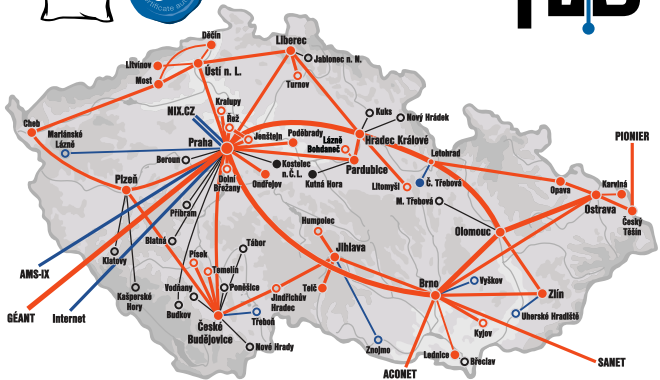
eduroam tajemství zbavený

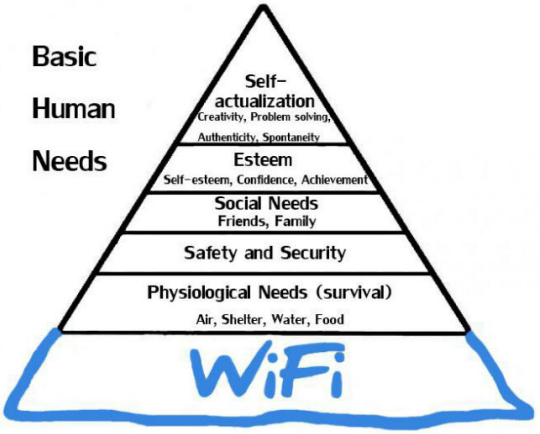
Ondřej Caletka

9. října 2016

O sdružení CESNET



Internet jako lidská potřeba



(Skoro) všichni chceme Wi-Fi

- rychlé a spolehlivé
- zdarma
- bez složité konfigurace
- bezpečné
- i v době LTE (specifický trh)
- zvláště pak v železobetonových katedrálách

Druhy Wi-Fi sítí

- nešifrovaná síť, přímý přístup
  - snadno provozovatelné
  - snadno použitelné
  - velmi nebezpečné pro uživatele i provozovatele
- nešifrovaná síť, captive portál
  - snadno provozovatelné
  - obtížně použitelné
  - velmi nebezpečné pro uživatele
- síť zabezpečená sdíleným WPA heslem
  - snadno provozovatelné i použitelné
  - velmi bezpečné pro uživatele
- síť zabezpečená pomocí 802.1X
  - obtížně provozovatelné i použitelné
  - velmi bezpečné

Když zaklepe policie…

- anonymní Wi-Fi sítě fungují dobře, než jsou zneužity k páchání kyberkriminality
- provozovatelé mají (alespoň někde) odpovědnost za chování uživatelů ve své síti
- přinejmenším to je nepříjemnost
- provozování anonymní sítě jako alibi pro svou vlastní nelegální činnost nefunguje

Captive portály

- klient se připojí k nešifrované síti
- jeho komunikace je blokována a HTTP provoz unášen (!) směrem k autentizačnímu portálu
- po ověření jména a hesla je komunikace pro danou MAC adresu povolena

Broken by design

- míchání autentizovaných a neautentizovaných uživatelů v jedné síti
- nekompatibilita s HTTPS (a IPv6, DNSSEC, atd.)
- nepříjemný uživatelský zážitek


13:04
internet hotspot
192.168.192.1/login?dst=http%3A%2F%2Fwww.mydealz.de%2F
Witamy w Hot Spot PR
Aby korzystać z internetu wpisz:
Login: Przewozy
Hasło: Regionalne
login
Przewozy
password
OK
Przewozy Regionalne


ŽELEZNIČNÁ SPOLOČNOSŤ SLOVENSKO
Username
guest
Password
Login
Copyright © 2015 DrayTek Corp. All Rights Reserved.

2

Zapamatované nešifrované sítě

- většina zařízení si připojení k nešifrované síti pamatuje
- následně se snaží aktivně objevovat takovou síť
- útočník triviálně zachytí výzvy a vytvoří požadovanou síť na míru
- dostupná řešení – např. Wi-Fi Pineapple

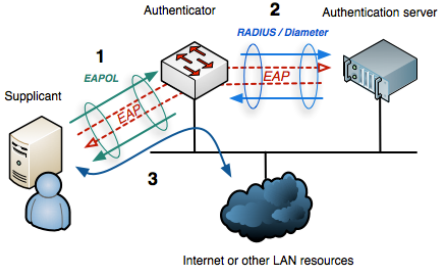
Nikdy nenechávejte nešifrované sítě v seznamu oblíbených!

