Asserting Wireless Network Connections Using DNS Resolvers' Identities

draft-wing-opsawg-authenticating-network-01

IETF115, Nov 2022

D. Wing (Citrix)

T. Reddy (Nokia)

Problem Statement

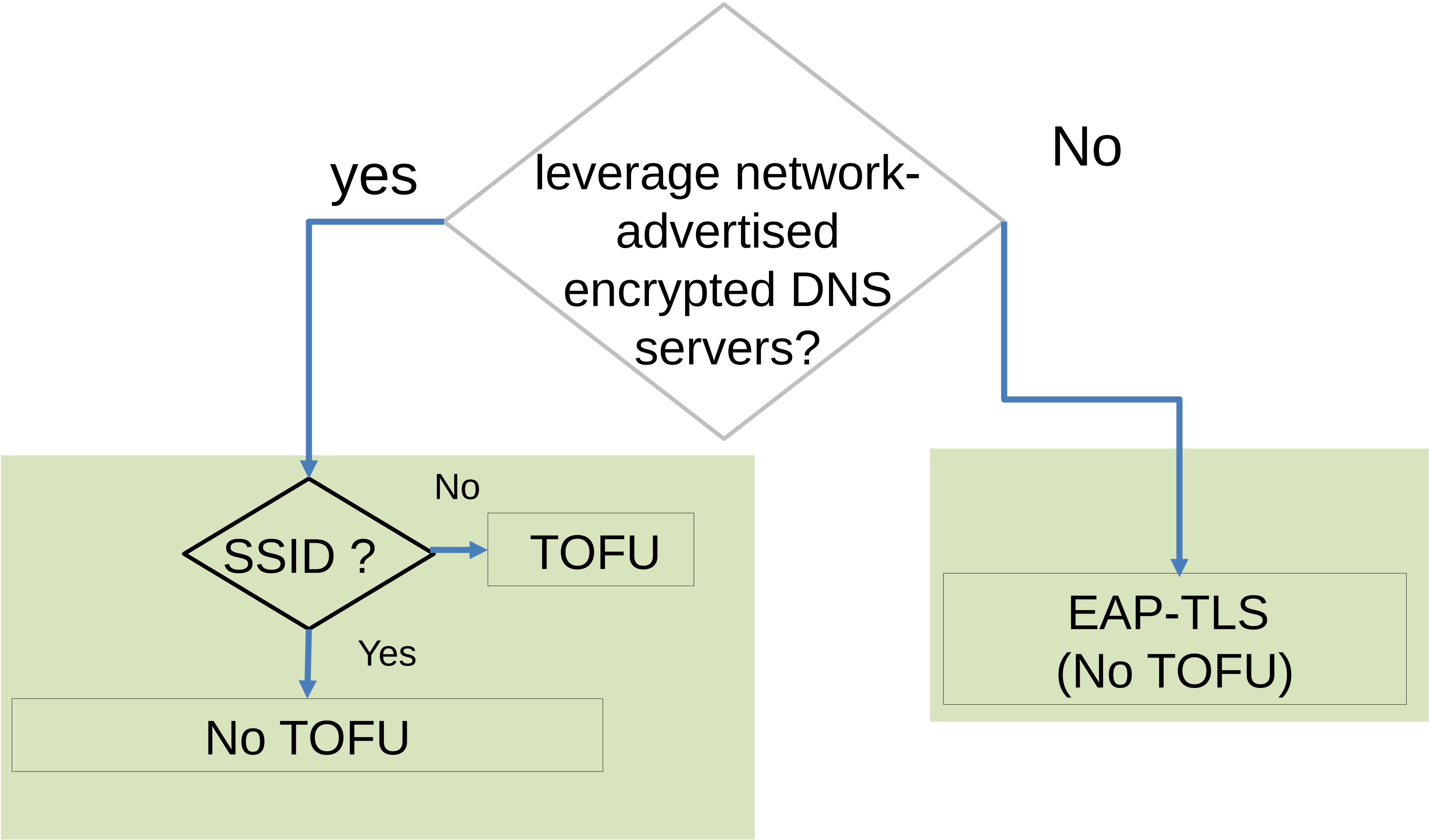
- 802.1X is not widely deployed
- Evil-Twin Attack: WLAN with the same SSID and WPA-PSK as the victim's network
  - Home Networks, Coffee shops
  - Small office/Home office networks

Active Attack: PSK is shared with all the devices including attackers

Problem Statement

- Networks using opportunistic Wireless Encryption [RFC8110]
- LTE/5G mobile networks where the long-term key in the SIM card on the UE can be compromised (FS for EAP-AKA’)

Proposed Solutions



TOFU: DNR/DDR

- On first use, uniquely identify the network:

```
{
  "networks": [
    {
      "SSID": "Example WiFi 1",
      "PSK-ID": 12,
      "Discovery": "DNR",
      "Encrypted DNS": "resolver1.example.com"
    },
    {
      "SSID": "Example WiFi 2",
      "PSK-ID": 42,
      "Discovery": "DDR",
      "Encrypted DNS": [
           "8.8.8.8",
           "1.1.1.1"
      ]
    }
  ]
}
```

TOFU: DNR/DDR

- On subsequent connection to the network:
  - Encrypted DNS server's identity must match

Evil-Twin: Encrypted DNS server's identity differs

No TOFU: DNR/DDR

- SSID name and DNS server's SAN match
  - ❑ Public WiFi hotspots: coffee-bar.example.com
  - ❑ May not be a viable option for home networks (John-Jones.example.net)

No TOFU and no dependency on network-advertised encrypted DNS servers

- SSID name matches SAN in EAP-TLS server certificate.
  - Endpoints not managed by MDM
  - Networks where client authentication is not required (e.g., Emergency services)
  - During the device registration process

Security Considerations

- Attacker network conveys the same encrypted revolver as the legitimate network
  - ➢Reduced visibility to traffic (with TLS 1.3 and ECH).
    - ➢ Larger anonymity set of backend servers offers better hiding.
  - ➢Attacker will have to rely on traffic metadata

Attacker will not have access to DNS messages, won’t be able to remove DNS records with ECH keys

Discussion: draft-wing-opsawg-authenticating-network-01

- Comments and suggestions are welcome