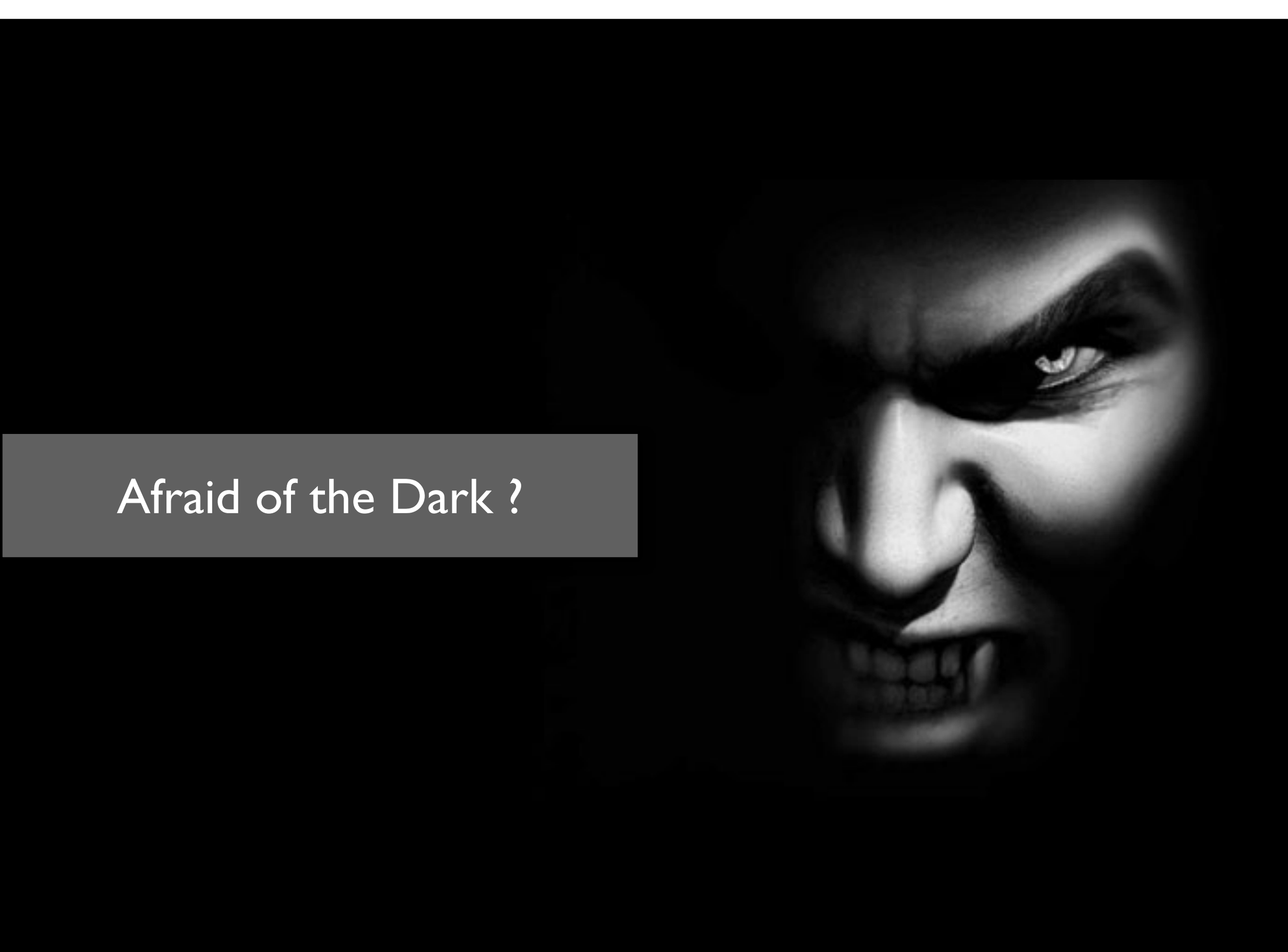
Session Juggler

Chinmay Soman, Elie Bursztein, Dan Boneh, John Michell
Stanford University


