Come gestire la sicurezza del collegamento ad eduroam

Daniele Albrizio
Università degli Studi di Trieste

Indice

- Security claim WizCase, Treathpost, ecc.
- Origine dei claim
- Approfondimento e contestualizzazione
- eduroamCAT
- Possibili soluzioni
- Pratiche comuni
- Raccomandazioni

Sensazionale

- “multiple issues affecting the configuration of the eduroam network” WizCase
- “most of the universities with misconfigured networks”
- “devices automatically sending their stored credentials [..] to the evil twin” WizCase
  - Questo avviene quando gli utenti (o i dispositivi) accettano qualsiasi certificato. Il tunnel TLS viene compromesso. Si espongono le credenziali PAP in chiaro o il challenge MS-CHAPv2 (RC4)

Precisazioni

- “It is important to note that the **exposure isn’t due to a technical vulnerability from eduroam**’s services/technology but from **wrong configuration instructions given to users by the admins** of each university.” WizCase
- “Thank you[…]. We are indeed occasionally made aware of eduroam Identity Providers who do not follow the requirements of the eduroam policy, and leave their own users unprotected. […] **this is an unacceptable behaviour on their end**.”

Responsible disclosure?

- “Following this reply, our team had decided to postpone the publication of their findings, hoping eduroam might have informed their users after our reach out.” WizCase
  - Problema noto almeno dal 2018 (disclosure?)
  - Coordinamento di realtà accademiche transnazionali
  - Autonomia dei singoli Identity Providers (IdP)
  - Problemi oggettivi correlati alle dimensioni imponenti della user-base e alla ridotta quantità di tecnici/helpdesk

eduroam Advisories

- https://eduroam.org/eduroam-advisories/ 8 in 13 anni
  - WPA related
    - FragAttacks 2021
    - KRACK + WPA3-Enterprise with 192-Bit Security 2018
    - Usare WPA2/AES+PMF optional o WPA3 – disabilitare WPA/TKIP e WPA2/TKIP (2009-2018)
  - eduroam SP
    - RFC5580 (Operator-Name and others) 2011
    - Do not use web logins for eduroam 2009
  - eduroam IdP
    - Recommendation regarding internationalised domain names for eduroam realms 2009

Evidenze

- Una ricerca per una tesi UniTS del 2018 (Alberto Bartoli, Eric Medvet, Filippo Onesti)
  - 36% degli utenti non usavano CAT anche se adottato e pubblicizzato dall'istituzione
    - 29,4% studenti - 4,3% staff
    - 2,3% roaming-in di altri enti
- Non mi aspetto cambiamenti sostanziali nel 2021 se non nel numero delle password in chiaro (android downgrade GTC). Ma...

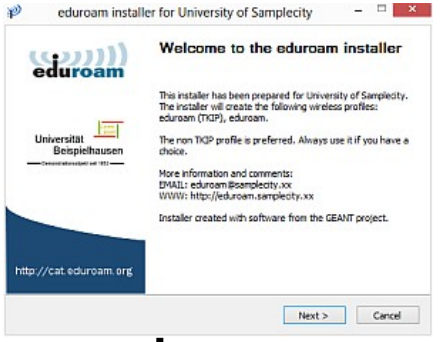
Evidenze

- 2020 survey con 1000 utenti (prof. Bartoli)
  - 50% configurazioni corrette con eduroamCAT
- *Perché? Proliferazione di dispositivi? Utenti insofferenti per la complessità?*
- 2020 survey 311 guide di 69 istituzioni accademiche
  - 40% contengono informazioni che possono portare a configurazioni insicure
- *Su questo possiamo/dobbiamo lavorarci*

Azioni intraprese (UniTS)

- Campagne di **avviso** (mail) **di configurazione errata** basate sull'outer identity **anonymous<versione profilo>**@ds.units.it hanno portato un beneficio temporaneo.
  - Nuovo dispositivo o aggiornamento comporta molto spesso il reinserimento delle credenziali che gli utenti rifanno **senza installer**
- Paradigma "bast che funz"

Premessa 0: usare CAT, usare CAT



- Le impostazioni di una rete Wi-Fi Enterprise sono troppe per essere configurate a mano da parte di un utente.
- Necessario un profilo: GÉANT eduroamCAT per gli amministratori è un web multi-tenant che permette di configurare e distribuire profili Wi-Fi e cablati generati automaticamente per le piattaforme più diffuse
  - Info di contatto, QR-code, statistiche sul download, forzare o suggerire un realm, forzare una determinata outer identity, EAP-Types, SSID multipli, CA chain, anchor sul DN del certificato, 802.1x cablato, ...

