Id}:-Unknown Access Point}
          CUI=%{%{reply:Chargeable-User-Identity}:-Unknown}
          MSG=%{%{EAP-Message}:-No EAP Message} RESULT=OK"

        Access-Reject = "%S eduroam-auth USER=%{User-Name}
          ORG=%{request:Realm} CSI=%{%{Calling-Station-Id}:-Unknown Caller Id}
          NAS=%{%{Called-Station-Id}:-Unknown Access Point}
          CUI=%{%{reply:Chargeable-User-Identity}:-Unknown}
          MSG=%{%{reply:Reply-Message}:-No Failure Reason} RESULT=FAIL"
    }
}
```

Implementare il CUI


```
linelog eduroam_inner_log {
    filename = ${logdir}/eduroam-log-inner
    format = ""
    reference = "inner_auth_log.%{%{reply:Packet-Type}:-format}"
    inner_auth_log {
        Access-Accept = "%S user-auth USER=%{User-Name}
            VISINST=%{request:Operator-Name}
            CSI=%{%{Calling-Station-Id}:-Unknown Caller Id}
            NAS=%{%{Called-Station-Id}:-Unknown Access Point}
            CUI=%{%{%{reply:Chargeable-User-Identity}:-%{outer.reply:Chargeable-User-
Identity}}:-Local User}
            RESULT=OK"

        Access-Reject = "%S user-auth USER=%{User-Name}
          VISINST=%{request:Operator-Name}
          CSI=%{%{Calling-Station-Id}:-Unknown Caller Id}
          NAS=%{%{Called-Station-Id}:-Unknown Access Point}
          CUI=%{%{%{reply:Chargeable-User-Identity}:-%{outer.reply:Chargeable-User-Identity}}:-
Local User}
          RESULT=FAIL"
    }
}
```

Filtrare gli attributi

- Ogni Vendor ha i suoi attributi
  - WLAN-Group-Cipher, WLAN-Pairwise-Cipher, Tunnel-Private-Group-Id, Tunnel-Type, Siemens-VNS-Name, Siemens-Topology-Name, Siemens-BSS-MAC, Siemens-AP-Serial, Siemens-AP-Name, Ruckus-SCG-CBlade-IP, Huawei-Version, Huawei-Startup-Stamp, H3C-NAS-Startup-Timestamp, H3C-Product-ID, Colubris-AVPair, Cisco-AVPair, Ascend-Home-Agent-UDP-Port, Aruba-Location-Id, Aruba-Device-Type, Aruba-AP-Group, Aruba-Auth-Survivability, Airespace-Wlan-Id

Filtrare gli attributi

- Filtrare solo quelli che servono secondo il principio di necessità (eduroam RP)

```
# pre-proxy
DEFAULT
    User-Name =* ANY,
    EAP-Message =* ANY,
    Message-Authenticator =* ANY,
    NAS-IP-Address =* ANY,
    NAS-Identifier =* ANY,
    State =* ANY,
    Proxy-State =* ANY,
    Operator-Name =* ANY,
    Class =* ANY,
    Calling-Station-Id =* ANY,
    Called-Station-Id =* ANY,
    Chargeable-User-Identity =* ANY
```

Filtrare gli attributi

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Evitare di trattare dati personali non voluti (eduroam RP)

