Eduroam: Secure WiFi roaming for education and research

Simeon Miteff
smiteff@csir.co.za

Context

- Meraka and SANReN
- Our impact
- Eduroam is a service
- Focus of this talk

WiFi

- Count the RF transceivers in your pocket
- Wifi == IEEE 802.11... specifically.

WiFi security basics

- The radio channel
- Protecting the data
- Network admission

- First attempts:
  - WEP and WPA(1)
- Current standard:
  - WPA2
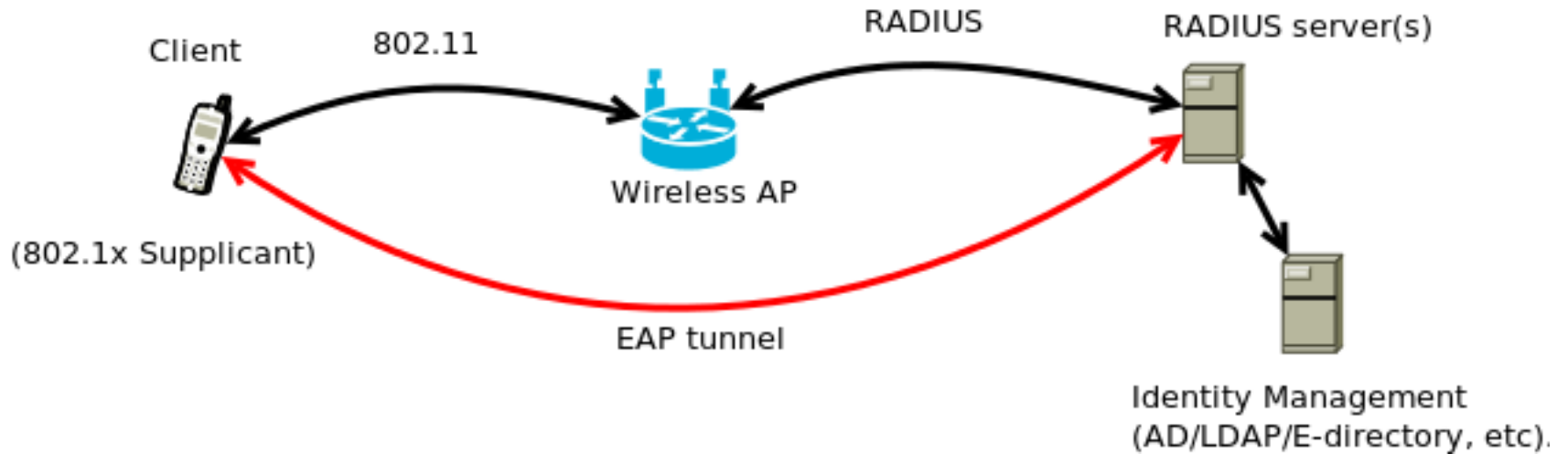
CSIR

our future through science

Authentication and key distribution

- WPA-Personal: common pass phrase
  - known by all users of the network

- WPA-Enterprise: per-user credentials
 - normally user name + password

CSIR
our future through science

WPA2-Enterprise

Client

802.11

(802.1x Supplicant)

Wireless AP

RADIUS

EAP tunnel

RADIUS server(s)

Identity Management
(AD/LDAP/E-directory, etc).

CSIR

our future through science

Mission accomplished!

- Secure WiFi for home users is simple
- Secure WiFi for enterprises is complex but once set up it works well

- Right?

CSIR

our future through science
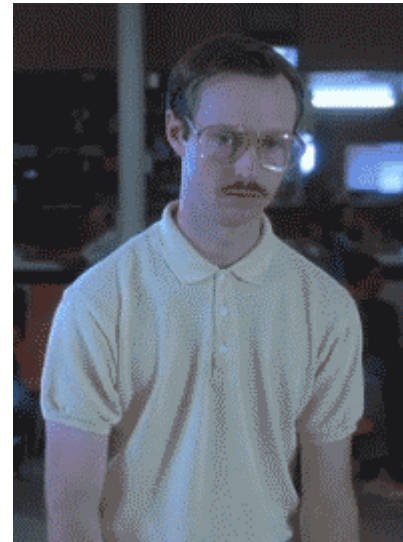
What about guests?

