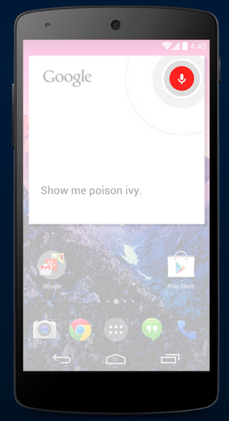
Device-Cenctric Auth and webcrypto

(a wish list for webcrypto)

Dirk Balfanz
Google/FIDO

Device-Centric Auth

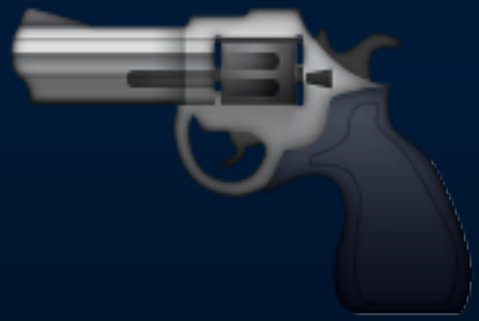
PIN
Biometric
…



Crypto

Device-Centric Auth

Password Thief



Public-Key Crypto

Demo

(of an approximation)

```
function sendBeginSignRequest() {
  $.post('/BeginSign',
   .done(function(si
      console.log(s
      showMessage("
     var sessionIds
      for (var i = 0
        sessionIds[si                    a[i].sessionId;
        delete signData[                 onId'];
      }
      u2f.sign(signData, function (response) {
           if (response.errorCode) {
             onError(response.errorCode, false);
           } else {
             response['sessionId'] = sessionIds[response.keyHandle];
             onTokenSignSuccess(response);
           }
       })
   })
   .fail(function(xhr, status) {
      showError("can't authenticate: " + status);
   });
}
```

version: U2F_V2,
appId: google.com,
challenge: 02938123938473 4,
keyHandle: wuasiuassowieklsdnmx,

My Wish List

- keys are origin-bound, but outside the browser
- user agent adds information to to-be-signed data
- keys are bound to local user authentication (biometric, screen lock)
- attestation
- key discovery of local authenticators

What’s Not on My Wish List

- An “authentication” API
- A way to talk with the user agent about user accounts
- A new UI that the user agent needs to show