Webfinger

and friends

Context

You *have*:

an identifier for a service or user

You *want:*

public metadata about the identifier

Interesting Identifiers

acct:bob@example.org

http://somecompany.com

https://mydomain.com

http://cliqset.com/users/jsalmon

...

Interesting personal metadata

public profile URL(s)
public activity stream(s)
photo sharing service(s)
social graph service(s)
email provider(s)
preferred payment service(s)
private service discovery service(s)
public key(s)
reputation service(s)
...

Interesting domain metadata

IdP endpoints
OAuth endpoints
public key(s)
reputation service(s)
...

Webfinger

Email and *email like* identifiers

Make up acct: URI scheme for the machines

GET http(s)://*hostname*/.well-known/host-meta
yields an XRD document with
a rel="lrdd" template
resolving to a user XRD documen
which contains
links to user services and metadata

Domain Discovery

Host names as identifiers - mycompany.com

Already have http(s): scheme

GET http(s)://*hostname*/.well-known/host-meta
yields an XRD document with
links to domain services and metadata

General (LRDD) Discovery

In: Any kind of URI as long as it's http(s) or acct

Use Webfinger-style lookup for all URIs by default
host-meta can say "look at resource instead" (-> Link: header and <link> elements)
if no host-meta, fall back to "look at resource"

Out: **links to services and metadata**

Example

http://webfingerclient-dclinton.appspot.com/lookup?identifier=jpanzer.at.acm@gmail.com&format=web

Example: Salmon

Mention @bob@example.com
Does a Webfinger lookup to find the rel="salmon-mention" endpoint for acct:bob@example.comPOSTs data to that endpoint

Verify a salmon from acct:alice@example.org
Does a Webfinger lookup to find the rel="magic-public-key" URL for aliceGETs data from that URL to check signature on message

Ask an IdP to sign a salmon on behalf of current user
Do domain discovery on IdP domain, look for rel="salmon-signer" URL and OAuth endpoints
Do OAuth dance (once) + POST to salmon signer

Security

Attack Vectors:

- MITM between client and any or all of the XRD providers
- DNS spoofing (of the client)
- Site defacement attacks on /.well-known or resources
- Implementation bug exploits

Mitigations:

- SSL w/CA validation *or* XRD signature w/CA validation
- Treat non-validated data as advisory/hints only, verify securely
- Keep protocol simple