- WPA2-Enterprise for normal users (staff, students, etc.)

- Now we have a (wanted) visitor...

- What are our options?

CSIR

our future through science
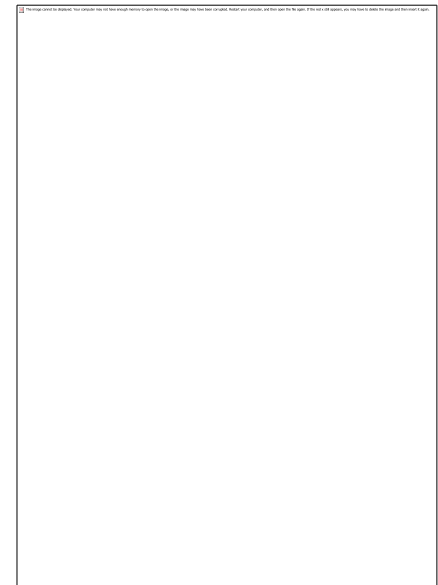
Ye Olde Guest Account

- The need for speed
- Dirty dishes the next morning

- Better idea: virtual access points (SSID) for guests

CSIR

our future through science

Security mechanisms for guest SSID

- No security
- "Hotel WiFi" - captive portal
- WPA2-Personal
- Don't permit guest access

CSIR
our future through science
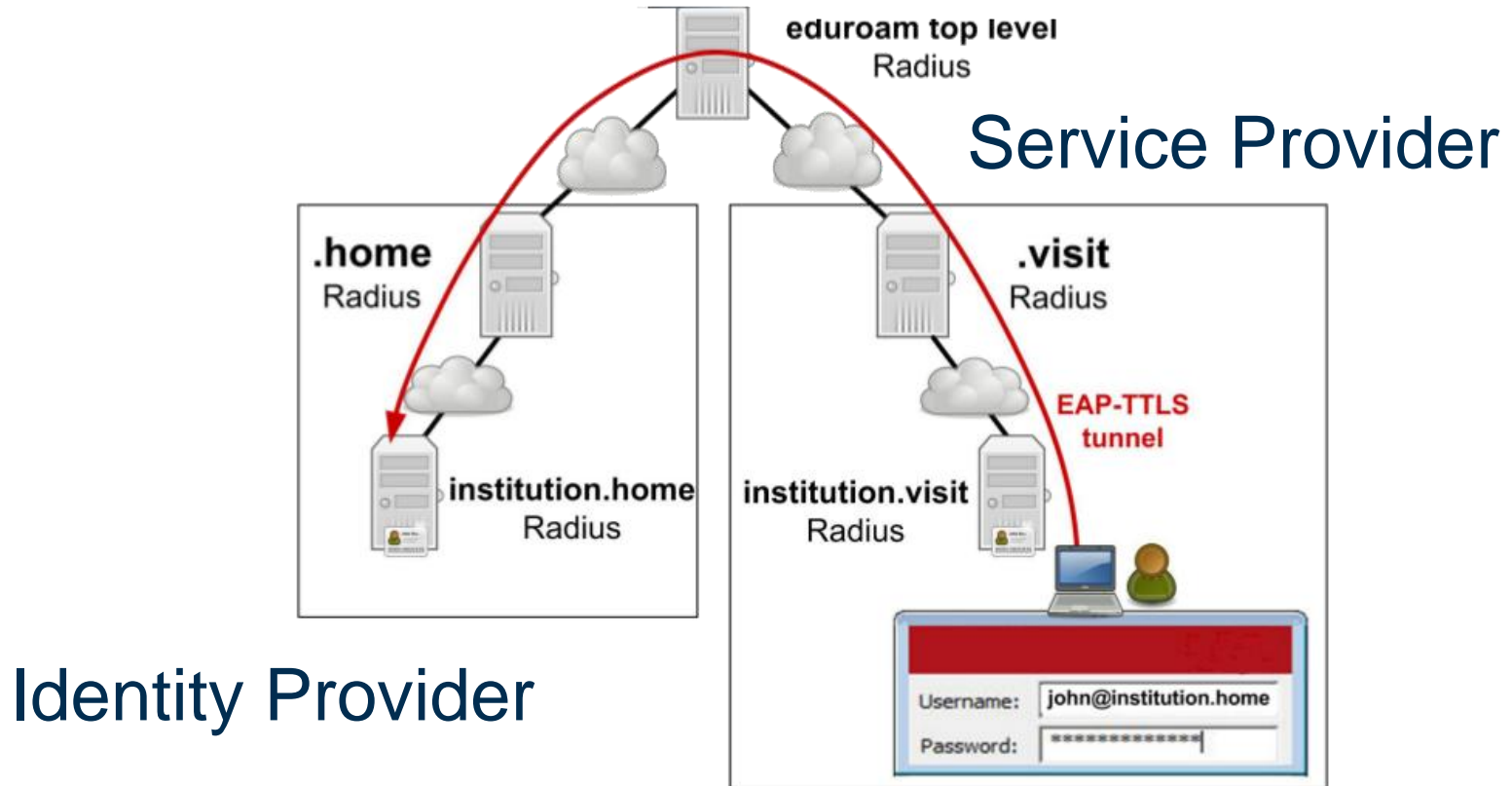
Pillars of information security