Antec

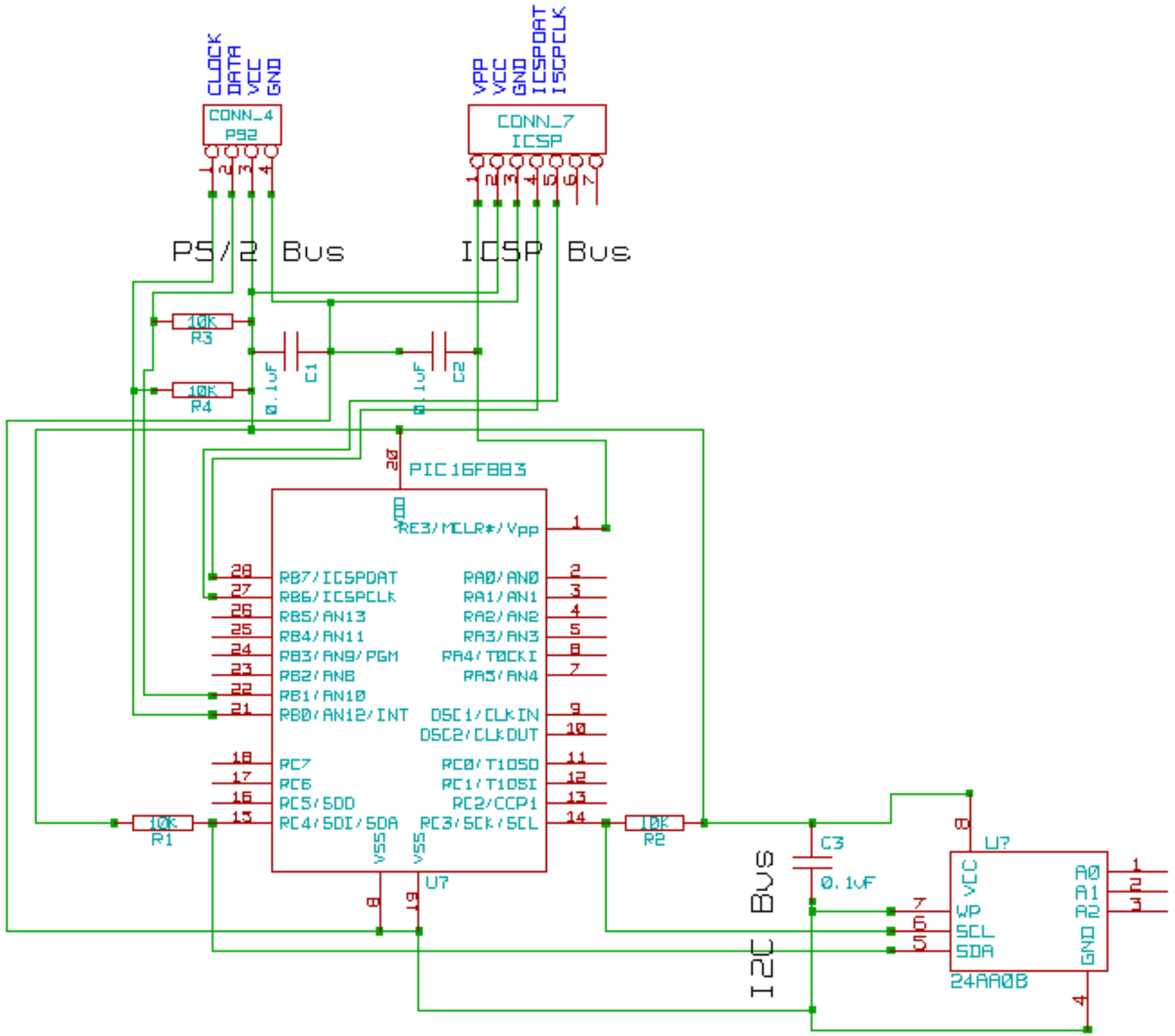

DELL
DELL

Afraid of the Dark ?



Looking for something ?

Looking for something ?



