BRSKI over IEEE 802.11

draft-friel-brski-over-802dot11

O. Friel, E. Lear, M. Pritikin Cisco

M. Richardson Sandelman Software Works

Related Draft

Bootstrapping Key Infrastructure over EAP

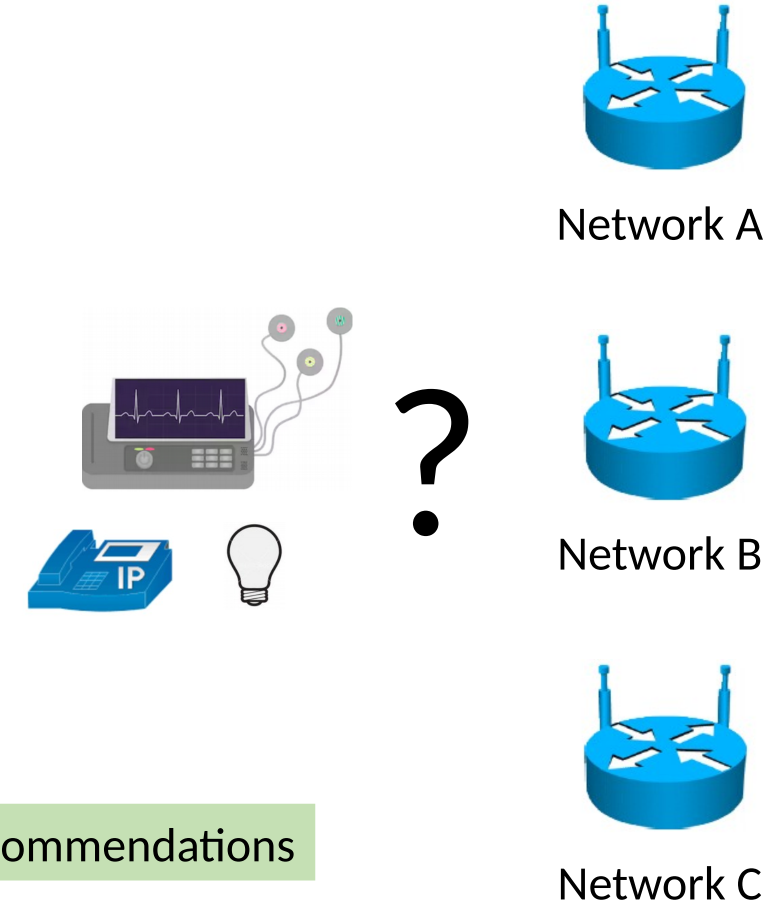
draft-lear-eap-teap-brski

E. Lear, O. Friel, N. Cam-Winget

- Detailed presentation in EMU session on Friday (time permitting)

What problems are we trying to solve?

- What Wi-Fi networks support BRSKI?
- What networks should the device try and connect to?
- How to avoid the device onboarding against the wrong network?
- What credential does the device use to connect to the candidate networks?
- How is network authentication managed pre-BRSKI when the device only has an IDevID vs. post-BRSKI when the device has an LDevID?



This draft outlines some possible solutions but does **not** make any final recommendations

Potential Building Blocks

SSID Discovery:

- IEEE 802.11u (u => external network interworking)
- IEEE 802.11aq (aq => service discovery)
- Wi-Fi Alliance Easy Connect (commonly known as Device Provisioning Protocol or DPP)

Trusted Introduction by manufacturer to deployment:

- 802.1AR for identity
- IEEE 802.11i and IEEE 802.1X for authentication
- ANIMA BRSKI for trust establishment and LDevID enrollment

Proof of Possession:

- WFA Easy Connect / DPP for proof of possession
- ANIMA BRSKI ‘sales channel integration’ for proof of possession

Bootstrap Steps

1. Discover candidate Wi-Fi networks
2. Initial connection to Wi-Fi network prior to completing BRSKI
3. Device completes BRSKI and enrols
4. Connection to Wi-Fi network after completing BRSKI

Proof of ownership can happen in any of these three steps.

SSID Discovery Options

#	Mechanism	Description
1	Well-known BRSKI SSID	• A well-known SSID prefix string for BRSKI networks e.g. “BRSKI” or “Wi-Fi IoT” • Multiple SSIDs could use this name
2	An IEEE 802 Extension	• A new 802.11u extension bit that advertises BRSKI capability • Multiple SSIDs could advertise this capability
3	A Wi-Fi Alliance Extension	• WFA DPP Configurator capability is extended to support 802.1X networks (already provides SSID)
4	802.11u Internet Access	• Wi-Fi networks can already advertise open access to the internet • Device could use this to fallback to vendor default BRSKI registrar

Additional options are outlined in draft-friel-brski-over-802dot11

Authentication Considerations

- Pre-BRSKI
    - A new device only has its IDevID
    - It needs to reach the BRSKI Registrar
    - Possible Wi-Fi authentication mechanisms include
        - Unauthenticated
        - WPA2 (PSK) / WPA3 (SAE)
        - 802.1X EAP TLS based on IDevID
- Post-BRSKI
    - A device has an LDevID
    - Probable Wi-Fi authentication mechanism is 802.1X EAP TLS based on LDevID
- An SSID typically cannot support multiple authentication mechanisms
- Having a device initially connect to one SSID and then reconnect to a different one after BRSKI results in a complicated device (and AAA) state machine
- Devices typically have to reboot and re-IP if they need to access different networks using different credentials

Authentication Options

#	Pre-BRSKI	Post-BRSKI	Comments
1	Unauthenticated	802.1X EAP TLS	• Device may have to reboot, switch SSIDs and re-IP
2	Personal Mode WPA2 or WPA3	802.1X EAP TLS	• Need to define an OOB mechanism to provision the WPA password • Device may have to reboot, switch SSIDs and re-IP
3	802.1X EAP TLS w/ IDevID	802.1X EAP TLS	• CoA could potentially be used by AAA to dynamically change access • Potentially avoids need to reboot, switch SSIDs or re-IP
4	New 802.11 BRSKI Authentication Algorithm	802.1X EAP TLS	• Define new native 802.11 Authentication Algorithm to complete BRSKI flow prior to 802.11 Association
5	802.1X EAP TEAP w/ IDevID	802.1X EAP TEAP	• Device does BRSKI inside TEAP TLS tunnel using new TEAP BRSKI TLVs* • LDevID enrolment happens at L2 prior to IP assignment • No need to reboot, switch SSIDs or re-IP

*TEAP-BRSKI will be described at EMU session on Friday

Additional options are outlined in draft-friel-brski-over-802dot11

Proof of Ownership Options

a.k.a. Don’t connect to the wrong SSID

#	Mechanism	Description
1	Prevention via MASA ‘sales channel integration’	• The MASA via some to-be-defined ‘sales channel integration’ has an explicit map of what network operator owns what device • The MASA only issues Vouchers to the owning network operator / Registrar
2	Detection via MASA audit logs	• A misbehaving network could accept any device • The owning network operator can query MASA audit logs to determine if Vouchers have been issued for missing devices • Does not prevent a device connecting to the wrong network
3	Rely on network operators to be good citizens	• Rely on the fact that networks will only get Vouchers for devices the actually own • In reality, some well-intentioned operators will have permissive policies and will accept any device connection attempt
4	Network must prove possession of a shared secret or key	• The network must prove to the device that it has knowledge of a shared secret before the device will connect to the network • Proof could happen prior to – or possibly absent – BRSKI (e.g. DPP) • Multiple options for implementing such a proof • Public key used for a handshake similar to DPP • Symmetric key used as an 802.1X EAP TLS 1.3 PSK

Summary

- Multiple options for SSID selection
- Multiple options for authentication
- Multiple options for proof of ownership
- Multiple options spanning multiple standards bodies

Discussion