O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web

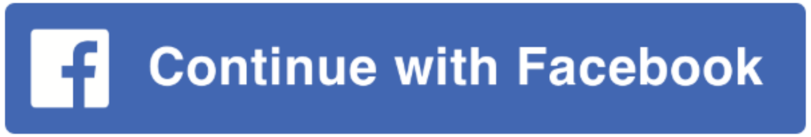
Mohammad Ghasemisharif, Amrutha Ramesh, Stephen Checkoway, Chris Kanich, and Jason Polakis

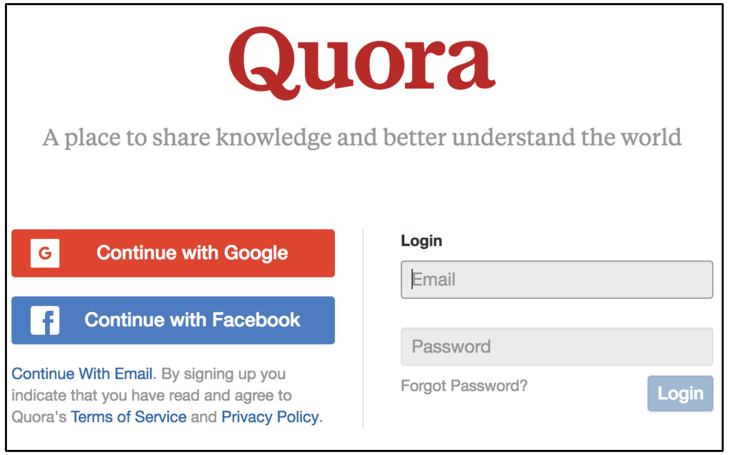
University of Illinois at Chicago

COMPUTER SCIENCE
COLLEGE OF ENGINEERING
UIC

USENIX Security Symposium, August 2018

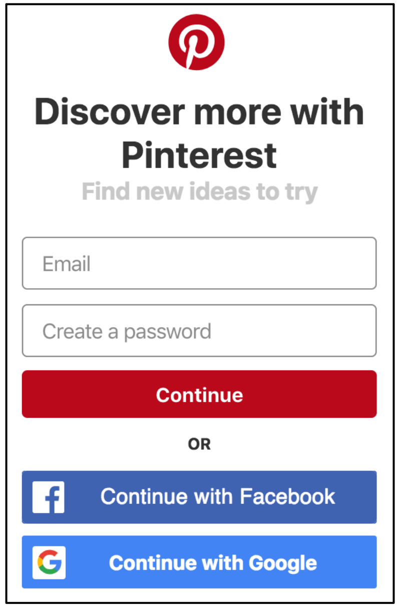
Single Sign-On





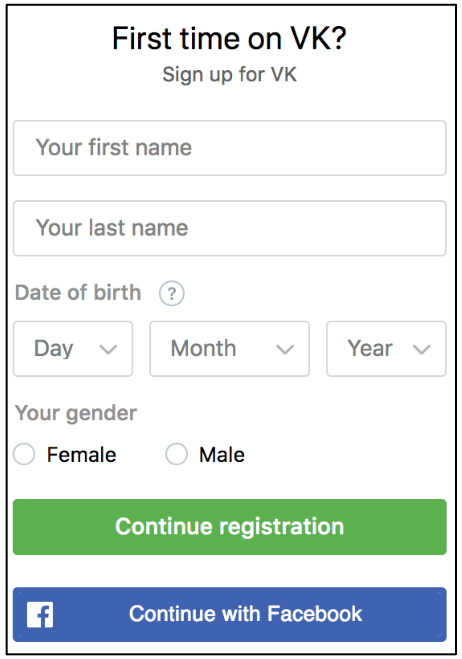
A place to share knowledge and better understand the world

Continue With Email. By signing up you indicate that you have read and agree to Quora's Terms of Service and Privacy Policy.



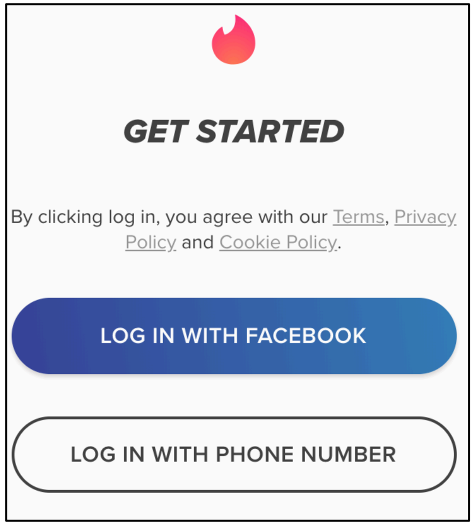
Discover more with Pinterest

Find new ideas to try



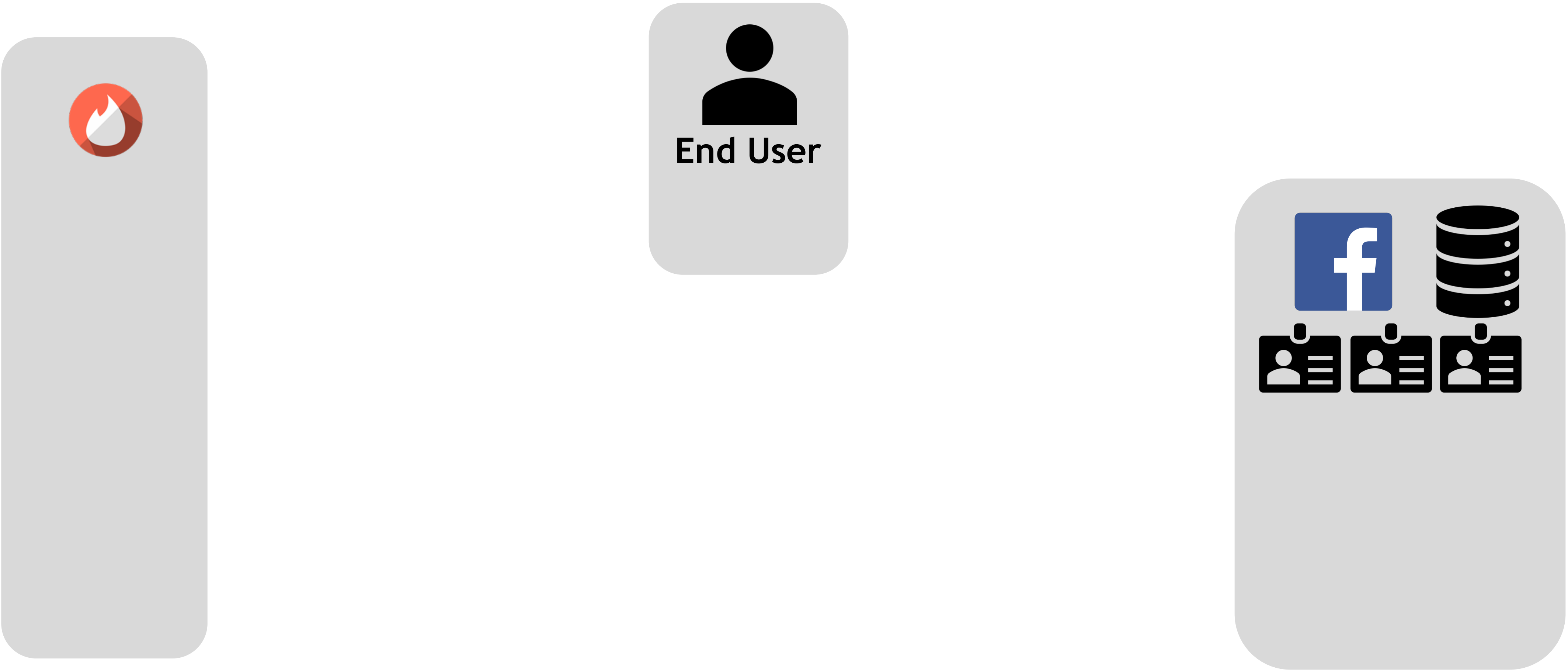
First time on VK?

Sign up for VK



By clicking log in, you agree with our Terms, Privacy Policy and Cookie Policy.