Ephemeral login

- Can’t trust the client at all
- Work for every browser on every site
- Use a secure device / secure channel (phone)

Not that easy

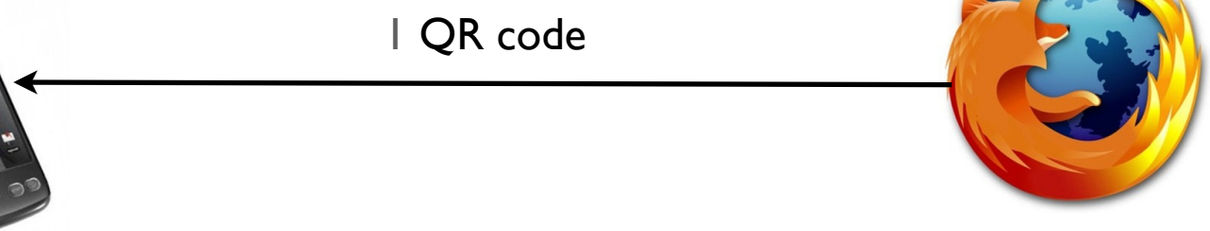
	[5]	[24]	[29]	[21]	[12]	[28]	[31]
year	1999	2004	2006	2007	2008	2008	2009
Trusted device	Palm Pilot	PDA	Phone	Phone	Phone	Phone	Phone
Requires server-side changes	✓	✓	✓	✓		✓	
Requires client-side changes	✓	✓	✓	✓	✓	✓	✓
Connection type	USB	USB	Net	USB/BT	USB	Net	NFC
Hardware needed					TPM		TPM/NFC

Sometime bad guys make the best good guys

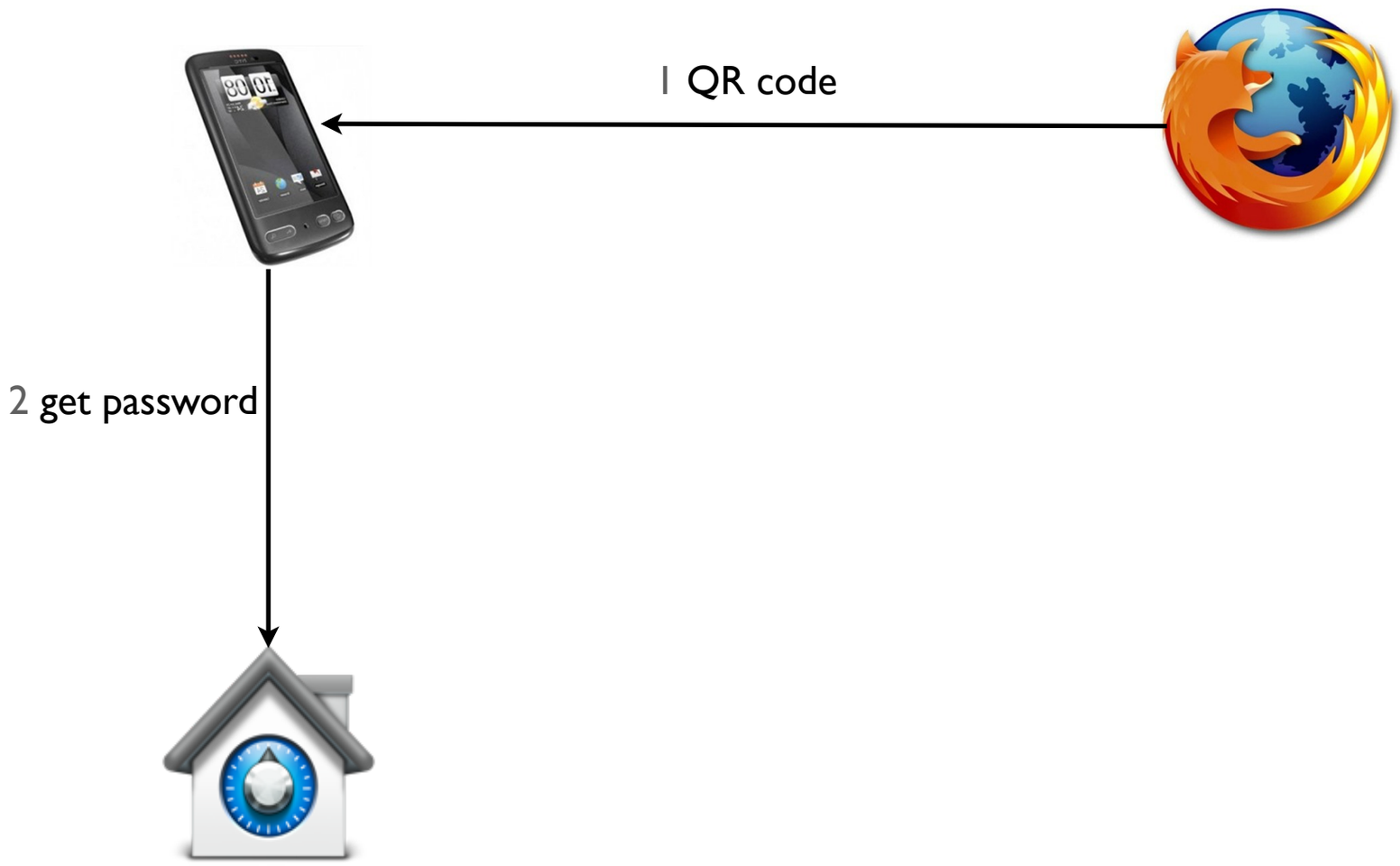
Let’s steal a session (demo)

