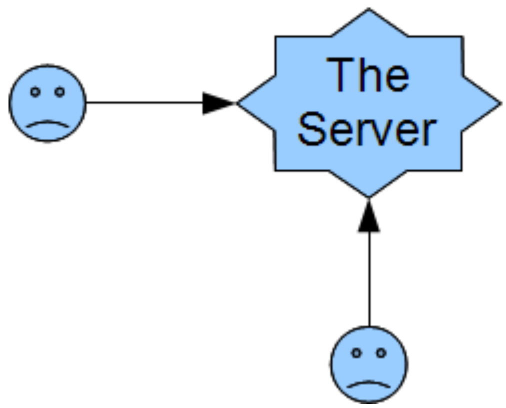
Securing the Social Web by Moving Beyond Client-Server Security

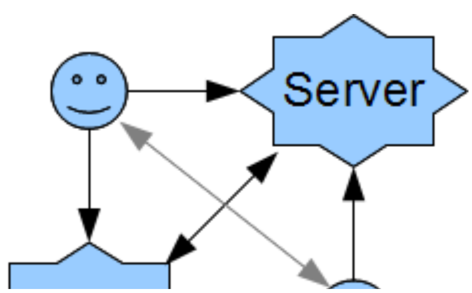
Tyler Close
Google, engineer

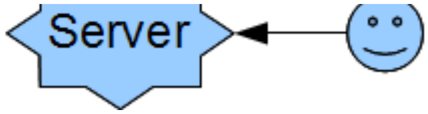
Client-Server Model



- Isolated clients connect to a single server.
- One identification and one possible attacker.

Web Model



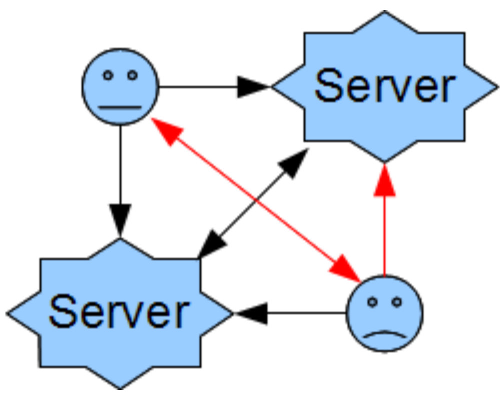


- Social (email, chat, napkins, ...) clients connect to many servers.
- One identification but many possible attackers.

Web as Client-Server

When used as a Client-Server model, all those extra arrows are attack vectors. Different names for different combinations: phishing, XSS, CSRF, clickjacking, ...

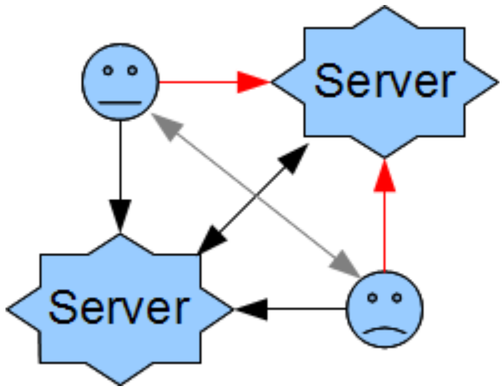
Phishing



One client gives another a link to an

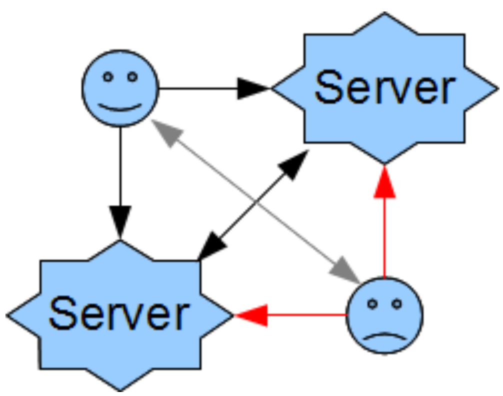
unexpected server.

XSS



A client gives a server content that it gives to another client.

CSRF or clickjacking



A server gives a client a link to an unexpected server.

But happy users

- Note the happy versus sad faces.
- Those other arrows aren't just attack vectors, they are also work and play vectors.
- Social Computing means ever more use of those other arrows.
- Need a different security model.

Where to from here?

- Social Web means frequent referrals over diverse channels
- Requests come from complex, multi-party collaboration
- "*Who* sent this request?" is a question with no useful answer
- "*What* access has been applied?" can be tracked using explicit token passing

web-key

- Every URL for an access controlled

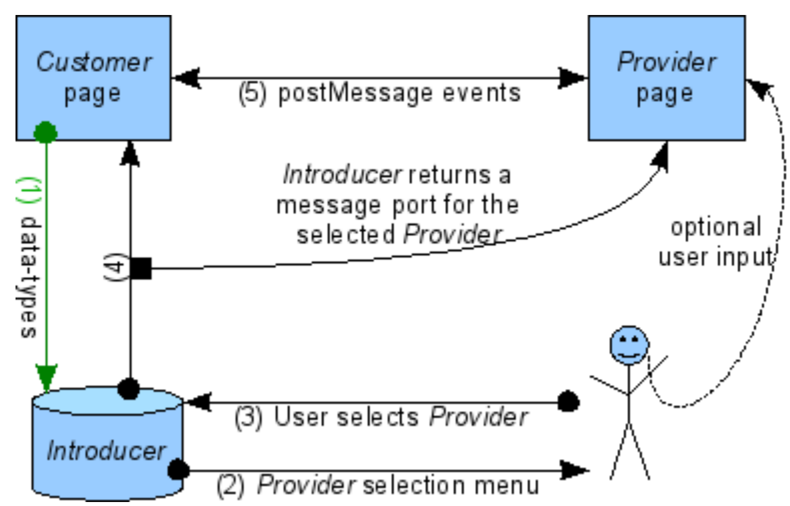
resource carries the corresponding permission token.

- `./#s=4mrz4gknjpc6zi`
- `./#s=`*(permission token)*

But what if…

- … accidentally send web-key for bank account
- Don't put valuable web-keys in harm's way
- Put them in the Introducer instead

Web Introducer



- DEMO: Edit a syndicated blog post

Go forth and make secure, social, killer

apps!

http://web-send.org/