Projekt eduroam

- vznikl v roce 2002 v Nizozemsku, do ČR dorazil v roce 2004
- problém pro akademiky, migrující mezi univerzitami
  - bylo třeba nahlásit MAC adresy
  - případně si zapůjčit správnou síťovou kartu
- myšlenka kooperace mezi akademickými provozovateli (bezdrátových) sítí
  - reciproční princip – kdo chce účet, musí poskytovat službu
- původně podpora 802.1x, VPN i captive portálů
  - od 1. 10. 2007 zákaz captive portálů
  - použití VPN nikdy pořádně nefungovalo
- řeší autentizaci, ne konektivitu (tu dodává hostitel)

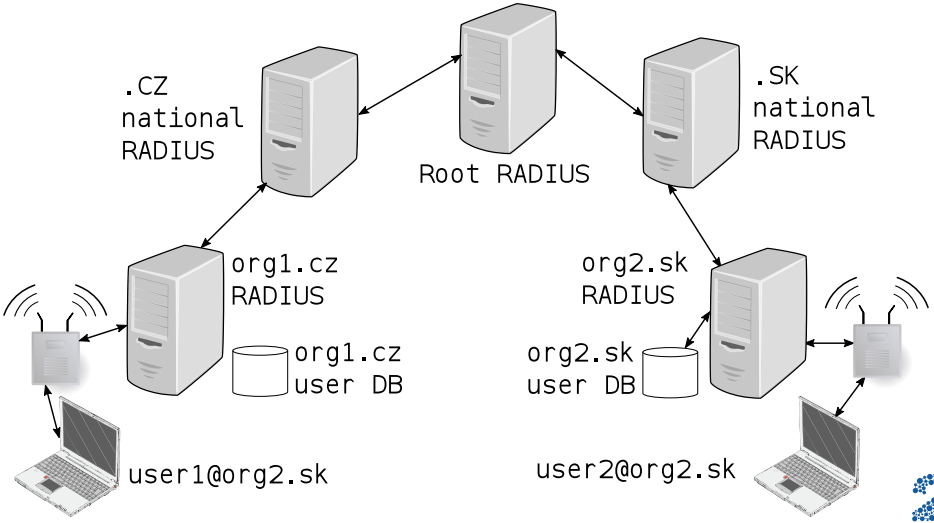
Autentizace podle 802.1x

- klient se fyzicky připojí k síti, veškerý provoz je blokován
- autentikátor vyzve klienta protokolem EAP-over-LAN
- zprávy EAPOL jsou *autentikátorem* (typicky switch nebo AP) předávány autentizačnímu serveru
- *supplicant* uvnitř klienta komunikuje s autentizačním serverem
- při pozitivní odpovědi je klient vpuštěn do sítě



Arran Cudbard-Bell, Wikimedia, FDL

Federace eduroam



Federace eduroam

- lokální uživatelé jsou odbaveni lokálně
- ostatní jsou směrováni pomocí realmu v uživatelském jménu
- EAP sezení je vždy navázáno od supplicanta k autentizačnímu serveru domovské organizace (IdP)
- pro uživatele není žádný rozdíl mezi domovskou a cizí organizací
- používané autentizační metody:

  EAP-TTLS/EAP-PEAP
  - vnější TLS tunel s autentizací serverového certifikátu
  - vnitřní EAP ověření klienta (EAP-MSCHAPv2, EAP-PAP)

  EAP-TLS
  - vzájemná autentizace certifikáty

Vnější a vnitřní identita

vnější (anonymní) identita

- putuje v otevřené podobě
- slouží pro směrování k IdP v rámci federace
- identita uživatele může být anonymizovaná (např. `anonymous@example.org`)

vnitřní identita

- putuje uvnitř TLS tunelu k IdP
- slouží k autentizaci
- vidí ji jen IdP

Propojení RADIUS serverů

- RADIUS protokol používá UDP, šifruje pouze heslo sdíleným tajemstvím
- pro vyšší ochranu transportován v IPSec
  - obtížná konfigurace
  - nekompatibilní s překlady adres
  - nutnost udržovat tunel naživu
- přechod na protokol RadSec
  - RADIUS protokol tunelovaný v TLS/TCP
  - vzájemná autentizace TLS certifikáty
  - snadná konfigurace