Single Sing-On Authentication Flow

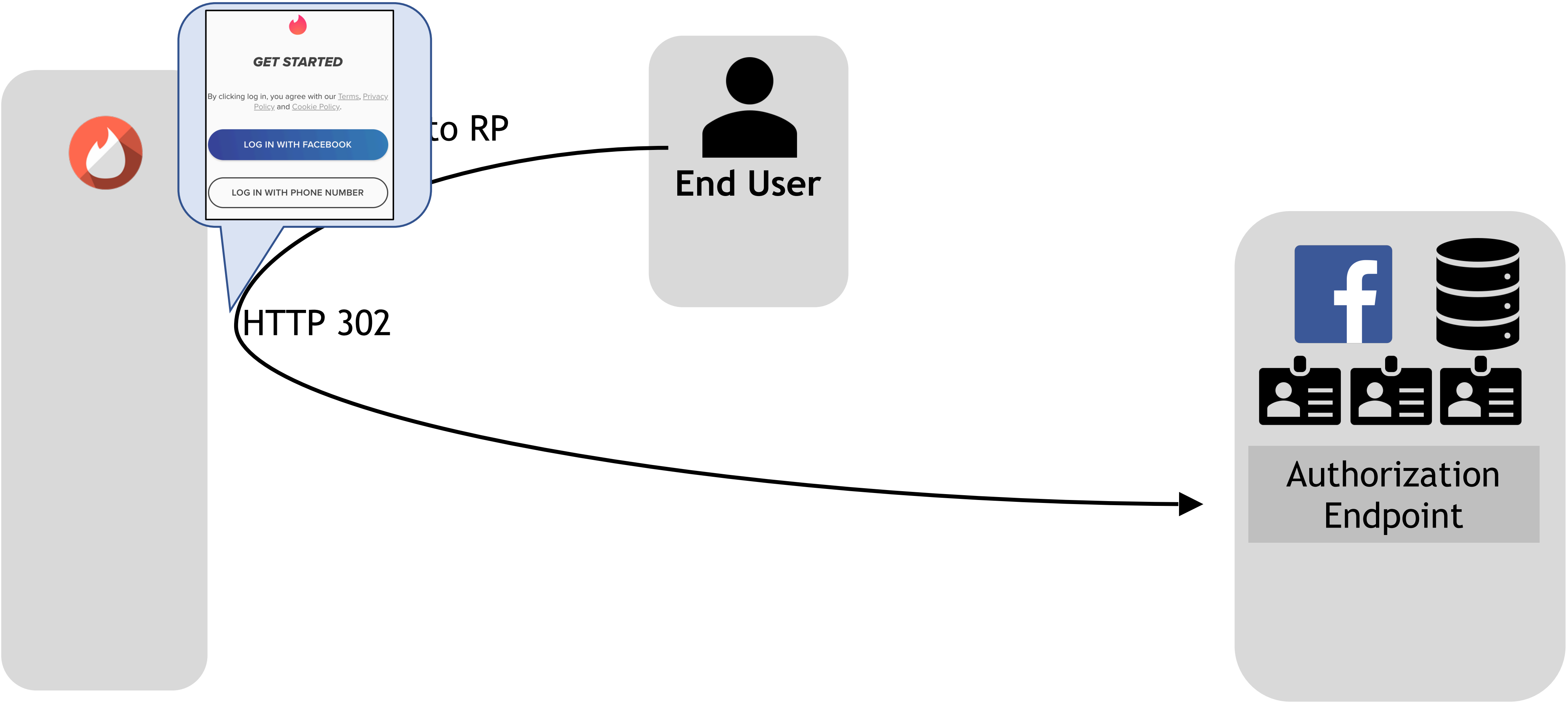


End User

Relying Party
(RP or client)

Identity Provider
(IdP or OP)

Single Sing-On Authentication Flow



GET STARTED

By clicking log in, you agree with our Terms, Privacy Policy and Cookie Policy.

LOG IN WITH FACEBOOK

LOG IN WITH PHONE NUMBER

to RP

End User

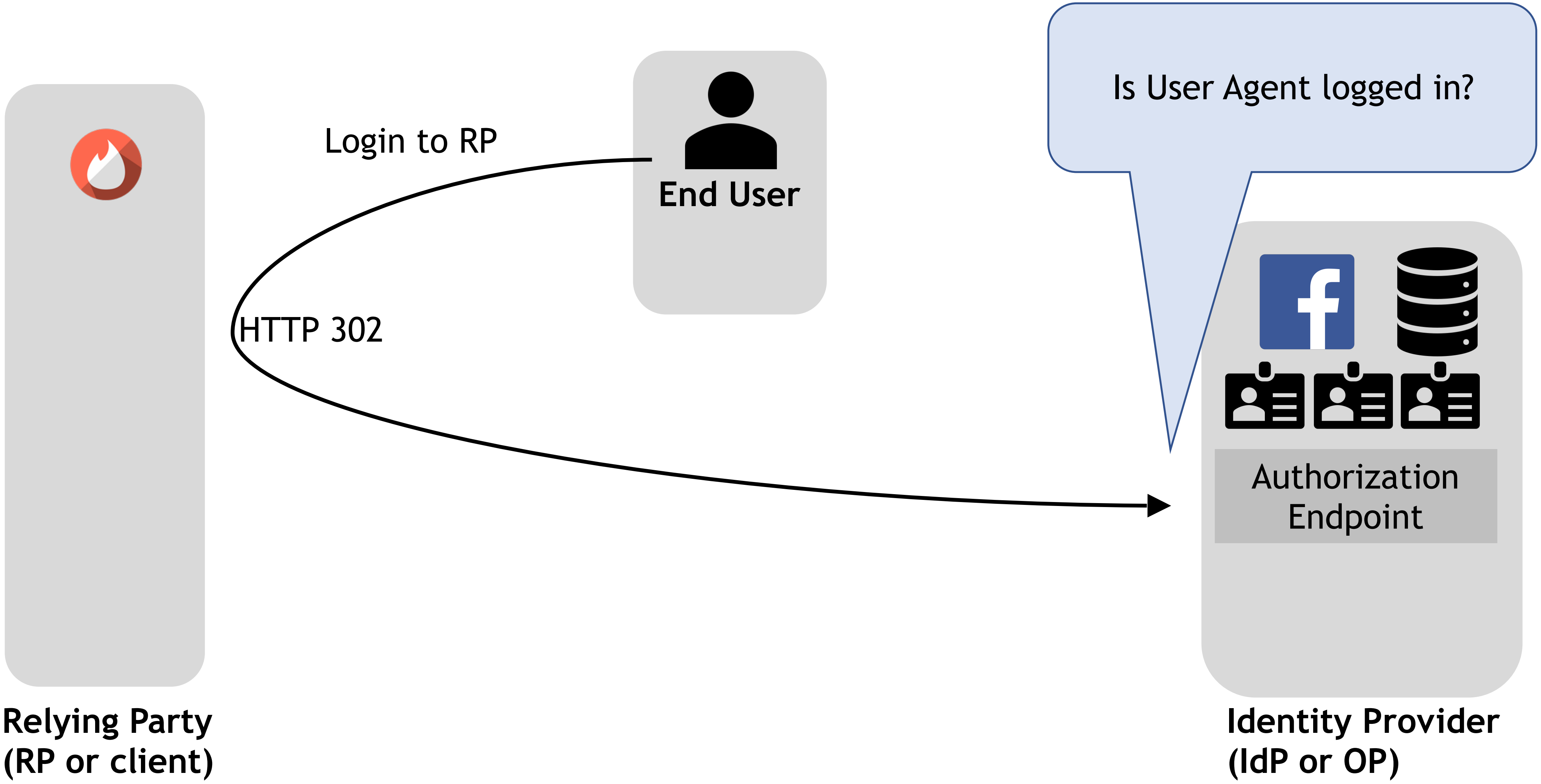
HTTP 302

Authorization Endpoint

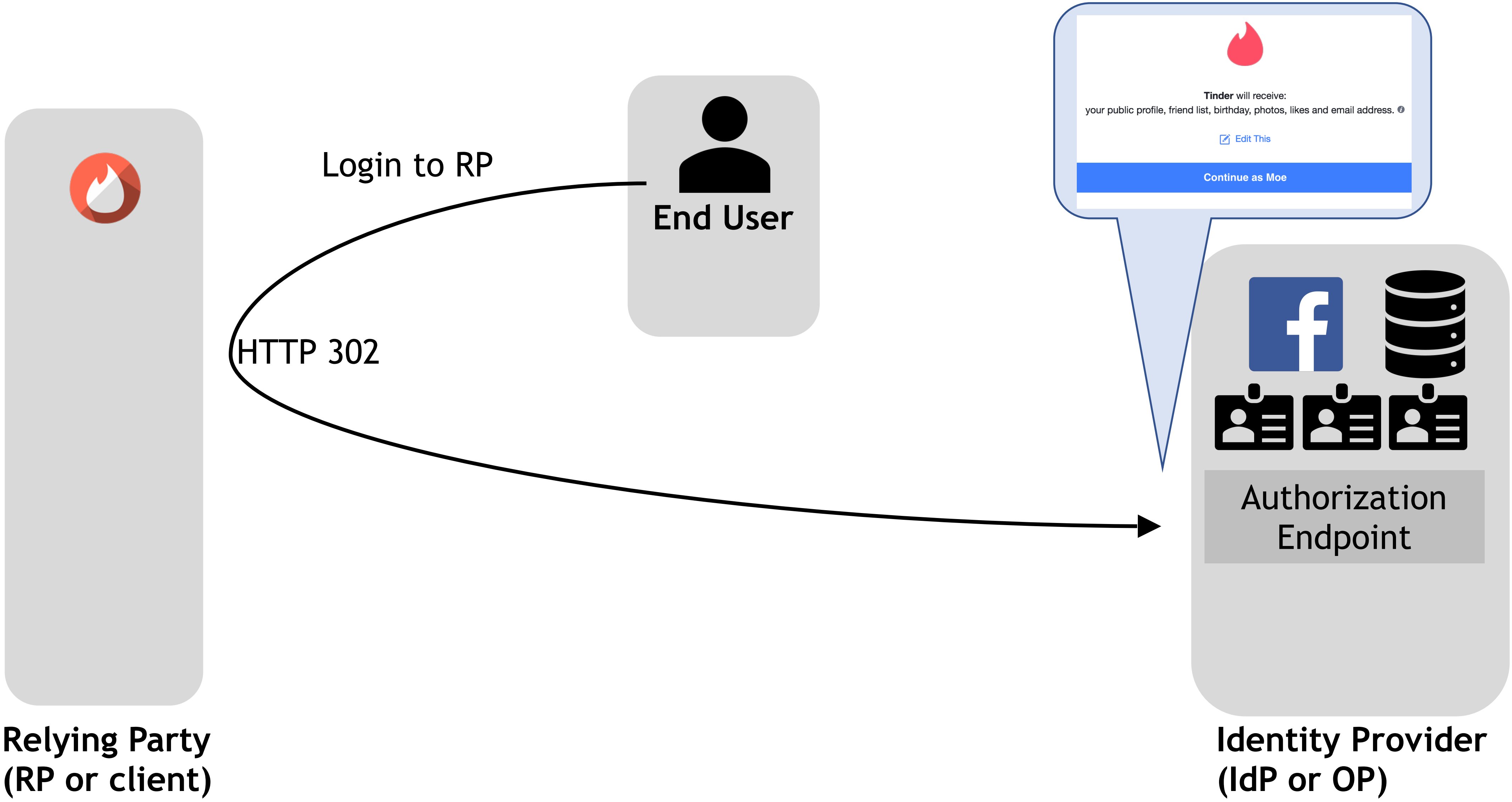
Relying Party
(RP or client)

Identity Provider
(IdP or OP)

Single Sing-On Authentication Flow



Single Sing-On Authentication Flow



Login to RP

End User

HTTP 302

Tinder will receive:
your public profile, friend list, birthday, photos, likes and email address.