```
# post-proxy
DEFAULT
    Reply-Message =* ANY,
    Proxy-State =* ANY,
    EAP-Message =* ANY,
    Message-Authenticator =* ANY,
    MS-MPPE-Recv-Key =* ANY,
    MS-MPPE-Send-Key =* ANY,
    State =* ANY,
    Calling-Station-Id =* ANY,
    Operator-Name =* ANY,
    User-Name =* ANY,
    Class =* ANY,
    Chargeable-User-Identity =* ANY
```

Marca temporale log

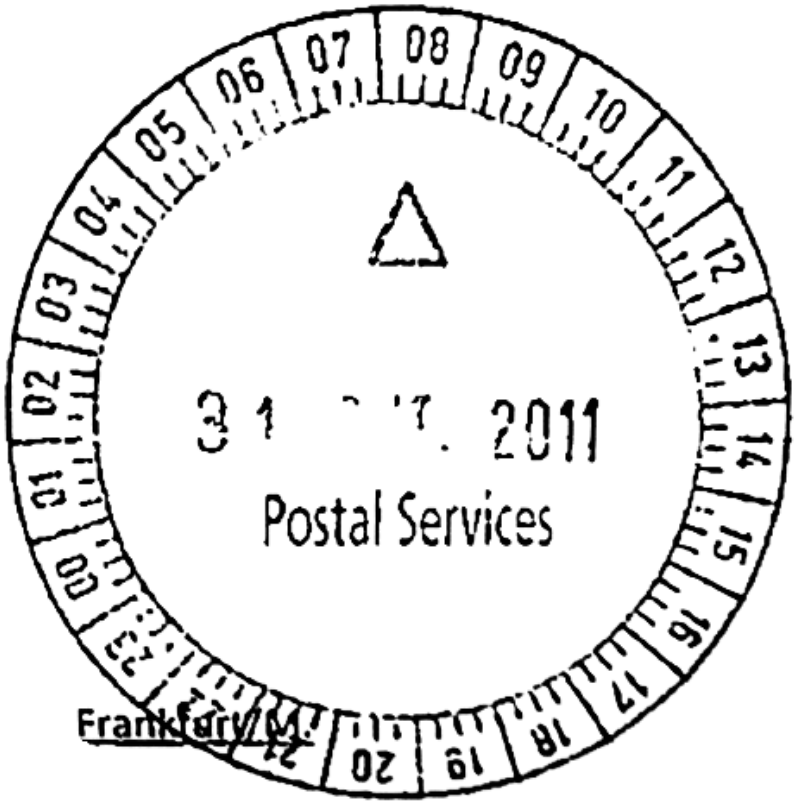
UNIVERSITÀ
DEGLI STUDI DI TRIESTE

```
# La riga seguente a cron:
# Firma gli hash sha1 dei file di accounting
01 03 * * * cd /etc/adminscripts/radius/log_tim…
                estamp_cert ; ./log_timestamp_cert.sh
```

Marca temporale log

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

https://github.com/speedj/log_timestamp_cert/



CC-BZ-SA Jan Schejbal

Marca temporale log

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

...
91d20126961e28d20be2eb170a6f5c39a115e5b2
/var/log/radius/radacct/193.206.158.71/pre-proxy-detail-2018
747a771940dc6b9a170069e9c72650487028d7bc
/var/log/radius/radacct/193.206.158.71/reply-detail-20180521
Verify timestamp using -> openssl ts -reply
-in /var/log/radius/radacct/loghashes.20180527.sha1.tsr
-text

Verify signature using -> openssl ts -verify -data
/var/log/radius/radacct/loghashes.20180521.sha1
-in /var/log/radius/radacct/loghashes.20180521.sha1.tsr
-CAfile cacert.pem
-untrusted tsa.crt

Marca temporale log

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

radius:/var/log/radius/radacct# openssl *ts -verify*
-data /var/log/radius/radacct/loghashes.20180521.sha1
-in /var/log/radius/radacct/loghashes.20180521.sha1.tsr
-CAfile cacert.pem -untrusted tsa.crt
Verification: OK

openssl *ts -reply* -in loghashes.20180521.sha1.tsr -text
...
Serial number: 0x0807C0
Time stamp: May 22 01:02:08.215271 2018 GMT
Accuracy: 0x01 seconds, 0x01F4 millis, 0x64 micros
...

Grazie

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Per l'attenzione e la pazienza

Thank You
CC-BY-NC-ND 2.0 Avard Woolaver

Links

- Linee guida in materia di privacy e protezione dei dati personali in ambito universitario
- Eduroam: installayione di base. Pasquale Mandato. Garr Workshop 2016
- CUI implementation for Radiator

Licenza

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Alcuni contentuti, come specificato sugli stessi, sottostanno ad una diversa licenza d'uso Creative Commons