OAuth 2.0 Device Flow

IETF 101 London, March 2018

William Denniss

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-08

OAuth 2.0 Device Flow – Recap

Authorization flow designed for devices that have an internet connection, but no browser and/or only limited input options.

The user will review the authorization request on a secondary device, like a mobile phone, or laptop.

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-08

OAuth 2.0 Device Flow – Recap

Using the browser on your device, visit:

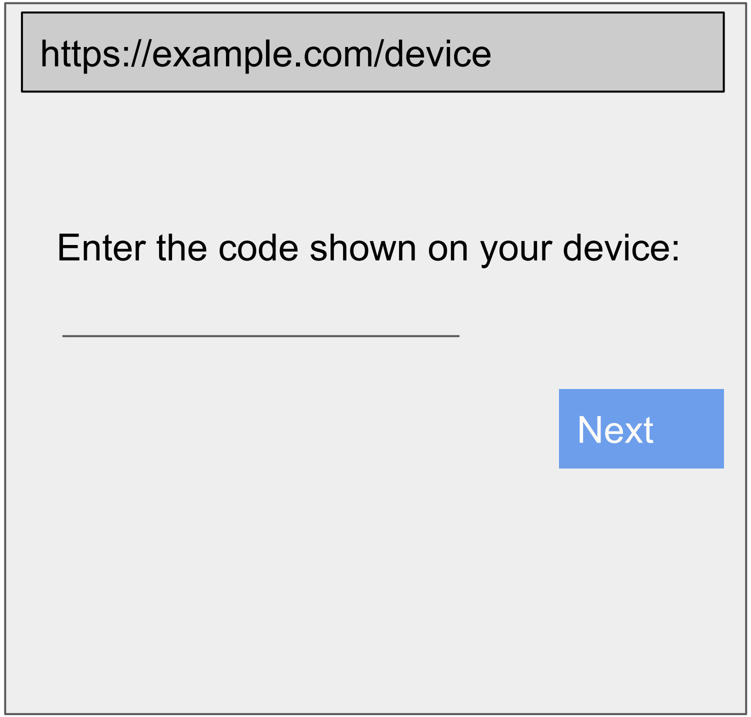
example.com/device

Enter the code:

WDJB–MJHT

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-08

OAuth 2.0 Device Flow – Recap

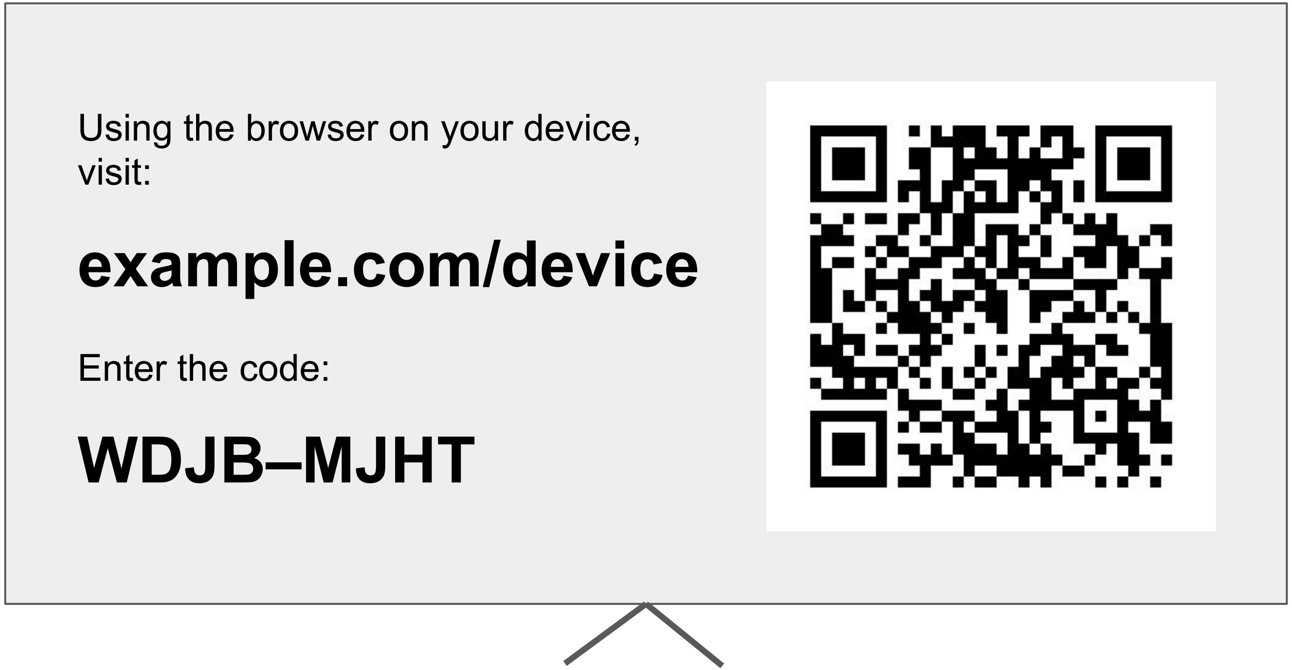


https://example.com/device

Enter the code shown on your device:

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-08

Example with QR Code (using verification_uri_complete)



Using the browser on your device, visit:

example.com/device

Enter the code:

WDJB–MJHT

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-08

Changes in -07

Following IETF 99 consensus, updated the non-textual transmission option to be a separate URI `verification_uri_complete`.

Added security consideration about spying.

Explicitly Required that `device_code` not be shown.

Added text regarding a minimum polling interval.

Changes in -08

Clarified entropy guidance for the user code (it’s still at the authorization server’s discretion, but added some detail).

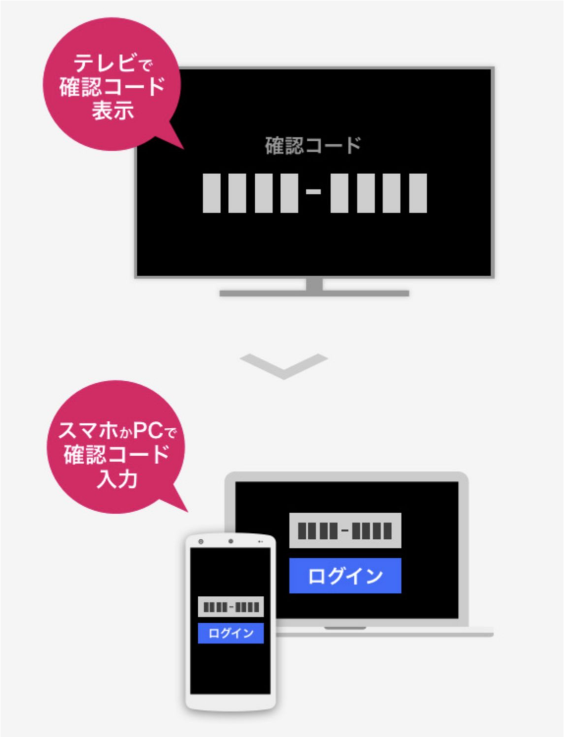
Documented the user-code brute force attack (a “reverse takeover” where the attacker’s credential is given to the victim’s device).

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-08

Running Code

Yahoo Japan implemented it:
https://goo.gl/NczxW8

Used by the Air Stick 4K
https://www.cccair.co.jp/airstick/



https://tools.ietf.org/html/draft-ietf-oauth-device-flow-08

Running Code (Server)

Open source server implementation:

MITREid 1.3

https://github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server

Running Code (Client)

Open source, but Google-specific client example:

https://github.com/google/GTMAppAuth/tree/master/Example-tvOS

Code will be moved to the AppAuth for iOS, macOS (and tvOS!) project once the spec is stable.

Tested on Google and MITREid's server implementations.

OAuth 2.0 Device Flow

Thank You

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-08