- Confidentiality
- Integrity
- Availability
  - Did you just DoS yourself?

- We need a better plan

The better plan: WiFi roaming

- Transparent
- Decent service
- Secured traffic
- People know you at home
- Take the tunnel

- How? WPA2-Enterprise and RADIUS proxies.

CSIR

our future through science

How Eduroam works

Service Provider

Identity Provider

eduroam top level
Radius

.home
Radius

institution.home
Radius

.visit
Radius

institution.visit
Radius

EAP-TTLS tunnel

Username: john@institution.home
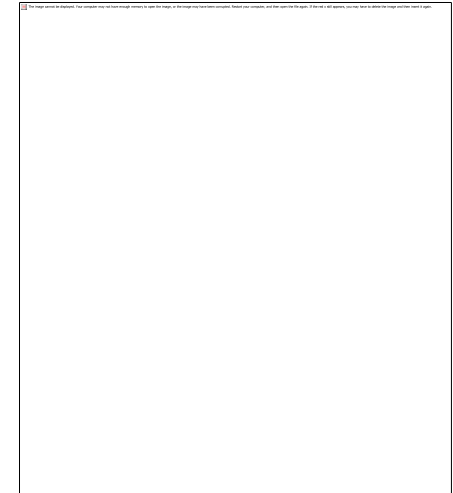Password: ************

CSIR
our future through science

Eduroam ecosystem

- IdP commitment
- At no cost to users
- Reciprocal
- IdP must be an SP
- SP can be a coffee shop
- NRO, RRO, GeGC

CSIR
our future through science

Security incident handling

- Outer identity: anonymous@csir.co.za
- Be a good (law-abiding) guest
- What is logged?
- Who understands it?