Edit This

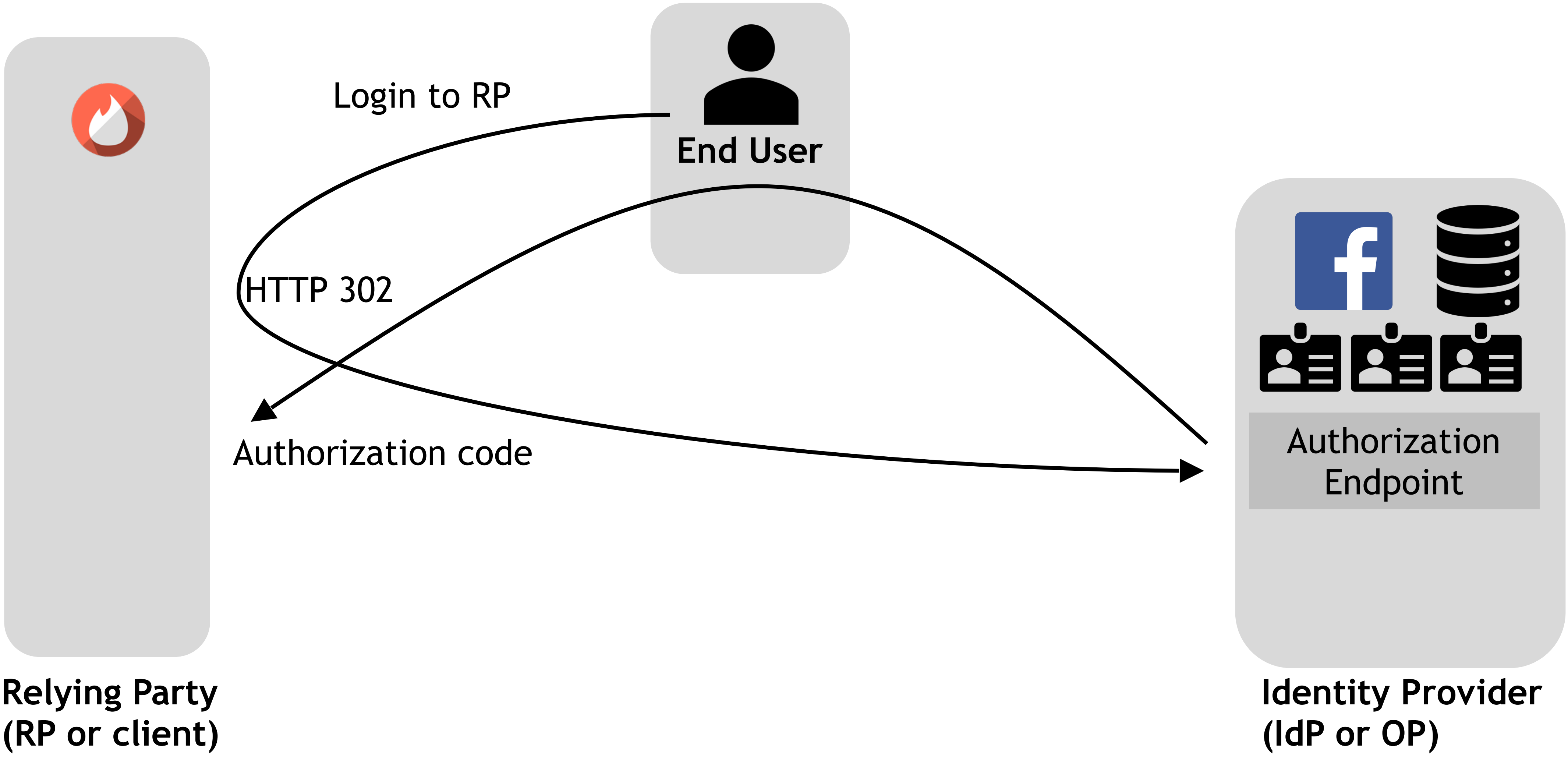
Continue as Moe

Authorization Endpoint

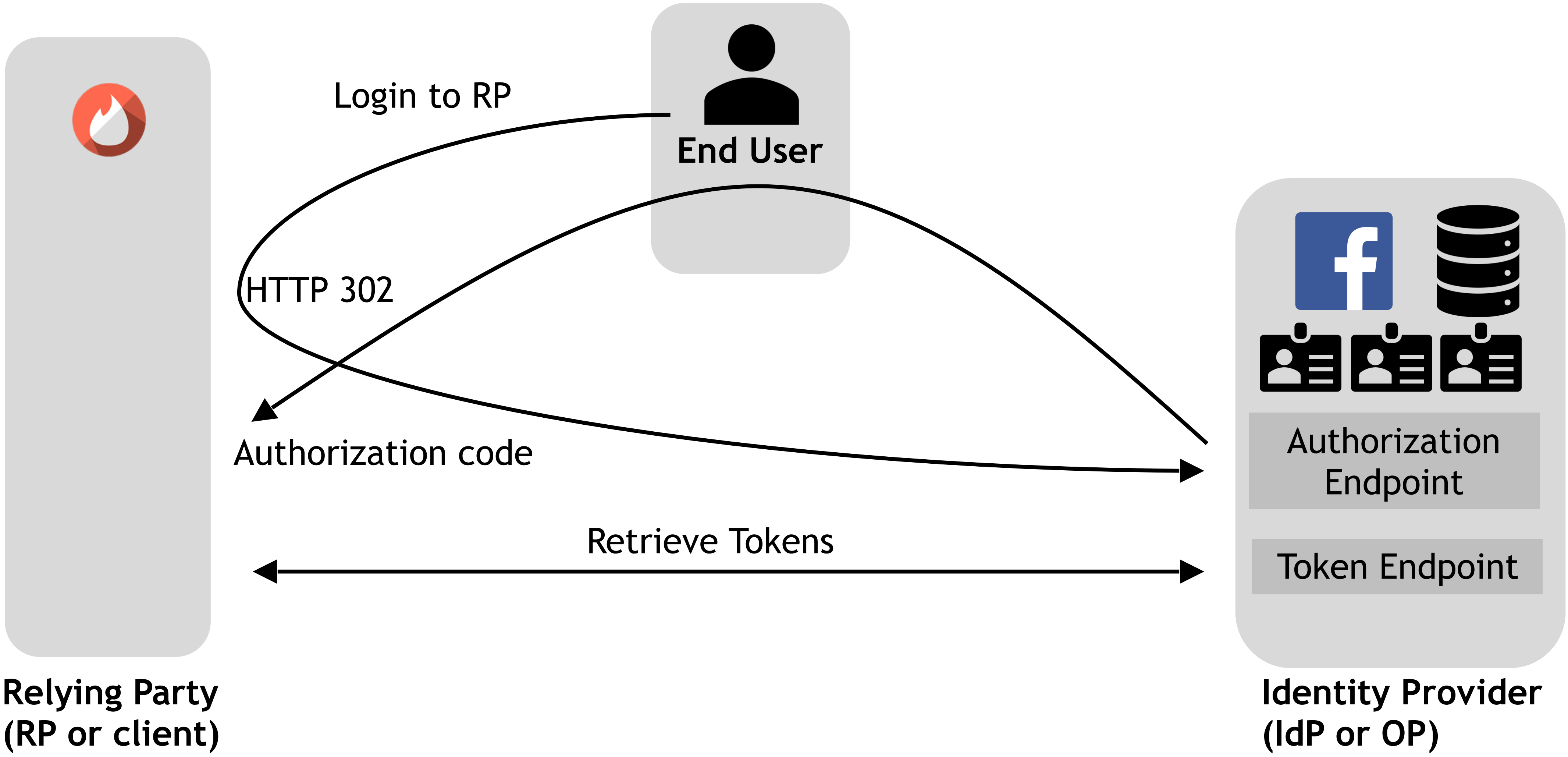
Relying Party
(RP or client)

Identity Provider
(IdP or OP)