Workflow

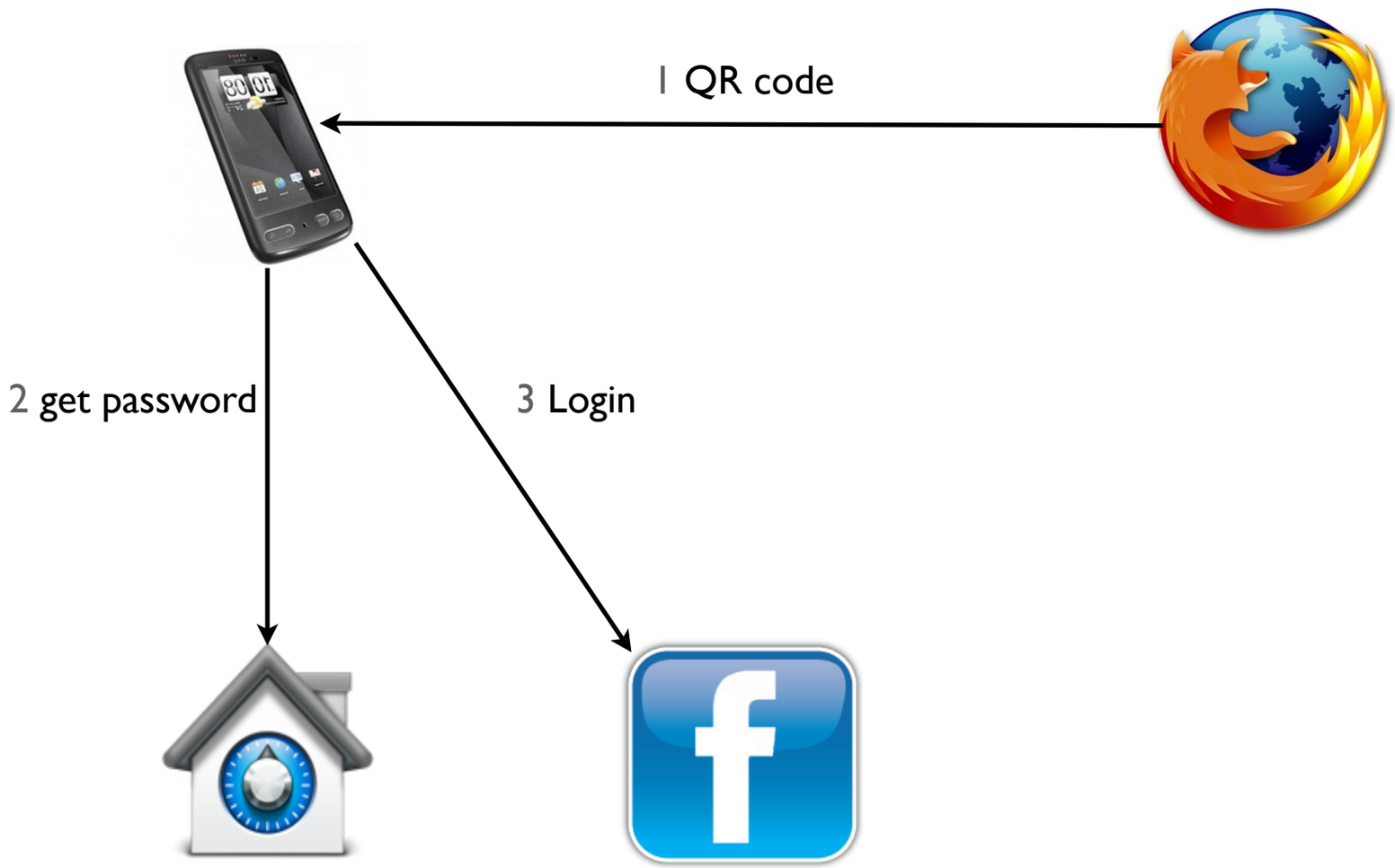
Workflow