Trust in the cloud

- Current method
  - We know those guys
  - RADIUS Secret
- Future decentralization
  - Realm to DNS to IdP RADIUS
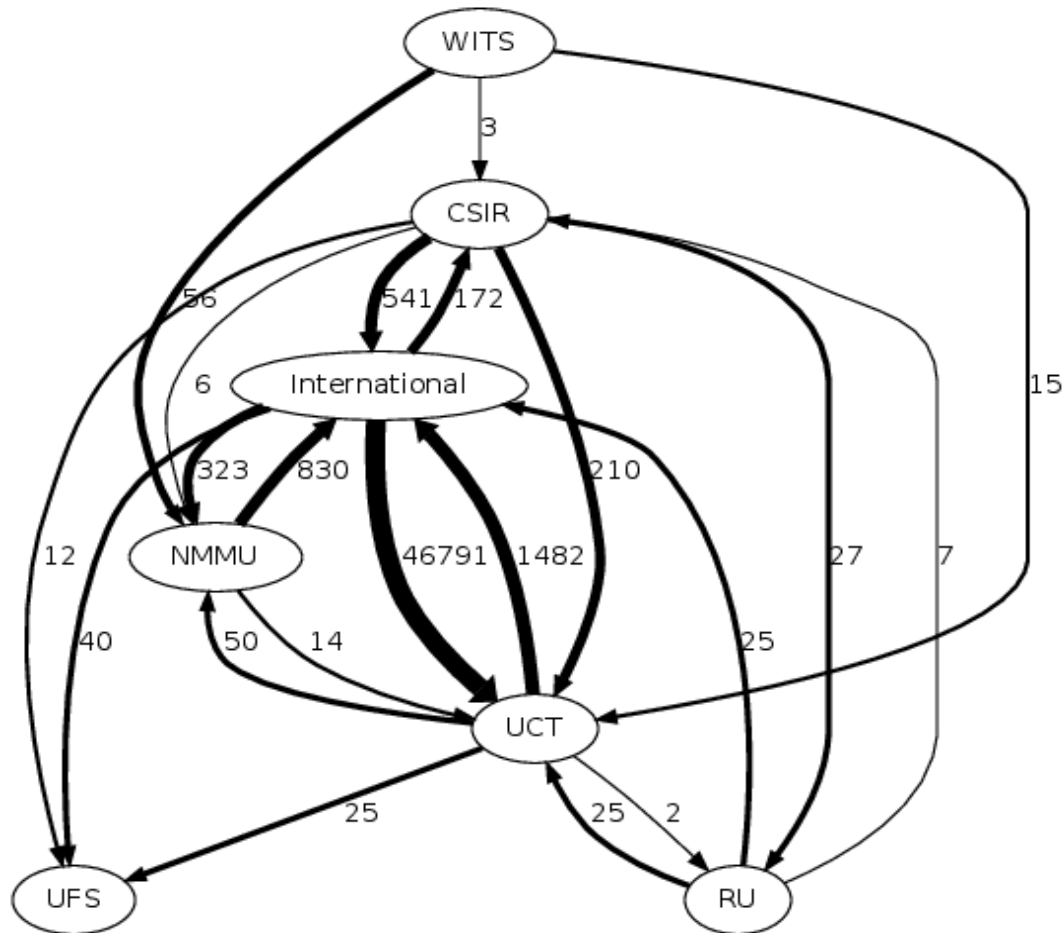 - Radsec (TLS) and x509
  - Club membership policy OID

CSIR
our future through science

Eduroam in South Africa

- Training workshops
- Pilot project success
  - Useful to our customers
  - http://eduroam.ac.za
- National Roaming Operator: Meraka
- Signatory: TENET
- National policy agreement: WIP