Dynamické objevování RadSec

- hierarchický systém doménových jmen funguje dobře jen s ccTLD
- připojení organizací s realmem `.eu` nebo `.edu` obtížně škálovatelné
- použití NAPTR a SRV záznamů v DNS pro objevení RADIUS serveru pro daný realm (obdoba ENUM pro SIP)
- ověření příslušnosti k eduroamu TLS certifikátem vydaným konkrétní autoritou
- povinné pro gTLD realmy, volitelné pro ccTLD
- zkrácení autentizační cesty, ideálně na SP – IdP bez prostředníků
- idea Let's RadSec – automatizovaně vydávat certifikáty s ověřením prostřednictvím existující hierarchie

eduroam v praxi

Problémy SP

Dohledání majitele dané adresy

- 802.1x řeší jen přístup k síti – zná pouze MAC adresu
- jen některá L2 zařízení registrují klientské IP(v4/v6) adresy v účtovacích datech
- je-li použit NAT, je třeba uchovávat informace o překladech

Zablokování konkrétního uživatele

- je k dispozici pouze MAC adresa (tu může měnit) a vnější identita (ta může být společná pro všechny uživatele dané organizace)
- spolehlivé zablokování vyžaduje manuální komunikaci s IdP
- řešením je nový IdP atribut Chargeable-User-Identity

Problémy IdP

Způsob autentizace, volba EAP protokolu

- nejčastěji heslem a EAP-MSCHAPv2
- samostatné heslo – bude uložené nechráněné v zařízeních
- generovat nebo nechat uživatele zvolit?
- podporovat/tolerovat anonymní vnější identity?

Volba certifikátu pro autentizaci vnějšího TLS tunelu

- zvolenou CA je velmi obtížné změnit
- veřejné CA funguje out-of-the-box, ale nebezpečně
- privátní CA vyžaduje složitější konfiguraci, ale může být bezpečnější

Problémy uživatelů

- jak službu nakonfigurovat aby fungovala
  - a aby byla bezpečná
  - a aby to zvládl i běžný uživatel
- problematické ověřování vnějšího TLS tunelu
  - Windows ve výchozím stavu vyžadují jakýkoli platný veřejný certifikát
  - Apple používá TOFU přístup, vyvolá dialog pro ověření otisku
  - ostatní ve výchozím stavu neověřují nic
- ideální správné nastavení
  - důvěra v privátní CA, která vydává certifikáty pouze pro RADIUS
  - důvěra ve veřejné PKI a **explicitně konfigurované jméno serveru**

Proč je ověřování certifikátu důležité

- kdokoli může nastavit své AP, aby vysílalo ESSID eduroam
  - i když tím riskuje žalobu od GÉANT
- autentizaci nezapojí do eduroamu, ale otočí proti svému serveru
  - klient nepozná, že nemluví s domovskou organizací
  - v případě použití EAP-PAP je heslo okamžitě odcizeno
  - MSCHAPv2 je dávno prolomený, získání hesla je otázkou max. hodin

Obtížné ověření certifikátu

- supplicant nezná správné jméno serveru
- bez připojení nelze kontrolovat revokaci

Ověřování klientským certifikátem

- eliminuje možnost odcizit heslo
- obvykle **velmi** obtížné pro uživatele
- problém s velkými pakety
  - ClientHello s certifikátem je velký
  - některé tunely mohou mít menší MTU a vynucovat fragmentaci
  - některé firewally blokují fragmenty
  - autentizační výzva do domovské organizace nedoputuje
  - v rámci ČR automaticky testováno

eduroam Configuration Assistant Tool

- nástroj pro snadnou a bezpečnou konfiguraci
- vychází z XML profilu, který publikuje IdP
- generuje instalátor pro konkrétní instituci a platformu
  - Windows Vista+
  - OS X / macOS
  - Linux (funguje téměř všude!)
  - Chrome OS
  - Apple iOS 5+
  - Android 4.3+
- jediná možnost, jak v Androidu nastavit kontrolu jména serveru

1996–2016 CESNET

Ruční konfigurace - WPA Supplicant

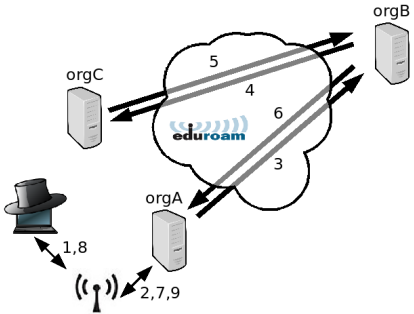
```
network={
        ssid="eduroam"
        key_mgmt=WPA-EAP
        eap=PEAP
        identity="caletka@cesnet.cz"
        password=hash:012c9edfb06b543233745c9aff836490
        ca_cert="/etc/ssl/certs/AddTrust_External_Root.pem"
        altsubject_match="DNS:rad1.ces.net;DNS:rad2.ces.net"
}
```