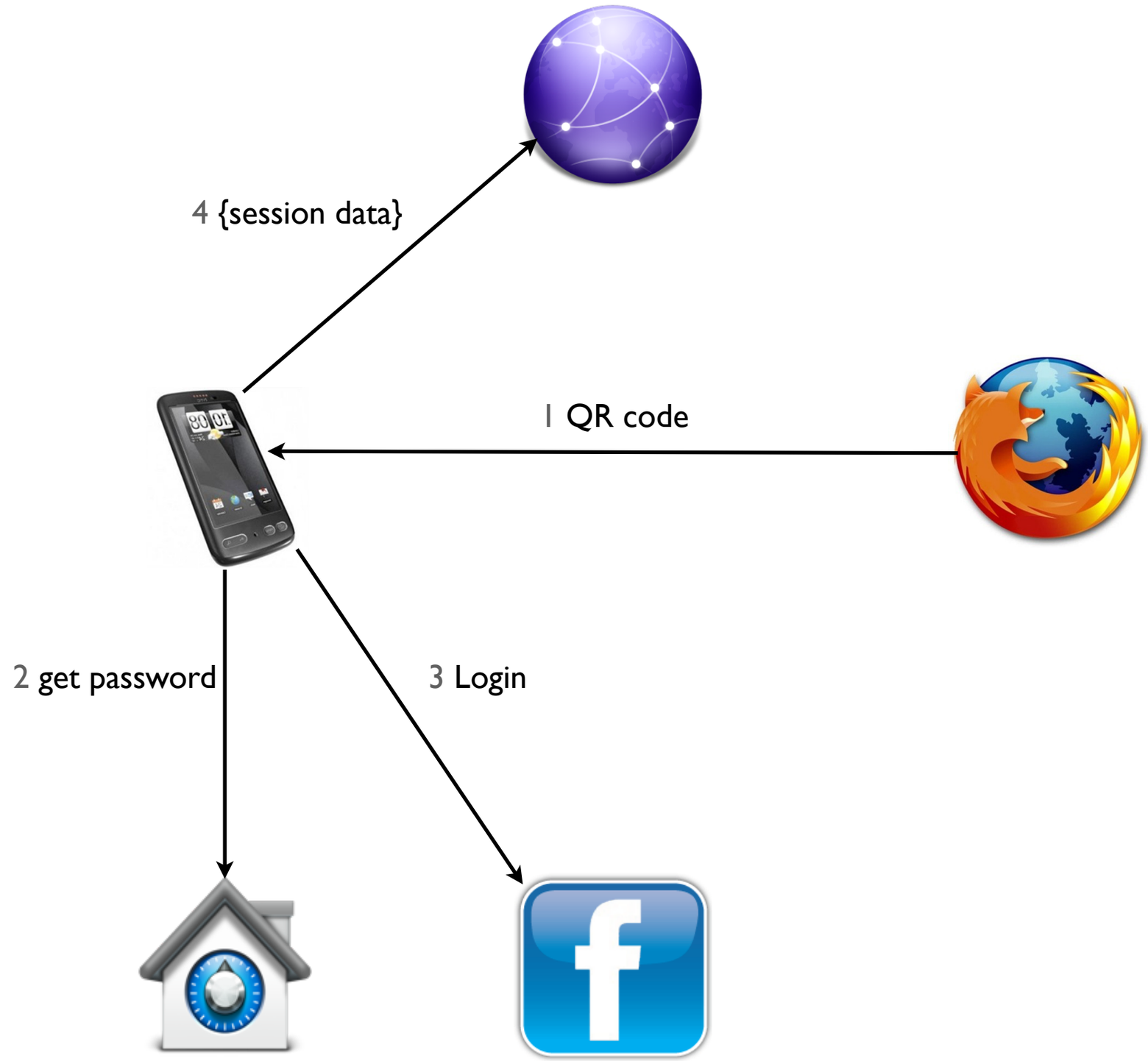
Workflow



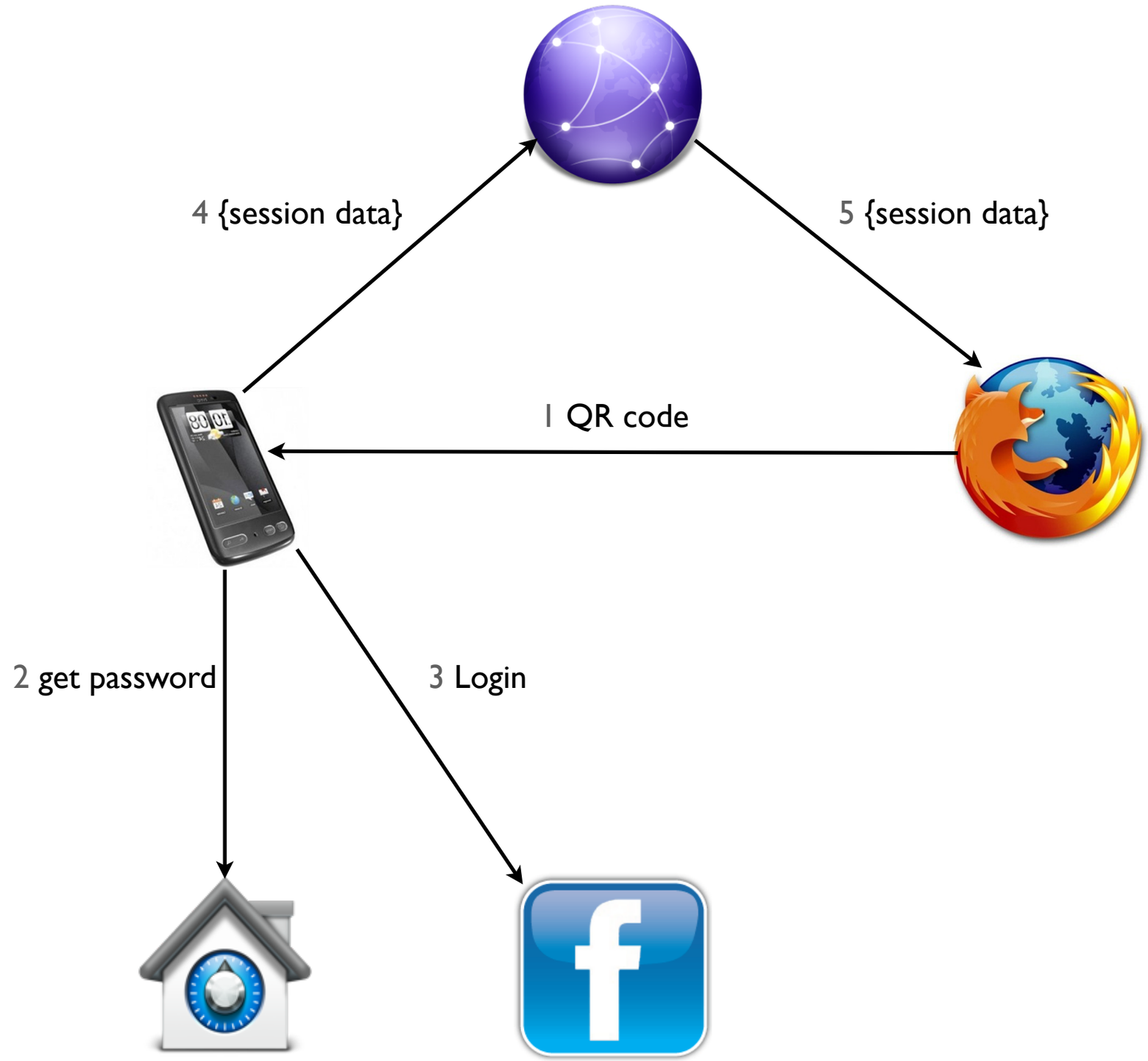
Workflow