CSIR
our future through science

Service uptake
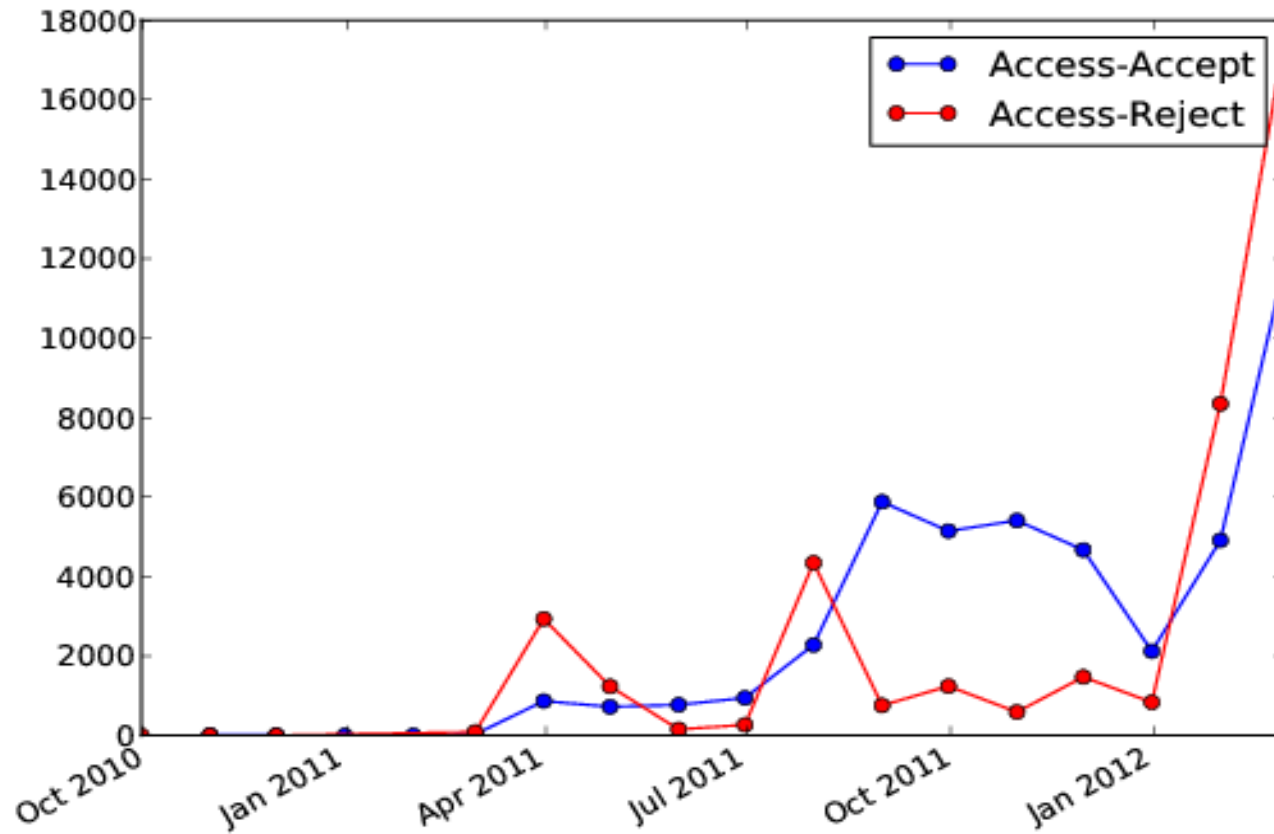
Graph of authentications

Thank you

- TERENA and Klaas Wierenga (for Eduroam)
- SURFNet (assistance and training)
- Department of Science and Technology
- Meraka/Trusted Network Infrastructures & Services: Johann Hugo, Karel Matthee, John Hay
- Meraka/SANReN: Roderick Mooi, Ntuthuko Sambo, Christiaan Kuun
- TENET: Duncan Greaves
- Guy Halse (Rhodes), Erisan Nyamutenha (UCT)
- You!

CSIR
our future through science

Attribution

- Cloud designed by Thomas Hirter from The Noun Project
- Plant designed by Rick Diaz-Granados from The Noun Project
- Brick Wall designed by Nicolas Hue from The Noun Project
- Plates designed by Joanna Smolonska from The Noun Project
- Kip clip from *Napoleon Dynamite* – Copyright 2004 Fox Searchlight Pictures

CSIR
our future through science