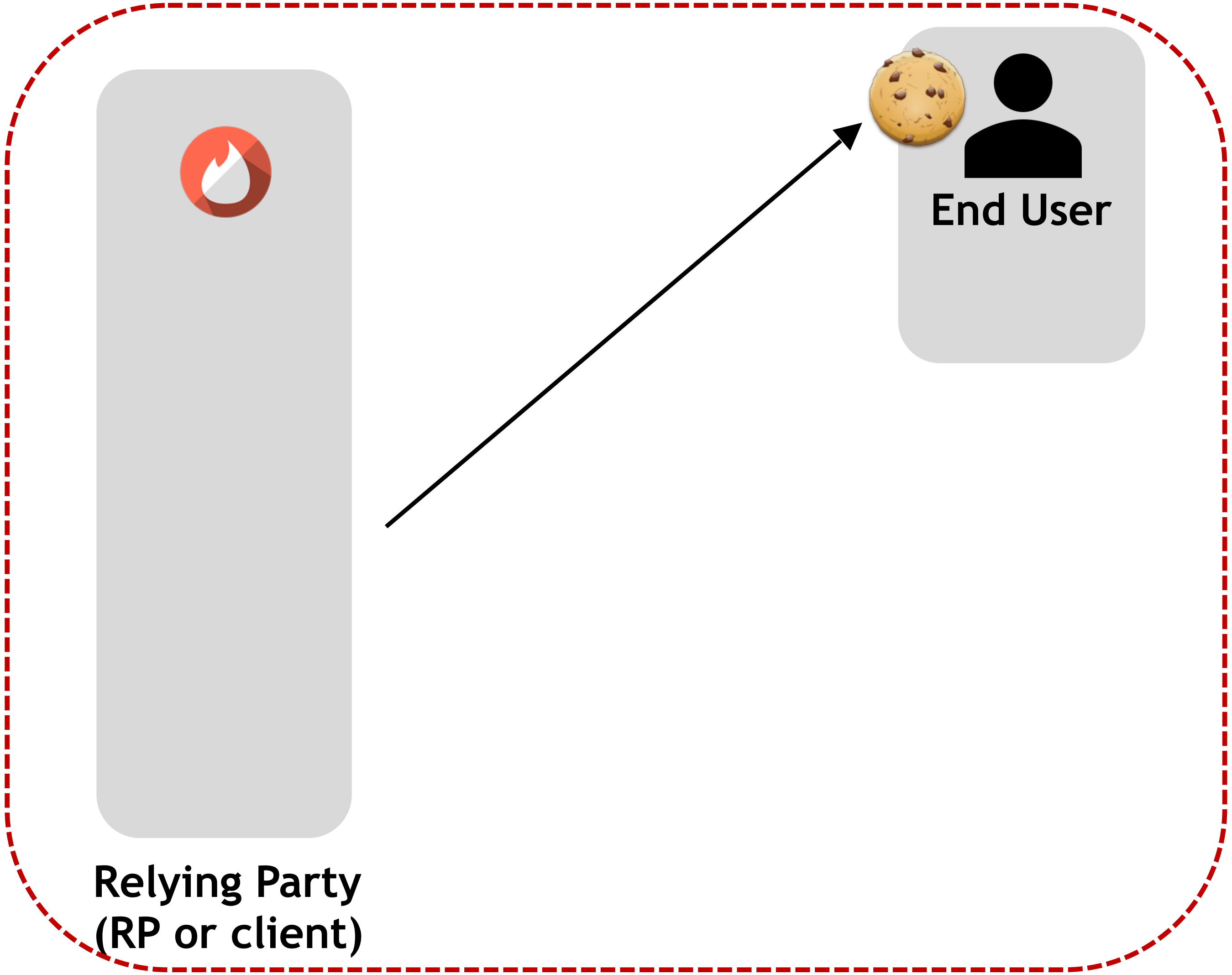
Single Sing-On Authentication Flow



Single Sing-On Authentication Flow



Single Sing-On Authentication Flow

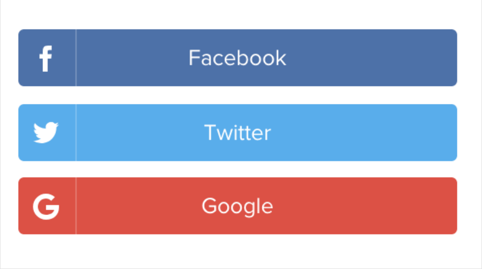


Single Sign-On, the Good, the Bad and the Ugly

Single Sign-On, the Good, the Bad and the Ugly

Good 😀

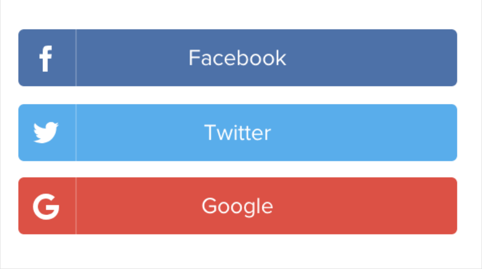
- Ease of use
- Integrated experience
- Eliminates burden of multiple account creation



Single Sign-On, the Good, the Bad and the Ugly

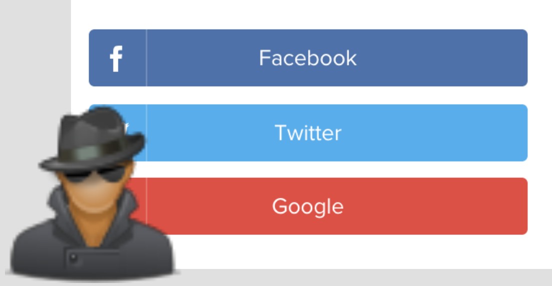
Good 😃

- Ease of use
- Integrated experience
- Eliminates burden of multiple account creation



Bad 😒

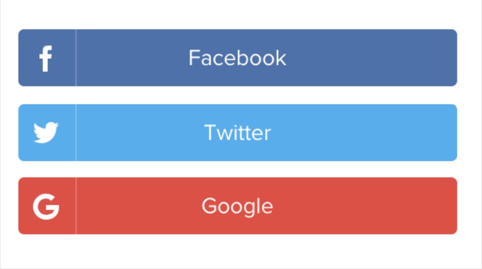
- Attackers can leverage the same functionality to increase access coverage even when it is implemented correctly



Single Sign-On, the Good, the Bad and the Ugly

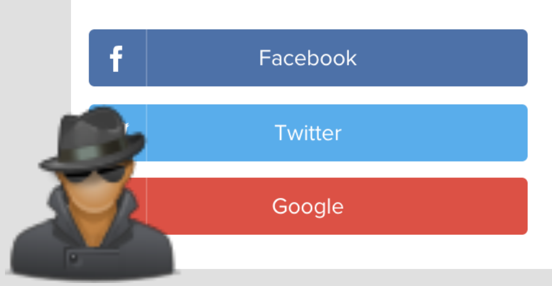
Good 😃

- Ease of use
- Integrated experience
- Eliminates burden of multiple account creation



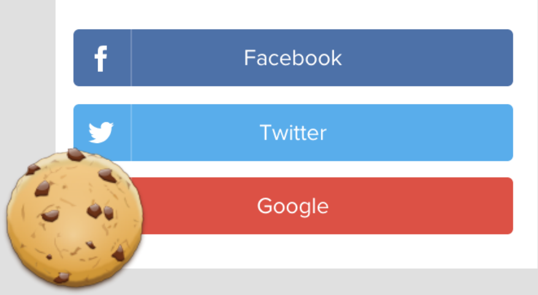
Bad 😑

- Attackers can leverage the same functionality to increase access coverage even when it is implemented correctly



Ugly 😲

- Very hard/impossible to recover from IdP account compromise



Threat Model

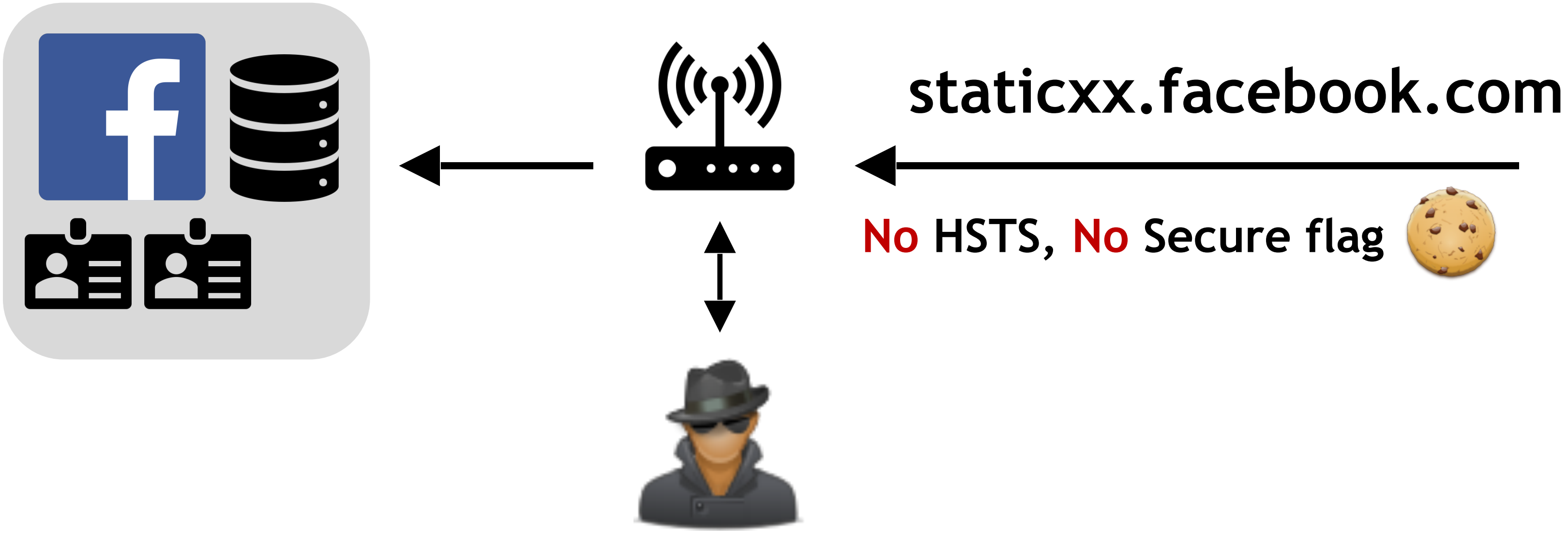
- IdP accounts are *keys to the kingdom*
  - We are not concerned with **how** they are compromised
- In our experiments we consider
  - Phishing (main type of Google account compromise [Bursztein et al., IMC'14])
  - Cookie hijacking [Sivakorn et al., S&P'16]
- These attacks capture different levels of capabilities and technical difficulty

