EAP-PPT

Privacy Preserving Network Access

Paresh Sawant, Bart Brinckman

EMU, IETF 120 Vancouver, July 2024
Industry has embraced network privacy as an important fundamental right.

- **Device Identity:** MAC randomization - MADINAS - https://datatracker.ietf.org/wg/madinas/about/
- **Application Identity:** Application proxy - MASQUE - https://datatracker.ietf.org/wg/masque/about/
- **User Identity:** Extensible Authentication protocol (EAP)
  - Identity can be used by networks or AAA (identity providers) to track location and monitor activities
    - Sharing personal information for marketing and monetization
    - Surveillance employees, students and visitors
  - Intentional and unintentional privacy compromise in RADIUS and Diameter
    - Chargeable-User-Identity
    - Location Information specific attributes
    - User-Name in Access-Accept
    - NAS-IP-Address, NAS-Identifier, Operator-ID in Access-Request (Proxy to Physical Location)
  - Effectiveness limitations of existing identity protections
    - Applicable to passive and active attacks
    - Limit protection against service providers and identity providers

**Example: OpenRoaming**

- Includes a privacy framework
- Leverages EAP methods such as EAP-AKA, EAP-TLS, EAP-TTLS
- IETF 118 hackathon exposed (unintentional) privacy leakage (https://datatracker.ietf.org/meeting/118/materials/slides-118-madinas-hackathon-openroaming-update-00)
  - Chargeable-User-ID in some cases allows for correlation between sessions
  - Identity leakage in class attributes with an IDP
  - Identity providers may be able to infer user location

**Conclusion:** Even with a privacy framework, implementers may unintentionally leak personal data.
Objectives

• Anonymous access to public and private networks

• Privacy protection against
  - Active and passive attackers
  - Network service providers
  - Venue owners, enterprises, educational institutions
  - Identity providers

Core Principles

• Carry attestation vs identity in EAP
  - Public: Identity: bob@icloud.com vs Attestation: This is an iCloud user logged into the Apple device that is authenticating to this network
  - Private: Identity: alice@cisco.com vs Attestation: This is a cisco employee, who’s devices meets the corporate security policy

• Unlinkable authenticator
  - Unlinkable to user
  - No collusion possible between actors
What we need?

• An identity free credential
• Unlinkability between credential issuance and verification
Solution - Privacy Pass Token

• Cryptographically generated unforgeable and unlinkable proof of attestation
  - Oblivious Pseudorandom Functions Using Prime-Order Groups
  - RSA Blind Signatures

• Server-Client, Issuer-Client, Attester-Server unlinkability guarantee
EAP-PPT

server

EAP-Request/Identity
EAP-Response/Identity ("@example.com")
EAP-Request/PPT-Challenge (TokenChallenge)
EAP-Response/PPT-Challenge (unblinded signature)
EAP Success

peer

attester (Identity Provider)

issuer

attestation
TokenRequest (blinded message)
TokenResponse (blinded signature)
TokenRequest (blinded message)
TokenResponse (blinded signature)
EAP Success
Q&A