Nessun controllo sul supplicant

- Il Wi-Fi non è (e non è mai stato) gestito in maniera carrier grade
- È nato per lo Home Office (SOHO) senza alcun tipo di controlli (open o con una chiave condivisa wep come ricorderete)
- L’amministratore della rete non ha modo di sapere se l’utente abbia configurato il dispositivo con un apposito profilo o lo abbia configurato più o meno correttamente a mano.

Possibili soluzioni SOFT

- AKA come forzare gli utenti a usare il CAT installer:
  - Campagne di comunicazione
  - enforcement di identità esterne anonime prestabilite (non è comunque possibile essere sicuri che l'utente non abbia immesso a mano proprio quella identità esterna copiandola dal suo compagno)
  - Campagne di comunicazione
  - Campagne di comunicazione

Adesivi e pagine di auto-aiuto

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Abilitare la rete di roaming mondiale

eduroam

eduroam **NON** funziona **come** il Wi-Fi a casa, in hotel o negli esercizi commerciali: cos'è eduroam?

Collegati ad eduroam in 3 semplici passi

*(perché è **fondamentale** seguire questi passi?)*

Seleziona il tuo ruolo:

Nuovo studente UniTS (*iscritto di recente*)

Studente UniTS

Docente e altro personale UniTS

Utente di altra università/ente di ricerca con account eduroam

Partecipante ad eventi temporanei privo di account eduroam

Informazioni complete e dispositivi particolari | FAQ

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Copyright info on last page

Studente

1. Sul dispositivo da collegare, scarica ed esegui il configuratore eduroamCAT.

Scarica

2. Inserisci lo username nella forma sXXXXXXX@ds.units.it e la tua password quando richiesti durante l'installazione.

3. Naviga da qualsiasi parte del mondo.

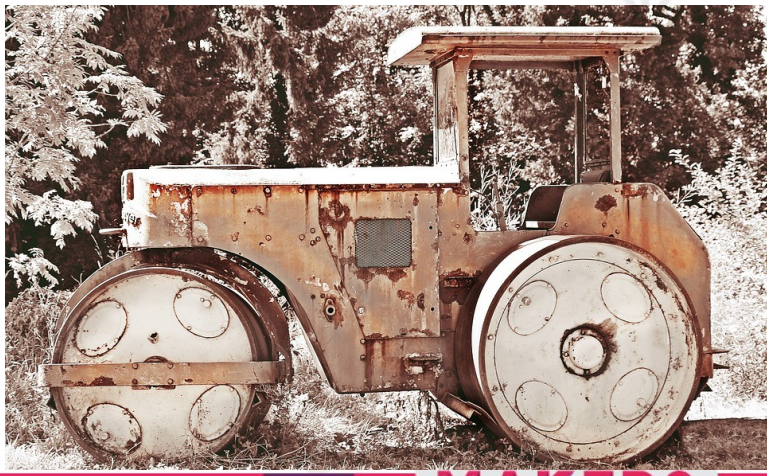
Informazioni complete e dispositivi particolari | FAQ

Possibili soluzioni HARD

- Rispondere al “bast che funz” con il “bast che NON funz”
  - Autorizzazione in base alla outer identity
  - Rifiutare PAP (TTLS-PAP)
- Soluzioni definitive ma (troppo) onerose o impattanti
  - Autenticare TTLS con una PKI interna
  - Cominciare ad usare WPA3v2 Trust Override Disable (TOD) – STRICT policy (?)

Pianificare il phase-out dei vecchi dispositivi

- Molti attacchi (cypher downgrade, KRACK, ecc…) non sono eseguibili su dispositivi nuovi
- Alcuni dispositivi vecchi non sono configurabili con CAT
- Non facciamo i buoni, abbiamo il coraggio di dire che il dispositivo è troppo vecchio e non più supportato:
  - Per i dispositivi BYOD
  - Per i dispositivi dell’amministrazione
  - Per i **nostri access point/controller**



Pratiche comuni

- Far verificare al client il CN del certificato
- Preferire WPA3 enterprise only (MFP obbligatorio, ~~SHA1~~, ~~TKIP~~, ~~WEP~~) o in transition mode (~~TKIP~~, ~~WEP~~)
- Preferire PEAP-MSCHAPv2 o EAP-TLS a TTLS-PAP
  Se il backend è openldap è comunque possibile
- Pagina eduroam.TLD con informazioni chiare e sintetiche sul servizio
- Campagne informative per utenti e per i tecnici **facendosi aiutare** dall'ufficio comunicazione

Incompatibilità e problemi implementativi

- WPA3 802.11r e alcuni dispositivi fino al 2018
- WPA3 con chiavi a 192bit
- eduroamCAT e Android 11+ (network profile)
- geteduroam e Android 10 (MIME types)
- Protected Management Frame PMF **enforcement**
- Samsung Android e identità esterna anonima diversa da anonymous@tld (solved)