Facebook Account Takeover

- Audited Messenger, Instagram, Main FB app on major platforms

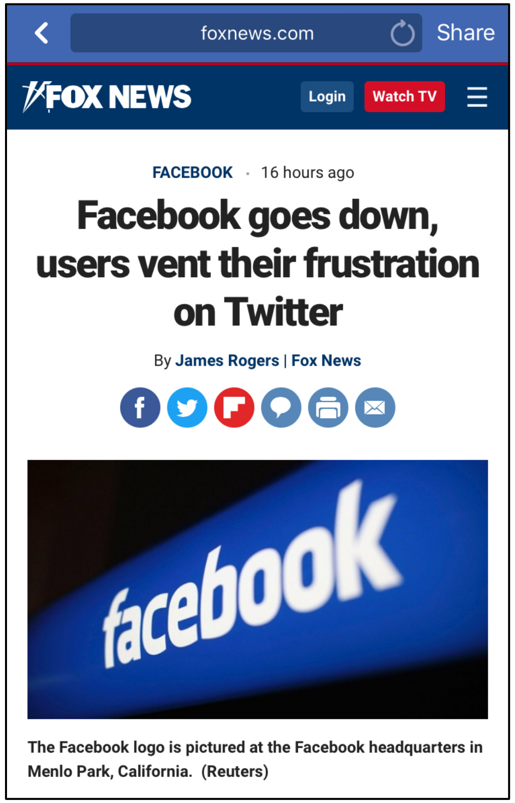
Facebook Account Takeover

- Audited Messenger, Instagram, Main FB app on major platforms



staticxx.facebook.com

No HSTS, No Secure flag



FACEBOOK · 16 hours ago

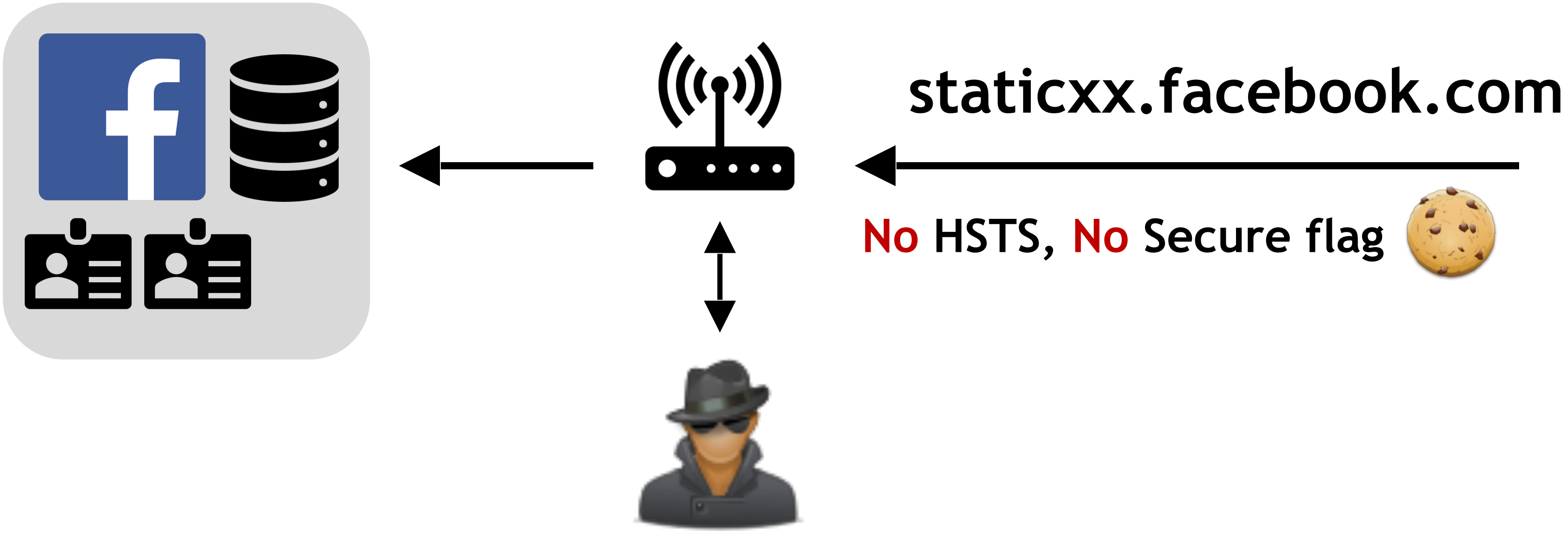
Facebook goes down, users vent their frustration on Twitter

By James Rogers | Fox News

The Facebook logo is pictured at the Facebook headquarters in Menlo Park, California. (Reuters)

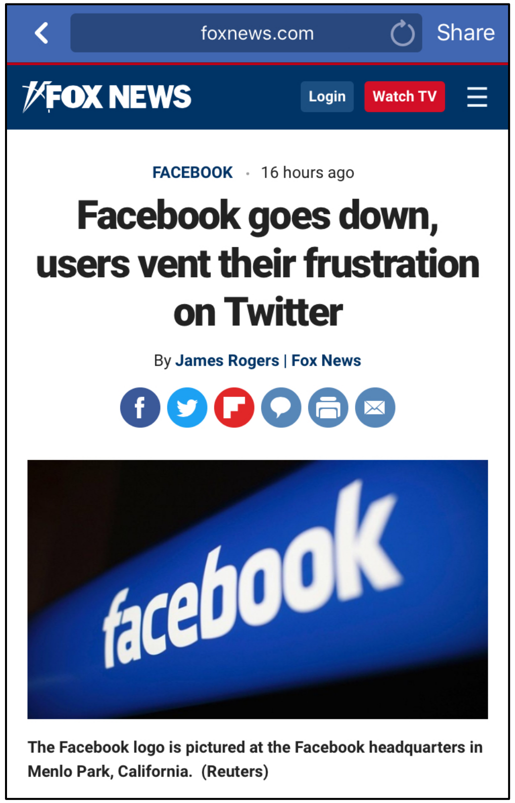
Facebook Account Takeover

- Audited Messenger, Instagram, Main FB app on major platforms
- Attacker’s session doesn’t show up in FB active sessions



staticxx.facebook.com

No HSTS, No Secure flag



FACEBOOK · 16 hours ago

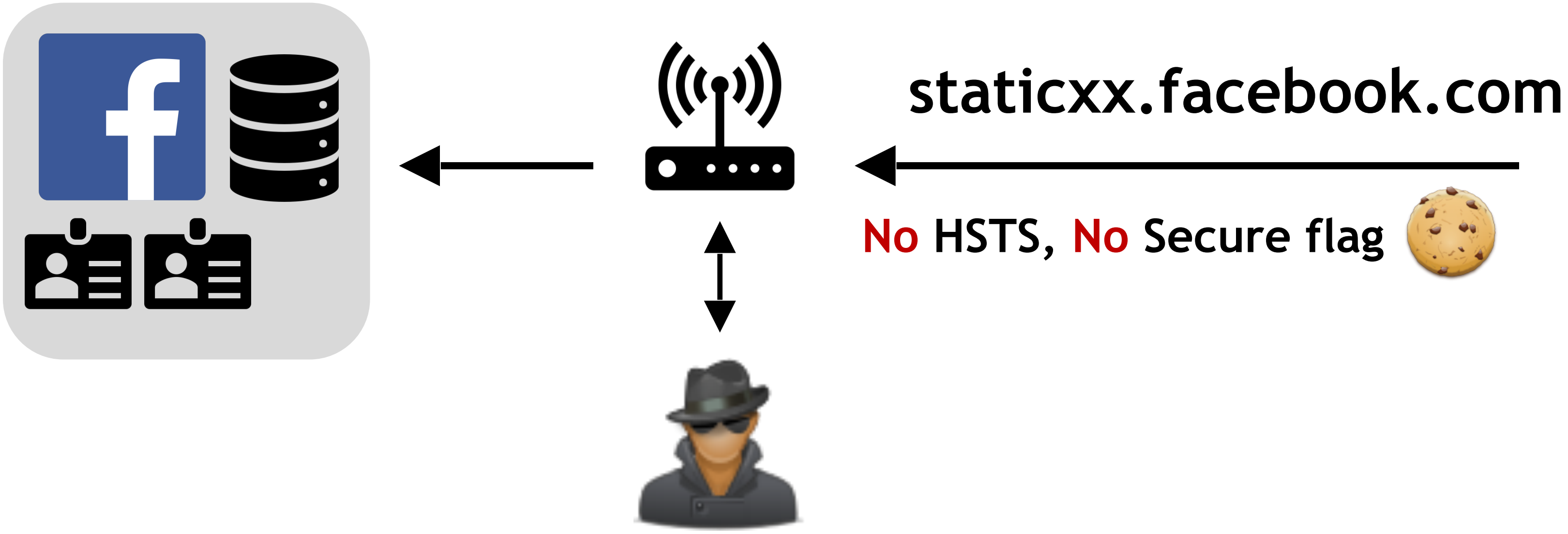
Facebook goes down, users vent their frustration on Twitter

By James Rogers | Fox News

The Facebook logo is pictured at the Facebook headquarters in Menlo Park, California. (Reuters)

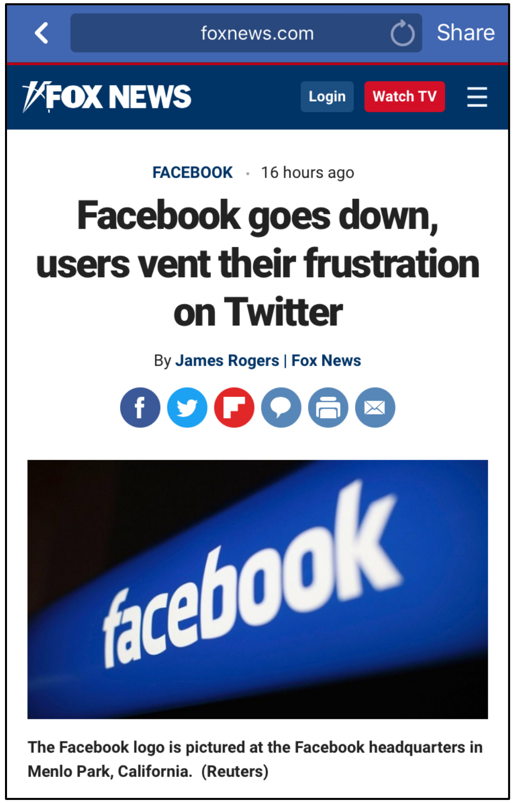
Facebook Account Takeover

- Audited Messenger, Instagram, Main FB app on major platforms
- Attacker's session doesn't show up in FB active sessions
- Session hijack also allows password overwrite



