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
• 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
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
WPA2-Enterprise

Client \rightarrow 802.11 \rightarrow Wireless AP \rightarrow RADIUS \rightarrow RADIUS server(s)

(802.1x Supplicant) \rightarrow EAP tunnel \rightarrow Identity Management (AD/LDAP/E-directory, etc.)
Mission accomplished!

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

- Right?
What about guests?

- WPA2-Enterprise for normal users (staff, students, etc.)
- Now we have a (wanted) visitor...
- What are our options?
Ye Olde Guest Account

- The need for speed
- Dirty dishes the next morning

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

- No security
- “Hotel WiFi” - captive portal
- WPA2-Personal
- Don't permit guest access
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.
How Eduroam works

Identity Provider

Service Provider
Eduroam ecosystem

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