EDUROAM: Usuarios propios y extraños

Universidad Carlos III de Madrid
www.uc3m.es

It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.

Arthur Conan Doyle (1891) *A Scandal in Bohemia*

Rafael Calzada Pradas/Nuria Prieto Pinedo
CERT de Universidad Carlos III de Madrid

@CertUC3M

Riesgos/Retos

- Eduroam permite que los usuarios se muevan entre instituciones, pero presenta algunas tentaciones y riesgos:
  - Cesión de contraseñas
  - Ataques de fuerza bruta para *adivinar* contraseñas
- Retos:
  - Los usuarios pueden tener varios dispositivos
    - ¿Cuantos puede ser el límite?
  - Los usuarios pueden contectar a través de varias instituciones en el mismo día
    - Proximidad geográfica.

Algunos datos de 7/05/2018

Dispositivos anónimos no UC3M

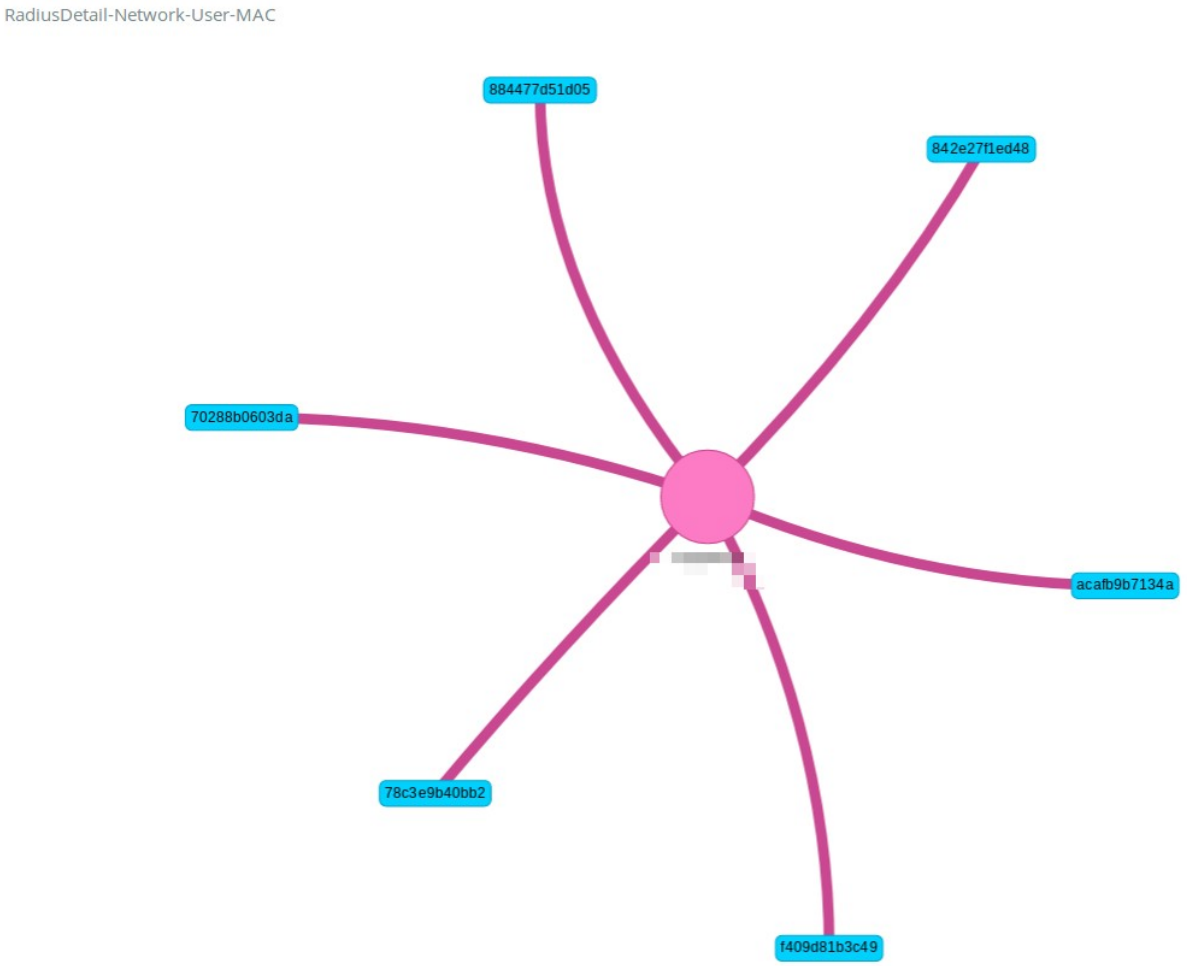
Radius-MAC-BigNumbers

Table

filters	Direcciones Ethernet
MACs Anónimos	399
MACs identificados	16,315

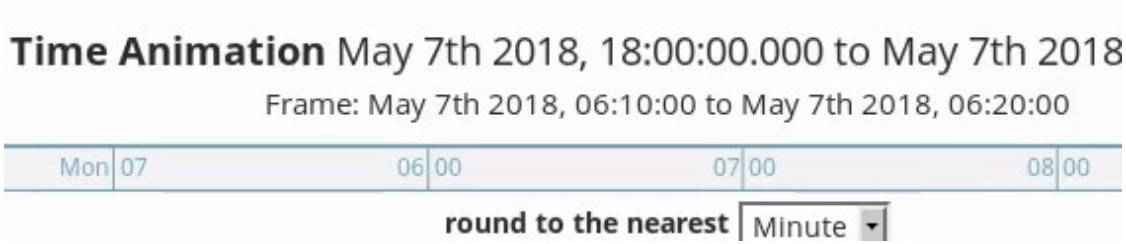
UAM: 131
UCM: 91
UPM: 24
URJC: 17
UPF: 14
UGR: 7

Usuarios identificados con hasta 6 dispositivos



Ubicación de los APs que dan servicio a un usuario

- Hay usuarios con don de ubicuidad
  - Muchos dispositivos, en diferentes ubicaciones
  - Y se mueven simultáneamente…



Acciones posibles

- Prevención:
  - Política de renovación de contraseñas
    - ¿Hasta que punto es efectiva?
    - No evita las cesiones *voluntarias*
- Detección:
  - ¿Alguien se anima a enviar sus logs?
    - ELK central
    - Acuerdos de Protección de Datos
  - ¿Y a geolocalizar sus APs…?
    - Servidor de Mapas central


grazie
dakujem
gràcies
merci
thanks
gracias
ありがとう
спасибо
hvala
obrigado
spas
díky
mochchakkeram
bedankt
danke
bakka bèr
شكراً
thank you
gracias
ačiū
ευχαριστώ
감사합니다
Tak
grazas
Arigatō
grazie
köszönöm
dzięki
gràcies
eskerrik asko
merci
aitäh
asante
obrigado
dankon
dank
kiitos
ngiyabonga
terima kasih
tack
Salamat
dankie
Շնորհակալություն

Universidad
Carlos III de Madrid
www.uc3m.es

web: sdic.uc3m.es
twitter: @CertUC3M
Mail: rafael.calzada@uc3m.es/cert@uc3m.es