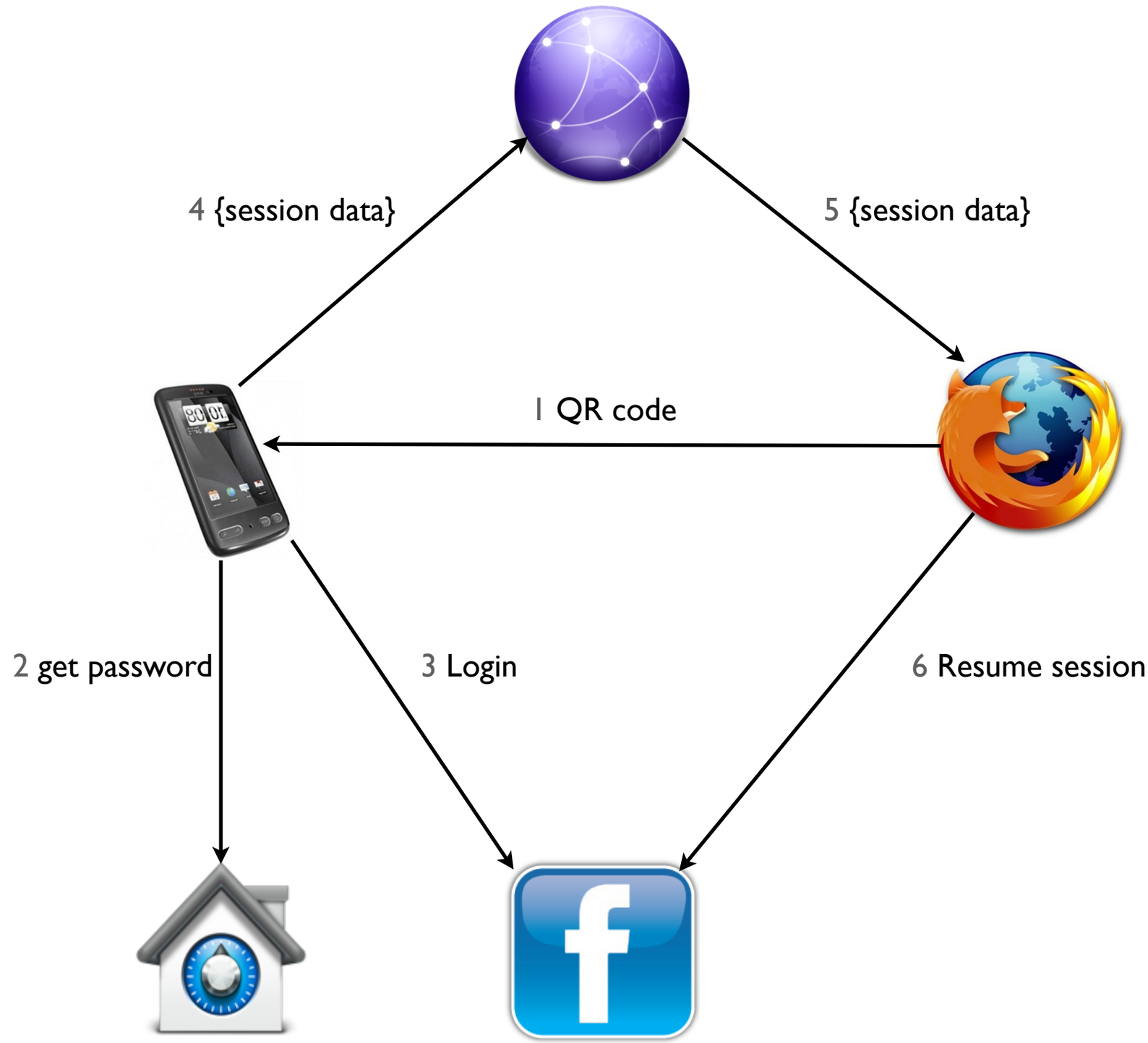
Workflow



Workflow



Workflow


4 {session data}
5 {session data}
1 QR code
2 get password
3 Login
6 Resume session