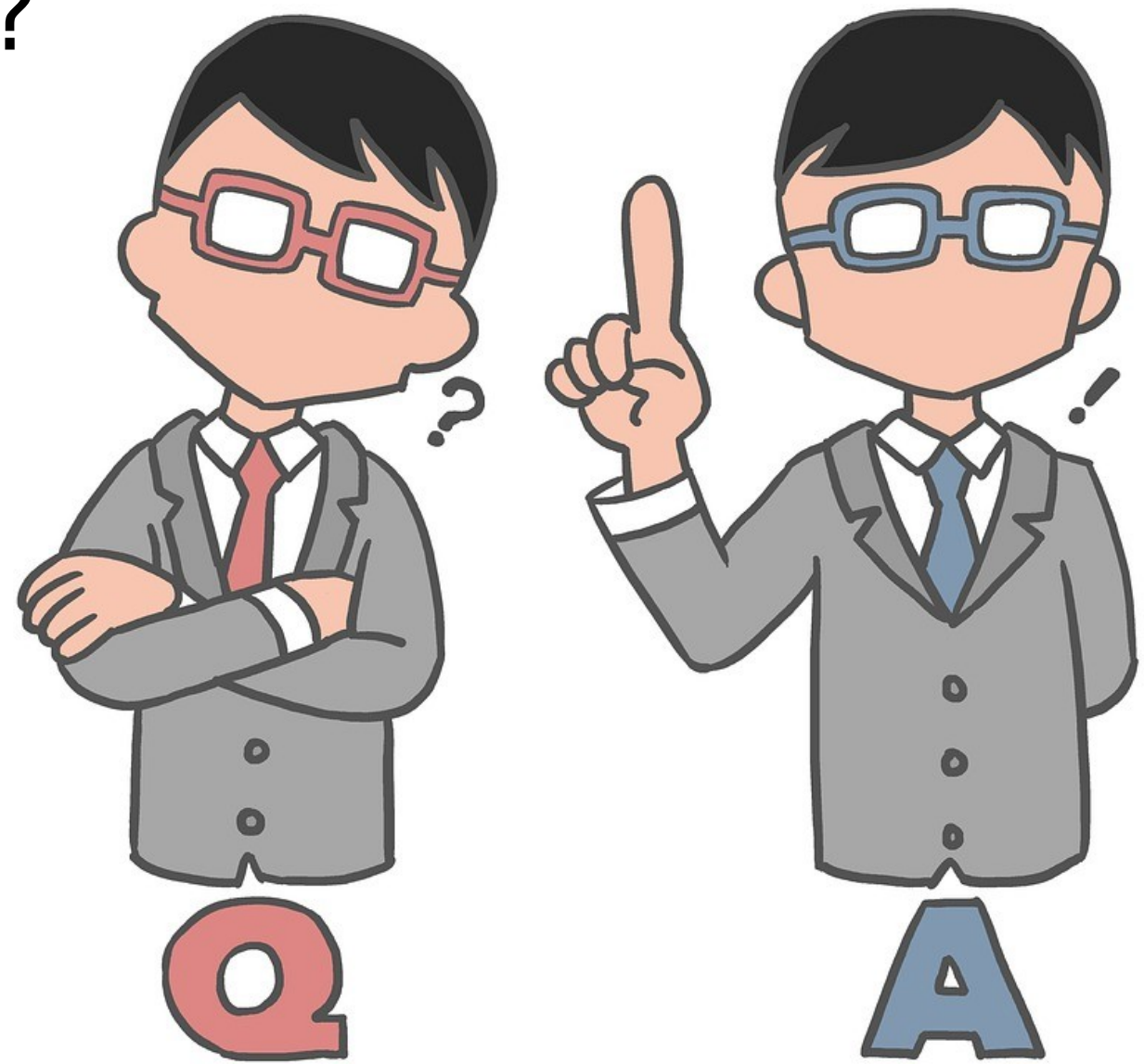
Misurare, analizzare

- Misurare, graficare, analizzare
  - le performance della propria infrastruttura
  - il tipo e la quantità di client collegati
  - numero di client per Access Point
- Tenere traccia dei cambi di configurazione per poter correlare problemi sui client o client scollegati.
- Ogni tanto guardare i log per stranezze/novità

Quindi

- Usare (bene) **eduroamCAT**
- Rivedere le proprie **guide** (compliance con le best practices)
- Vigilare la propria rete e riconfigurarla con quanto si trova sulle **guide ufficiali eduroam.org**

Domande?



Virtual Coffee Break 12:45

Links

- WizCase advice 2021
- Threatpost article 2021
- Understanding Server Authentication in WPA3 Enterprise 2020
- Evil twins and WPA2 Enterprise: A coming security disaster? 2018
- Crack WPA(2) Enterprise - PEAPv0-MSCHAPv2 2018

CA propria o esterna?

- Problema ben descritto sul wiki di eduroam in EAP Server Certificate considerations
- Propria (ADVANCED)
  - Recommended certificate properties (cambiano nel tempo)
    - Versione X.509, FQDN per il CN che corrisponde al SubjectAltName:DNS e che va valorizzato, no wildcard, firma minima: SHA-256, chiave pubblica lunga almeno 2048 Bit - 3072+ Bit raccomandata, Extend: Key Usage TLS Web Server Authentication - CRL url valida - BasicConstraint critical, CA:FALSE, Certificato Domain-Validated (DV) o Organisation-Validated (OV), validità < 825 giorni ...

CA propria o esterna?

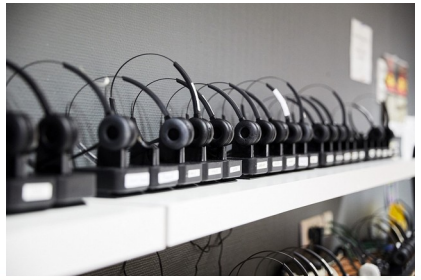
- GÉANT Trusted Certificate Services – CA commerciale
  - Scadenza certificato di circa 1 anno
  - Fissare il CN del server radius nella configurazione di CAT
  - CA e relativa chain cambiano ogni 5 anni (di contratto GÉANT)
    - Pianificare il rollover della chain a seconda del lifetime della CA

CA chain switch-over

- Annuncio nuovo vincitore gara GÉANT
- Annuncio nuova CA chain
  - Aggiungere subito la chain in CAT
    - Cambiare l’outer identity se si usa un identificativo di versione per tenere traccia delle installazioni
- Annuncio end of certificate signing della vecchia CA
  - Rinnovare il certificato dei radius server con la vecchia CA il giorno prima

CA chain switch-over

- Prima della scadenza del certificato firmato dalla vecchia CA
  - avvisare l’helpdesk che i dispositivi potrebbero non collegarsi più e della necessità di scaricare e installare un nuovo profilo
- Alla scadenza del certificato firmato dalla vecchia CA
  - Sostituire CA chain e certificato sul radius server off-peak
  - Prepararsi alle chiamate di helpdesk



Licenza

Daniele Albrizio
albrizio@units.it

WORKSHOP GARR 2021

NET MAKERS