Získání hashe hesla – ochrana před letmým pohledem

```
$ python -c 'import getpass,hashlib; print(hashlib.new("md4",
> getpass.getpass().encode("utf-16le")).hexdigest())'
Password: CorrectHorseBatteryStaple
012c9edfb06b543233745c9aff836490
```

Včelka Mája

- chybná konfigurace RADIUS serveru při neshodě realmu vnitřní identity předává autentizační zprávy dál
- uživatel z orgC navštíví orgA s použitím anonymní identity orgB
- orgA se mylně domnívá, že uživatel přichází z orgB
- orgC se mylně domnívá, že uživatel roamuje v orgB



Problematická signalizace

- vyhodnocování živosti realmů
  - server konkrétního realmu přestane odpovídat
  - klient přeposílá dotaz přes nadřazený server
  - nadřazený server nemá jak odpovědět
  - klient vyhodnotí nadřazený server jako nefunkční
  - přestanou fungovat i jiné realmy
- špatné chování supplicanta
  - nezobrazují uživateli důvod odmítnutí žádosti
  - timeout odpovědi vyhodnotí jako špatné heslo
- neexistuje žádný způsob komunikace IdP/SP s uživatelem

Expirované účty

- při opuštění univerzity uživatelé zapomínají odkonfigurovat uložené účty
- vybíjí si baterii, kdykoli jsou v dosahu eduroamu
- pro autentizační servery žádný praktický problem
- situace se zhoršila se zálohou Wi-Fi sítí do cloudu

Kolize Wi-Fi sítí

- typický problém v kampusech
  - jedna budova, 3 různé eduroamy
  - každý poskytuje nezávislou IP konektivitu
  - některá zařízení se trvale drží nesprávné sítě
- nemožnost vynutit použití konkrétní sítě/technologie
  - essid typu `eduroam-5Ghz`, `eduroam-cesnet` rozbíjí roaming
  - řešením může být HotSpot 2.0

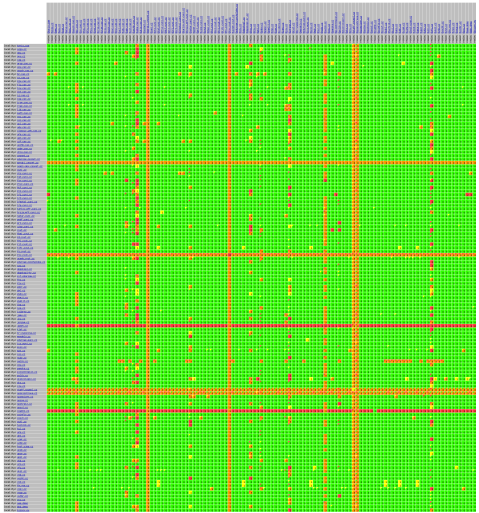
Hot Spot 2.0 / Passpoint / 802.11u

- rozšíření metadat Wi-Fi AP
- možnost komunikace s uživatelem před autentizací
- možnost identifikovat asociaci nezávisle na essid

