Class Notes Monday

September 27th 2021

**RSA UBI Keys:**

A small device that creates a random one-time passcode that is more secure than using biometrics for authentication. This helps against phishing because the UBI Key checks against which website is sending the validation for the code, if it's not the expected website, the attacker can not use the information that was stolen.

**Challenge Response:**

Relying Party(website) -> Challenges the device

Browser -> The middleman in the transaction

Device (UBI Key) -> Responds to the challenge through the browser

**FiDO Universal Two Factor Protocol:**

* Authentication
* Registration (on a given website)

**FiDO Authentication Steps:**

1.) Input username and password

2.) The browser contacts the RP for the challenge

3.) The browser will construct authentication request message then sends to device

4.) Device then constructs an authentication response message to the challenge

5.) Browser forwards response to the relying party

6.) Relying party verifies the response

**Authentication Request Message:**

* Control (1 byte) - Controlled by the browser (Verify if user is physically present)
* Challenge Parameter (32 bytes) - SHA 256 HASH - computed by challenge RP & domain name
* Application Parameter (32 bytes) - SHA 256 HASH to verify the app your communicating with
* Key Handle Length (1 byte)
* Key Handle (variable length) - The device will use different key pairs for each application, so the handle is a way of denoting which app is using it.

**Authentication Response Message:**

* User Presence
* Counter (4 bytes)
* ECDSA Signature – Computed by app parameter, user presence, counter, and challenge param

The relying party will compute and compare the Elliptic Curve Encrypted Signature with the one from the response and if they match, then the user is allowed to finally log in.

During the registration process, the device must go through an attestation which is a 3rd party verifying your Identity on your behalf for the relying party. It’s used to prove that the device is legitimate and not a forgery.