Architectures à base d'EAP

Gabriel Campana

France Télécom R&D

5 juin 2008

Définition d'EAP

- Extensible Authentication Protocol : protocole de transport d'authentification (RFC 3748)
- sert de support à des méthodes d'authentification (EAP-TLS, PEAP, EAP-MD5, EAP-SIM, ...)
- avantages : extensible et flexible
- très hype :
  - originellement conçu pour être transporté par PPP
  - mais actuellement surtout utilisé dans le monde du sans-fil

Architectures basées sur EAP

IEEE 802.11i (WPA2)

IKEv2 : UMA/I-WLAN

IEEE 802.16e : WiMAX "Mobile"

Risques engendrés par EAP

- implémentations dans le serveur AAA et le client :
  - du protocole EAP
  - des méthodes d'authentification EAP (EAP-TLS, EAP-MD5, ...)
- failles d'implémentation :
  - déni de service
  - exécution de code arbitraire

Comment trouver ces failles d'implémentation ?

- le fuzzing est une méthode efficace
- Sulley : framework de fuzzing
- développement de scripts Sulley
  - description du protocole à partir des RFC et de captures réseaux
  - encapsulation d'EAP dans RADIUS
  - transmission des données
  - surveillance de la cible par un débuggueur

Démonstration

- serveur FreeRadius volontairement vulnérable

Conclusion

- architectures EAP sensibles, car accessibles par des utilisateurs non authentifiés
- bugs trouvés dans 3 des 6 produits testés
- le fuzzing est une méthode efficace pour trouver des failles d'implémentation dans des environnements fermés

Merci de votre attention !