staticxx.facebook.com

No HSTS, No Secure flag



FACEBOOK · 16 hours ago

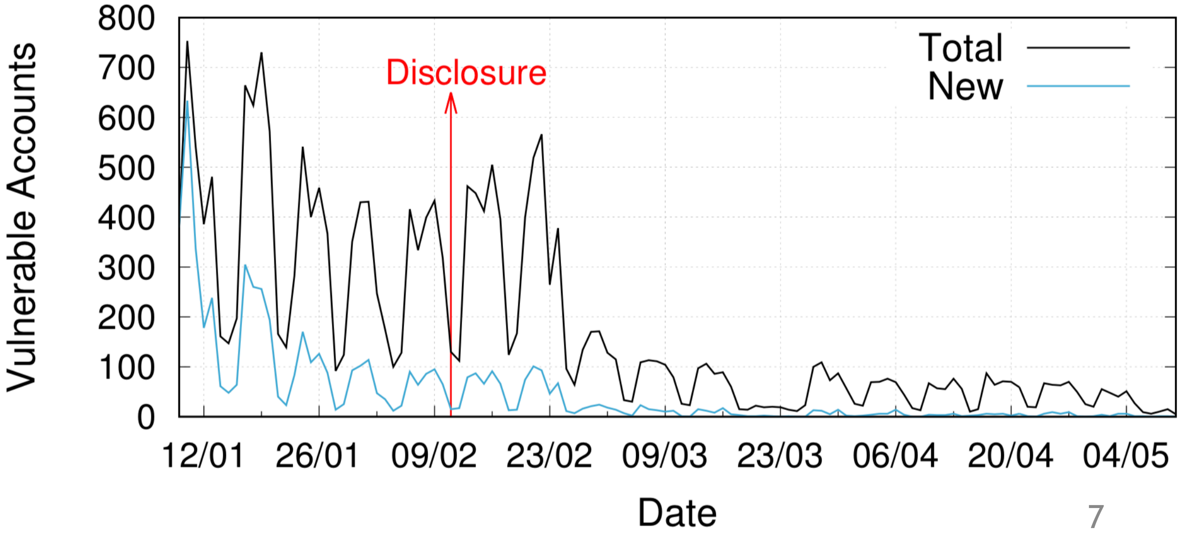
Facebook goes down, users vent their frustration on Twitter

By James Rogers | Fox News

The Facebook logo is pictured at the Facebook headquarters in Menlo Park, California. (Reuters)

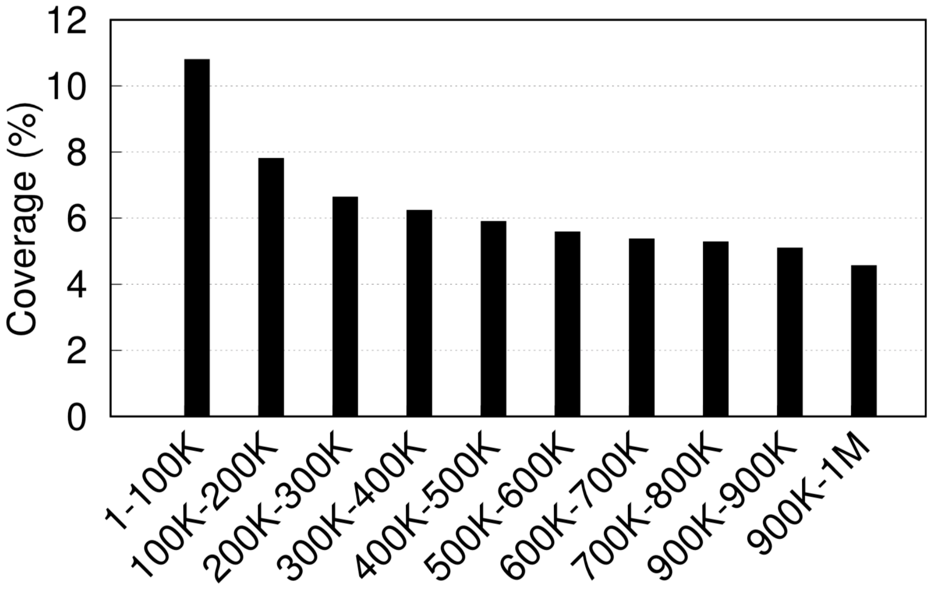
Quantifying Facebook Vulnerability

- Passively monitored university's wireless traffic for duration of four months (January – May 2017) [IRB approved]
- **5,729** unique session cookies
- Total account takeover through cookie hijacking
- 11 different subdomains



Quantifying SSO Adoption

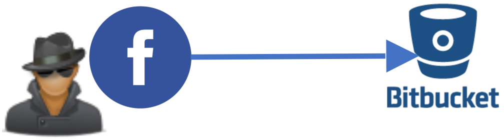
- 65 IdPs (OAuth 2.0 and/or OpenID Connect)
- Crawled Alexa top 1 million
- 912,206 correctly processed
- 57,555 (6.3%) SSO support
  - Prominent IdP: Facebook (4.62%)
  - Google (2.75%)
  - Twitter (1.34%)