Hijacking defense

Defense	% of Alexa100
Login over HTTPS	83%
Using secure cookies	52%
Seperating mobile and desktop sessions	6%
Binding session to IP address	8%
Checking local time	1%
Binding session to `user-agent` header	0%
Binding session to local language	0%
Logout over HTTPS	1%

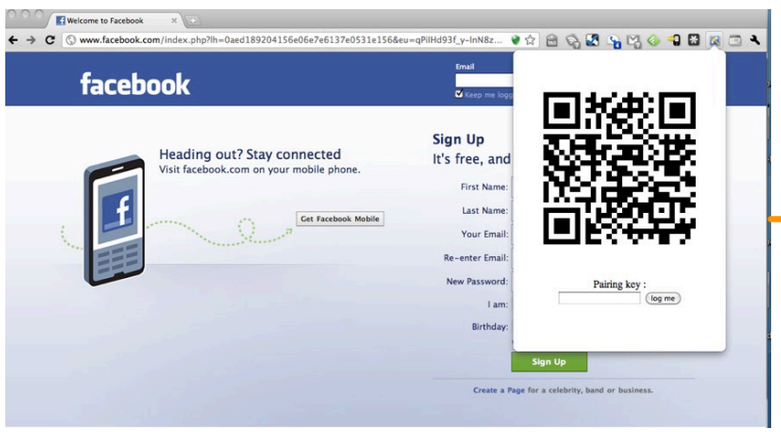
Experimental results

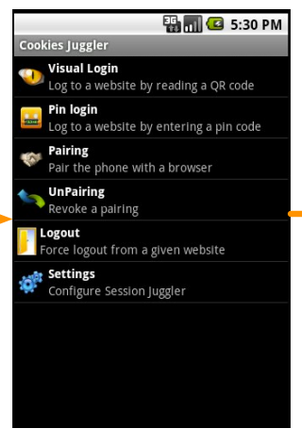
- Works on 98% of the Alexa top 100
- Can be extended to work against arbitrary defense

Conclusion

- Steal http session to provide a temporary login
- No server side or client modification

Questions ?

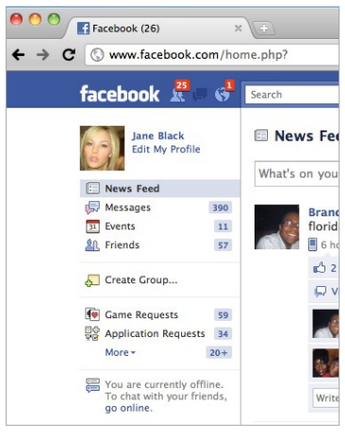

Welcome to Facebook
www.facebook.com/index.php?lh=0aed189204156e06e7e6137e0531e156&eu=qPiIHd93f_y-InN8z...
facebook
Email
Keep me logg
Heading out? Stay connected
Visit facebook.com on your mobile phone.
Get Facebook Mobile
Sign Up
It's free, and
First Name:
Last Name:
Your Email:
Re-enter Email:
New Password:
I am:
Birthday:
Sign Up
Create a Page for a celebrity, band or business.
Pairing key :
log me


5:30 PM
Cookies Juggler
Visual Login
Log to a website by reading a QR code
Pin login
Log to a website by entering a pin code
Pairing
Pair the phone with a browser
UnPairing
Revoke a pairing
Logout
Force logout from a given website
Settings
Configure Session Juggler


9:38 AM
Do you want to be logged to
www.facebook.com
Discard
Log me in


5:35 PM
login
facebook
Facebook helps you connect and share with the people in your life.


5:37 PM
login
facebook
Search
Jane Black
Edit My Profile
News Feed
Messages
Events
Friends
Create Group...
Game Requests
Application Requests
More
Transfer Session


Facebook (26)
www.facebook.com/home.php?
facebook
Search
Jane Black
Edit My Profile
News Feed
Messages
Events
Friends
Create Group...
Game Requests
Application Requests
More
You are currently offline. To chat with your friends, go online.

Alternative architecture