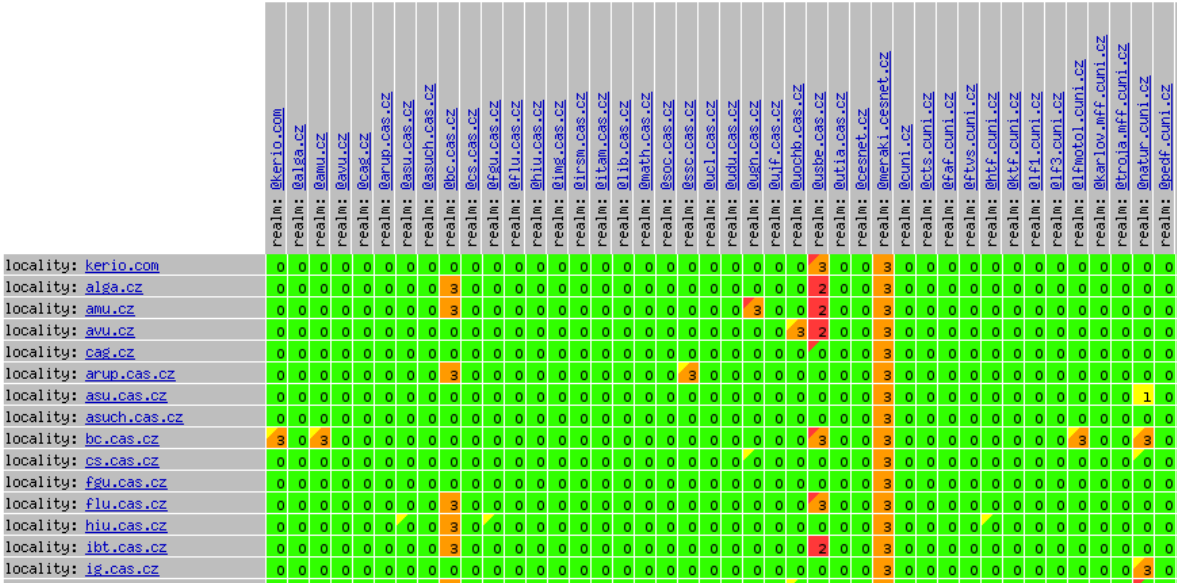
Příliš paranoidní SP

- organizace poskytující eduroam může připojovat uživatele dynamicky do různých sítí
- místní uživatelé mohou být připojování libovolně
- hosté by měli být připojování do sítě s přístupem alespoň k:
  - HTTP/S, FTP
  - SSH
  - OpenVPN/IPSec/PPTP
  - IPv6 in IPv4
  - SMTP/S, POP3/S, IMAP/S
- testovací účty by neměly mít přístup nikam

Matice dostupnosti



https://ermon.cesnet.cz/matrix/index.html


realm: @kerio.com
realm: @alga.cz
realm: @amu.cz
realm: @avu.cz
realm: @cag.cz
realm: @arup.cas.cz
realm: @asu.cas.cz
realm: @asuch.cas.cz
realm: @bc.cas.cz
realm: @cs.cas.cz
realm: @fgu.cas.cz
realm: @flu.cas.cz
realm: @hiu.cas.cz
realm: @ibt.cas.cz
realm: @ics.cas.cz
realm: @ifcm.cas.cz
realm: @ifa.cas.cz
realm: @lib.cas.cz
realm: @math.cas.cz
realm: @soc.cas.cz
realm: @ssc.cas.cz
realm: @ucl.cas.cz
realm: @udu.cas.cz
realm: @ufchtm.cas.cz
realm: @uif.cas.cz
realm: @uochb.cas.cz
realm: @usbe.cas.cz
realm: @utia.cas.cz
realm: @cesnet.cz
realm: @meraki.cesnet.cz
realm: @cuni.cz
realm: @cts.cuni.cz
realm: @faf.cuni.cz
realm: @ftvs.cuni.cz
realm: @htf.cuni.cz
realm: @ktf.cuni.cz
realm: @lfi.cuni.cz
realm: @lf3.cuni.cz
realm: @lfmotol.cuni.cz
realm: @karlov.mff.cuni.cz
realm: @troja.mff.cuni.cz
realm: @natur.cuni.cz
realm: @pedf.cuni.cz
locality: kerio.com
locality: alga.cz
locality: amu.cz
locality: avu.cz
locality: cag.cz
locality: arup.cas.cz
locality: asu.cas.cz
locality: asuch.cas.cz
locality: bc.cas.cz
locality: cs.cas.cz
locality: fgu.cas.cz
locality: flu.cas.cz
locality: hiu.cas.cz
locality: ibt.cas.cz
locality: ig.cas.cz

Projekt eduroom

- kompletní řešení pro nasazení eduroam SP v malých organizacích a na cestách
- postavené na komoditním hardwaru a OpenWRT
- automatický provisioning certifikátu i nastavení z projektu BeeSIP
- připojení k federaci pomocí RadSecproxy
- netflow sonda pro zaznamenávání překladů adres
- addrwatch pro zjišťování adres účastníků
- podpora IPv4 i IPv6 (podle hostitelské sítě)
- dálková správa a logování pomocí OpenVPN
- možnost LTE uplinku

Shrnutí

- captive portály jsou zlo
- 802.1x má slabá místa, ale poskytuje vysoký komfort
- nikdy **nenechávejte nešifrované sítě** v seznamu oblíbených
- vždy konfigurujte svůj eduroam účet bezpečně
  - volte silné heslo
  - ověřujte identitu svého IdP
- přednostně používejte nástroj `https://cat.eduroam.org`
  - není-li vaše instituce v nabídce, požádejte správce svého IdP
- námět na start-up
  - rozšířit koncept eduroam mimo akademickou obec
  - konkurovat řešením postaveným na captive portálech
  - využívat národní e-identity

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz