Expanding Universal Second Factor (U2F) to Non-Browser Applications

Saurabh Gandhele | smg6512@rit.edu
Prof. Stanislaw P. Radziszowski | spr@cs.rit.edu

PROBLEM STATEMENT

- There is a critical need for improving the authentication standards because of breaches being caused by weak usernames and passwords.
- With more than 60% rise last year in credential thefts occurring across global major corporate organizations, second factor authentication is a must.
- To address these concerning issues, the FIDO alliance launched a new protocol in 2015 called the Universal Second Factor (U2F).

SECOND FACTOR EXPERIENCE (U2F standards)

- Core idea: Standard public key cryptography.
- Privacy: Site Specific Keys, No unique ID per device.
- Security: Not vulnerable to attacks, Set alternative back up authentication if device is lost/stolen/tampered.
- Trust: Verify the company that produce U2F devices.
- Pragmatics: Affordable today to everyday user.
- Speed for user: Fast crypto in device, uses

UNIVERSAL SECOND FACTOR

Authentication

- Registers a U2F device with a user by creating a binding between the service and device.
- Relying party (server) issues a challenge and application_id that are fed into the browser.
- Browser collects info from the challenge, origin, state of SSL to construct client data object.
- User provides his acknowledgement by tapping the device and a new credential is created.
- Device validates correctness of origin is verified by SSL state and the server stores.
- Correctness of origin is verified by SSL state and the server stores

IMPLEMENTATION

- Simulated U2F protocol on an Android application that communicates with the BLE (Bluetooth Low Energy) key.
- U2F key has a full elliptic curve (secp256r1) implementation.
- Kpub & key handle are points generated on the curve in key.
- The BLE key first needs to be paired with the Android device.
- Register button will display the Kpub, key handle & certificate response received from the BLE U2F key.
- Authenticate button will display the user presence, counter increment & signature response received from BLE U2F key.

CONCLUSION & FUTURE WORK

- Other second factor authentications like OTP and Google Authenticator are still vulnerable and inconvenient to use for certain users because of network or device unavailability.
- U2F protocol overcomes these disadvantages by offering devices that provide security at maximum level combined with a simple and easy to operate user experience.
- U2F plans to cross reference all the browsers, operating systems and channels across each other in future for more feasible use and easy access.

References: