Combining WebAuthn and Payment Handler Gestures

Adrian Hope-Bailie
March 2020
Goals

Increase security

- Use WebAuthn for authentication

Reduce friction for users

- Reduce number of user interactions
user gesture to launch Payment Handler
Current Flow with WebAuthn

1. User clicks/taps “Pay” button
2. Browser invokes Payment Handler (PaymentRequestEvent)
3. Payment Handler invokes WebAuthn API
4. User provides WebAuthn gesture

2 user gestures
Proposed Flow with WebAuthn (at Registration)

```javascript
registration.paymentManager.instruments.set(
    "dc2de27a-ca5e-4fbd-883e-b6ded6c69d4f",
    {
        name: "Visa ending ****4756",
        method: "basic-card",
        credentials: [{
            publicKey: {
                allowCredentials: [ ... ],
                timeout: 60000
            }
        }]
    }),
```

provide credential options (except challenge) during registration
Proposed Flow with WebAuthn (at Payment)

Browser performs `navigator.credentials.get(x)` algorithm where `x` is credentials provided during registration with challenge added.

Challenge is generated using payment details and Payment Request ID (random UUID) using a standard deterministic algorithm.

```javascript
self.addEventListener("paymentrequest", function(e) {
  e.respondWith(new Promise(function(resolve, reject) {
    const assertion = e.credential;
    const challenge = e.challenge;
    resolve({assertion, challenge})
  }));
});
```

Result of WebAuthn challenge and the challenge that was provided are available as properties of the event.
Your payment

Order summary | Total | USD $0.00
---|---|---
Payment | Visa **** 0086 | VISA

Basic Card
A bare bones 'amex'.

Android Pay Only
Only supported method is Android Pay.
WebAuthn UI to launch Payment Handler
Notes and Discussion

- This proposal is not likely to work for JIT install as WebAuthn requires an explicit credential enrollment step.
- Question: Challenge is generated by the browser, which saves a round-trip to the server. Will that work?
- Question: Are scenarios where this flow should not be followed (e.g., the payment handler is not yet set up for this)?
- Would it be useful to augment this proposal for other forms of authentication through the Credentials API?