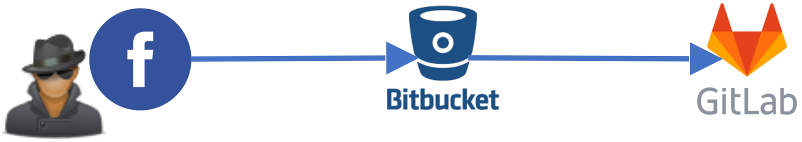
Some RPs Are IdPs

Some RPs Are IdPs

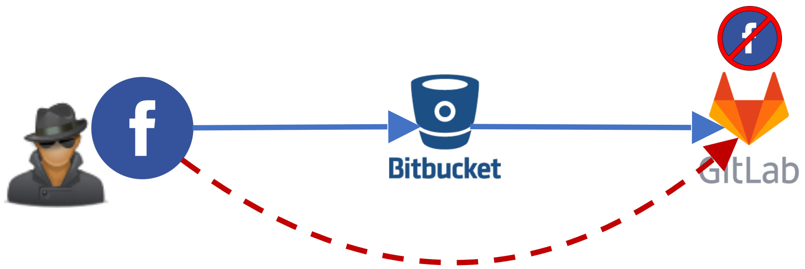
Some RPs Are IdPs



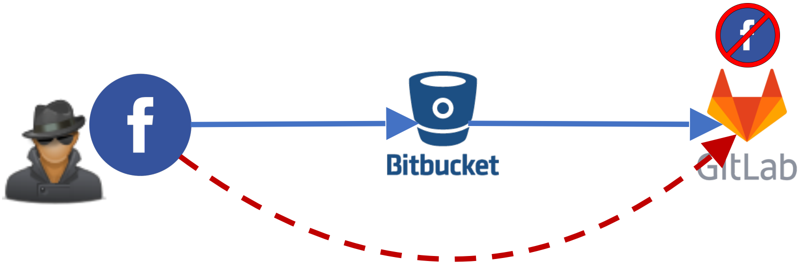
Some RPs Are IdPs

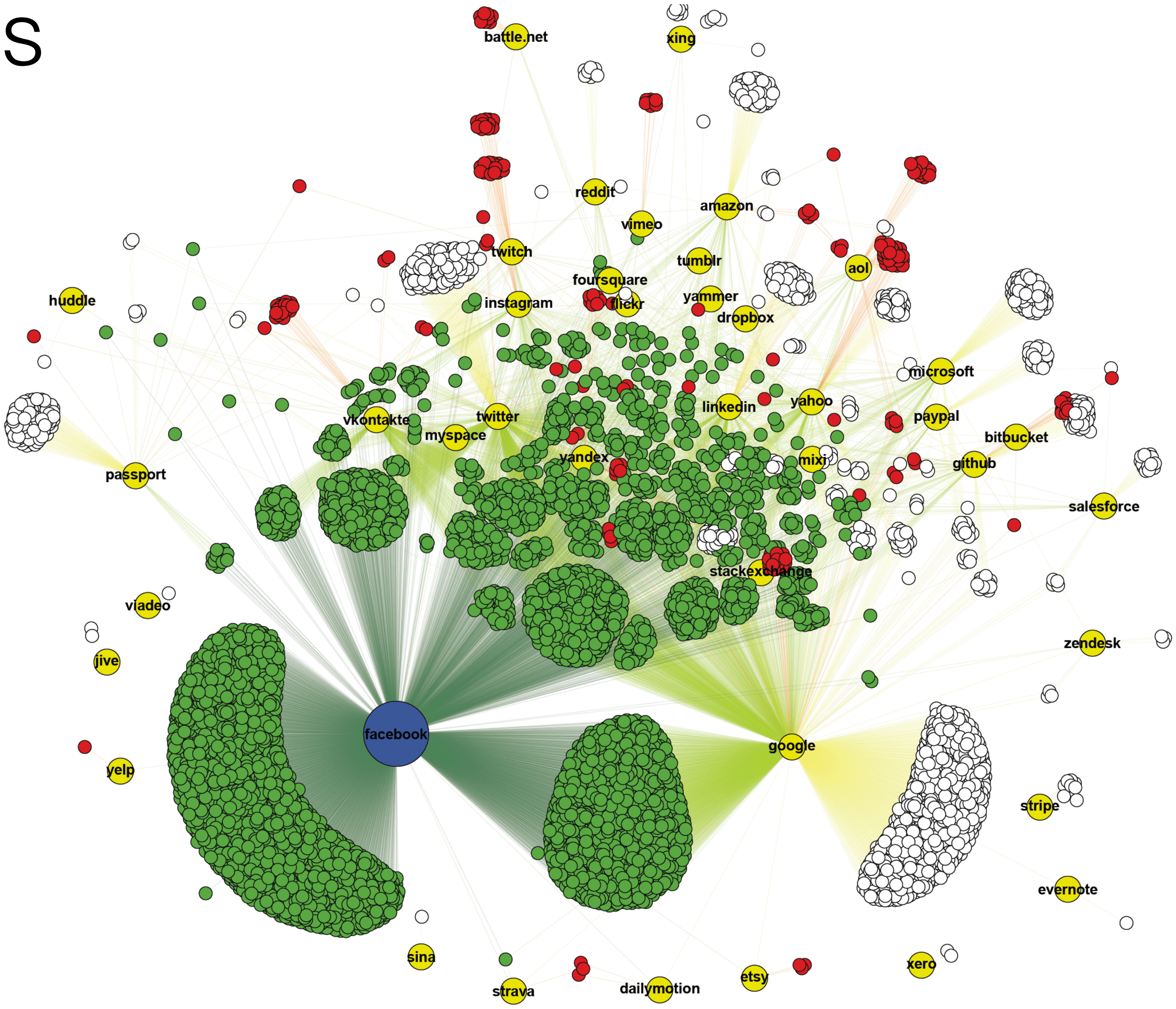


Some RPs Are IdPs



Some RPs Are IdPs





Dual behavior in IdPs: 52%

3.1% increase coverage in Alexa top 100K

Attack Scenarios

- RP account takeover
- Preemptive RP account takeover

Relying Party Account Takeover

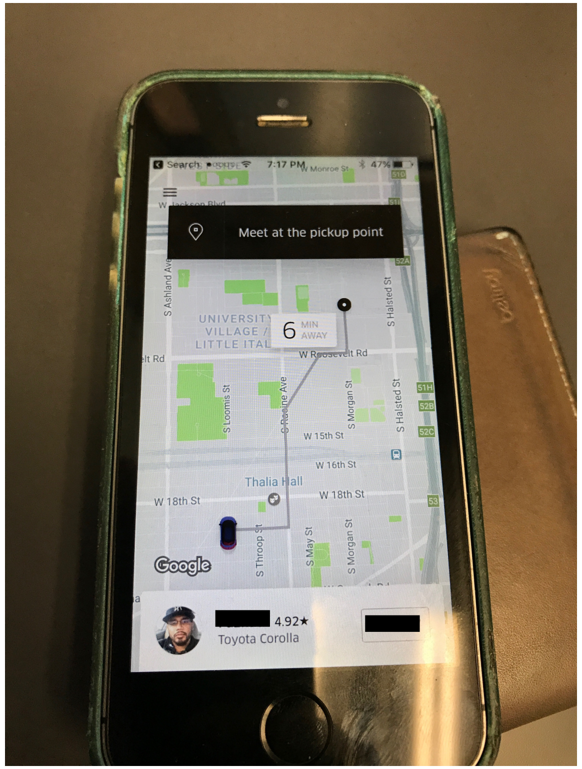
- Studied 95 major services
    - 29 Web from Alexa top 500
    - 66 iOS applications

- *Is it feasible to access RP services using hijacked IdP cookie?*
- *How much of the attack is visible to the victim?*
- *How long can the attacker maintain the access?*

Relying Party Account Takeover

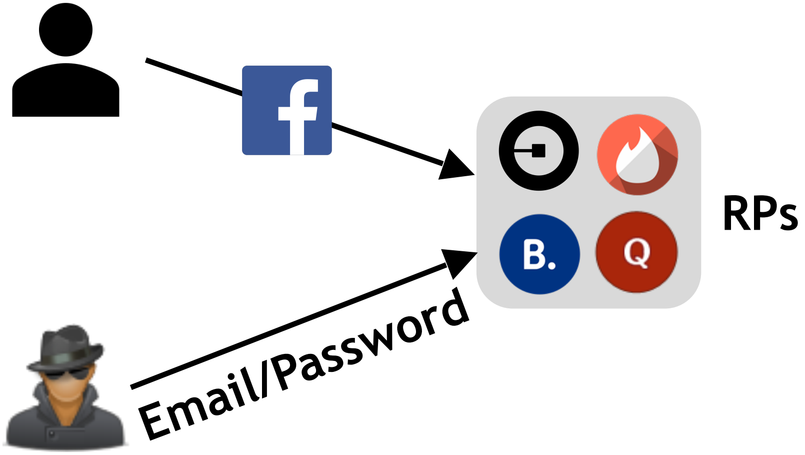
- 98% **did not** require reauthentication when using cookies
- Visibility test on 95 services:
  - None of the RPs notified victim
  - No alarm on Facebook

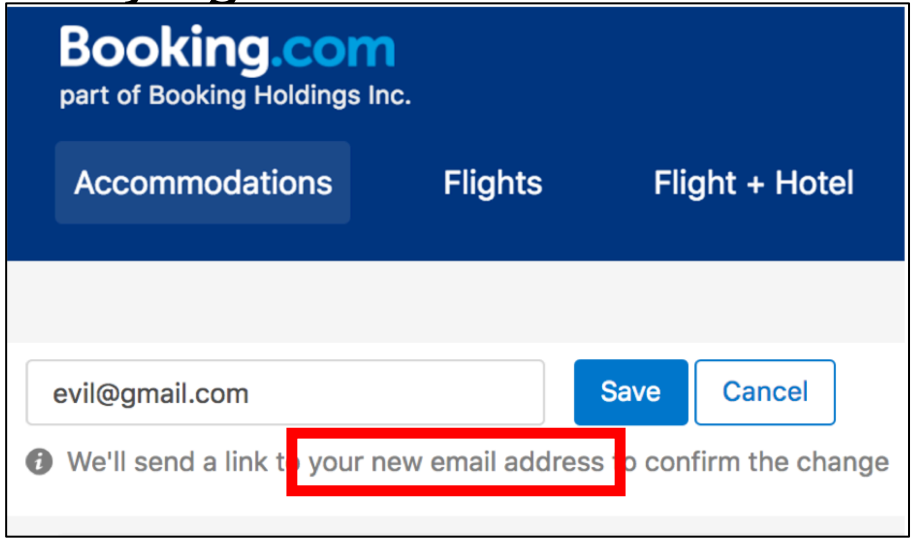
- HUD (Dating app)
  - Messages remain unread
- Uber
  - Real-time tracking
  - Past trips
  - Can even tip the driver :-)



Long-term Access (variation 1)

- Lines between SSO and local account management become blurry
  - Gain initial access over SSO, switch to email/password afterwards
  - Enables stealthy long-term access
- Email modification
  - 15 out of 29 **did not** require password for modifying emails



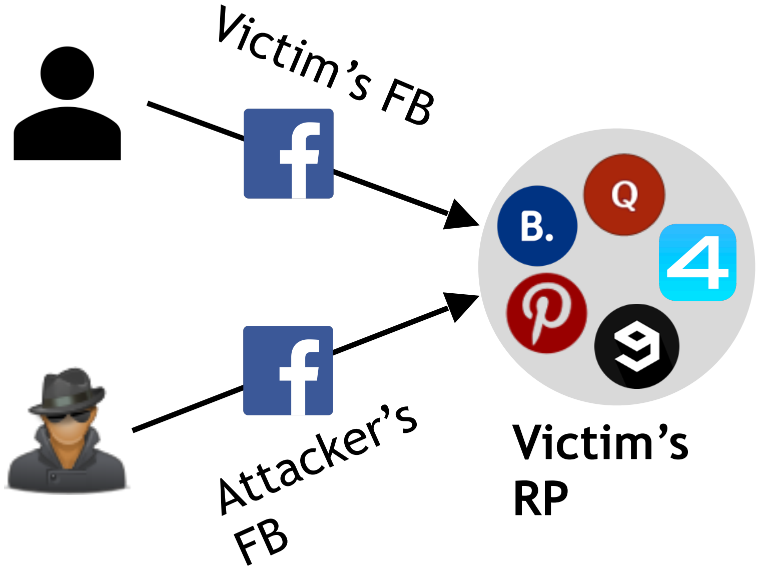


evil@gmail.com

We'll send a link to your new email address to confirm the change

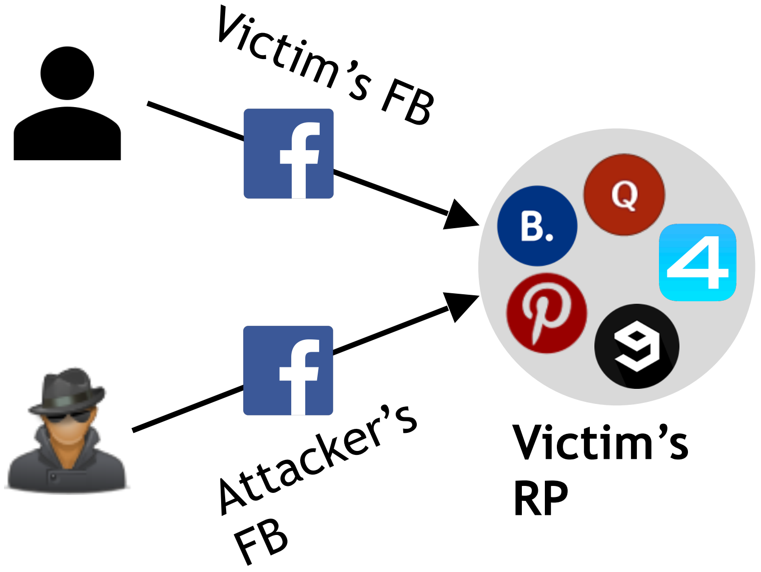
Long-term Access (variation 2)

- Account linking attack
  - 5 out of 29 are vulnerable
- Stealthy – victim never gets notified
- Exhaustive manual work for remediation

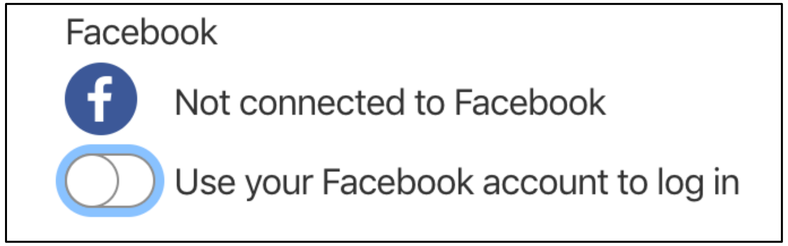


Long-term Access (variation 2)

- Account linking attack
  - 5 out of 29 are vulnerable
- Stealthy – victim never gets notified
- Exhaustive manual work for remediation



1



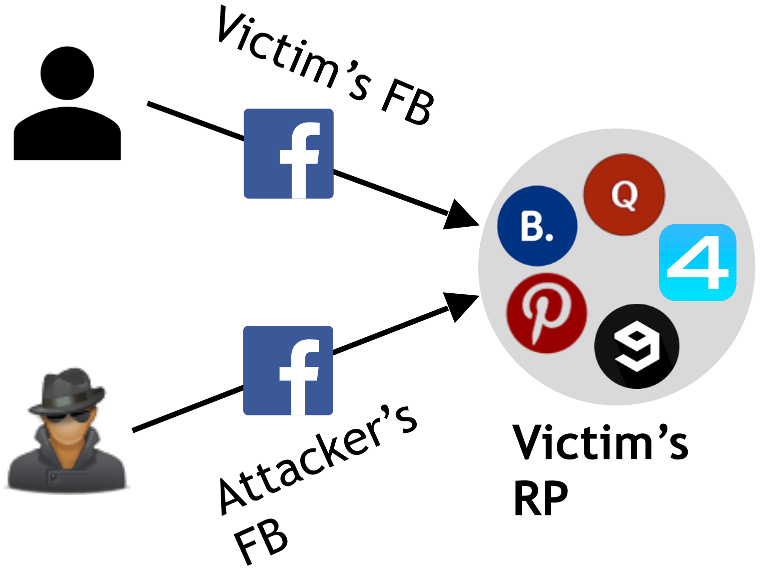
Facebook

Not connected to Facebook

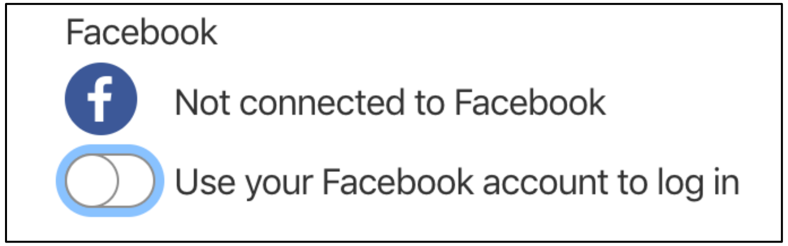
○ Use your Facebook account to log in

Long-term Access (variation 2)

- Account linking attack
  - 5 out of 29 are vulnerable
- Stealthy – victim never gets notified
- Exhaustive manual work for remediation



1

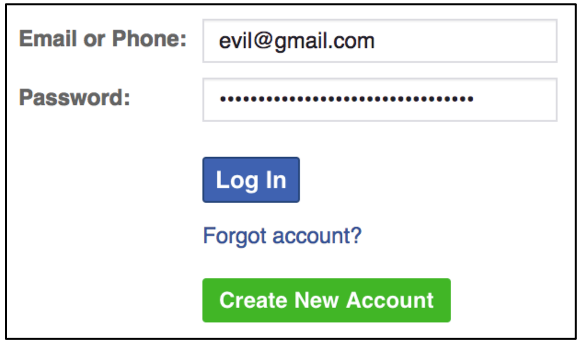


Facebook

Not connected to Facebook

Use your Facebook account to log in

2

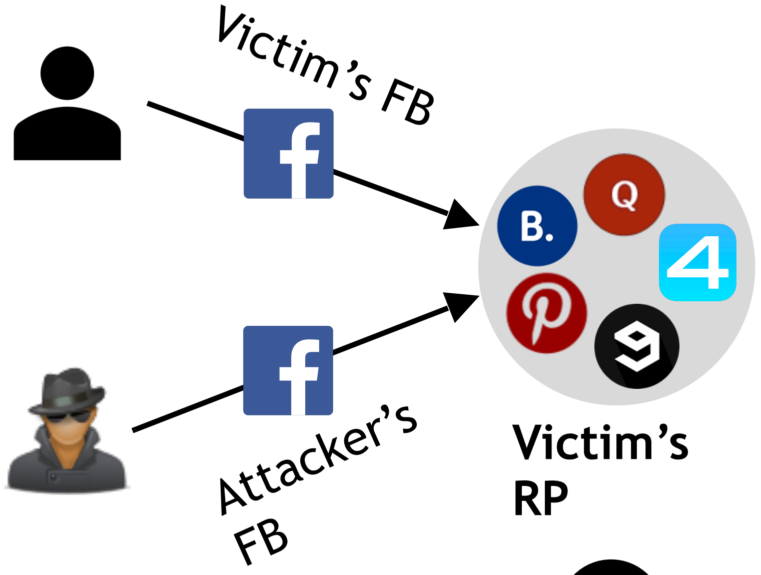


Email or Phone: evil@gmail.com

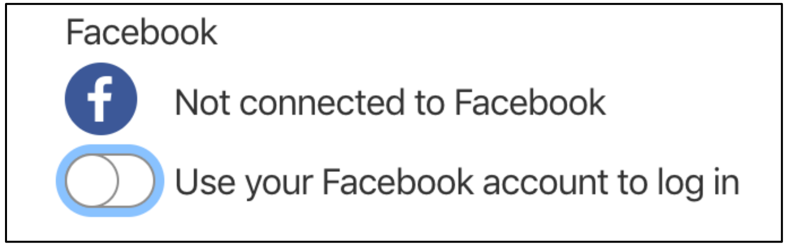
Password: ••••••••••••••••••••••••••••••••

Long-term Access (variation 2)

- Account linking attack
  - 5 out of 29 are vulnerable
- Stealthy – victim never gets notified
- Exhaustive manual work for remediation



1

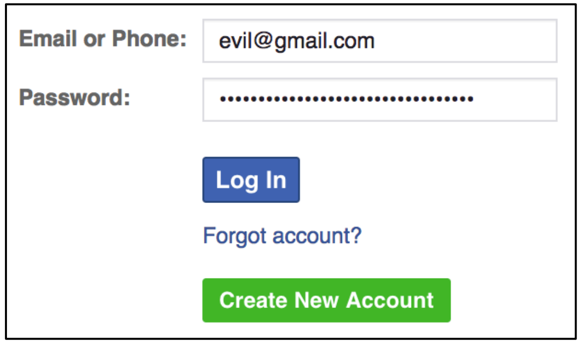


Facebook

Not connected to Facebook

Use your Facebook account to log in

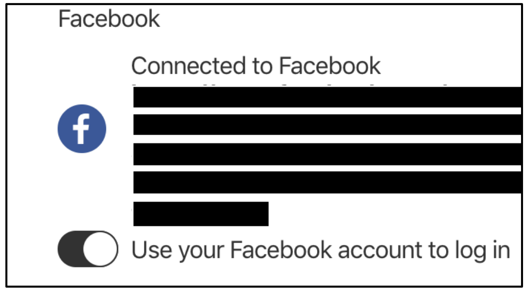
2



Email or Phone: evil@gmail.com

Password: ••••••••••••••••••••••••••••••••••

3



Facebook

Connected to Facebook

[redacted]

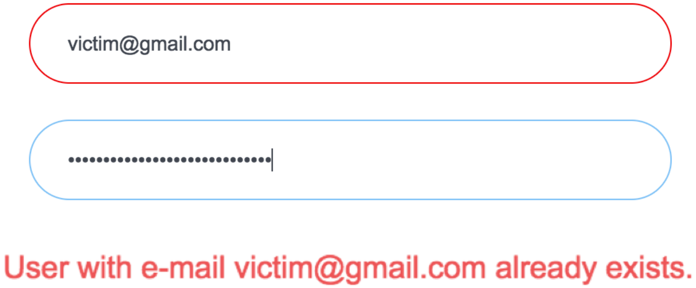
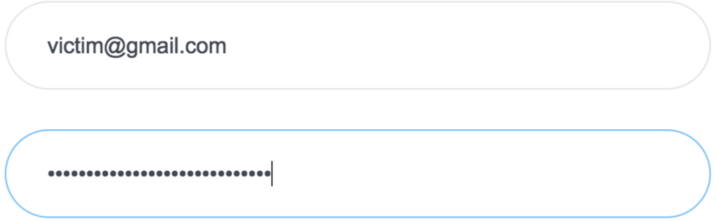
Use your Facebook account to log in

What if the victim doesn’t yet have an RP account?

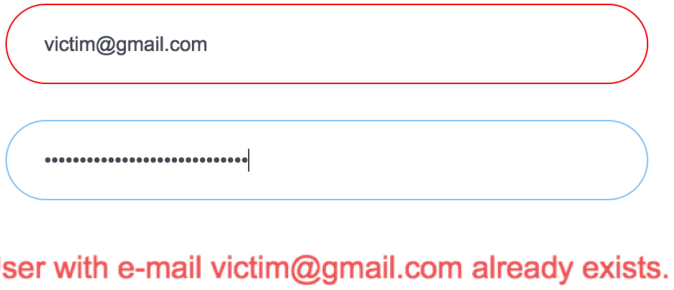
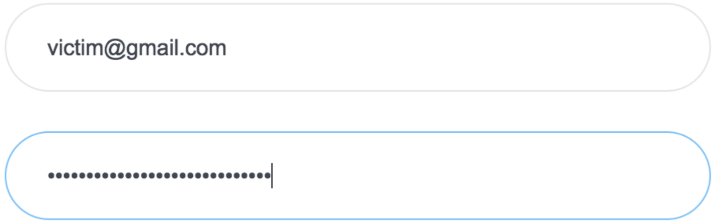
Preemptive Relying Party Account Takeover

Authentication Method	Account Already Exists	Account Doesn’t Exist
Traditional credential-based authentication		
Single Sign-On		

Preemptive Relying Party Account Takeover

Authentication Method	Account Already Exists	Account Doesn’t Exist
Traditional credential-based authentication	 victim@gmail.com •••••••••••••••••••••••••••••••• User with e-mail victim@gmail.com already exists.	 victim@gmail.com ••••••••••••••••••••••••••••••••
Single Sign-On		

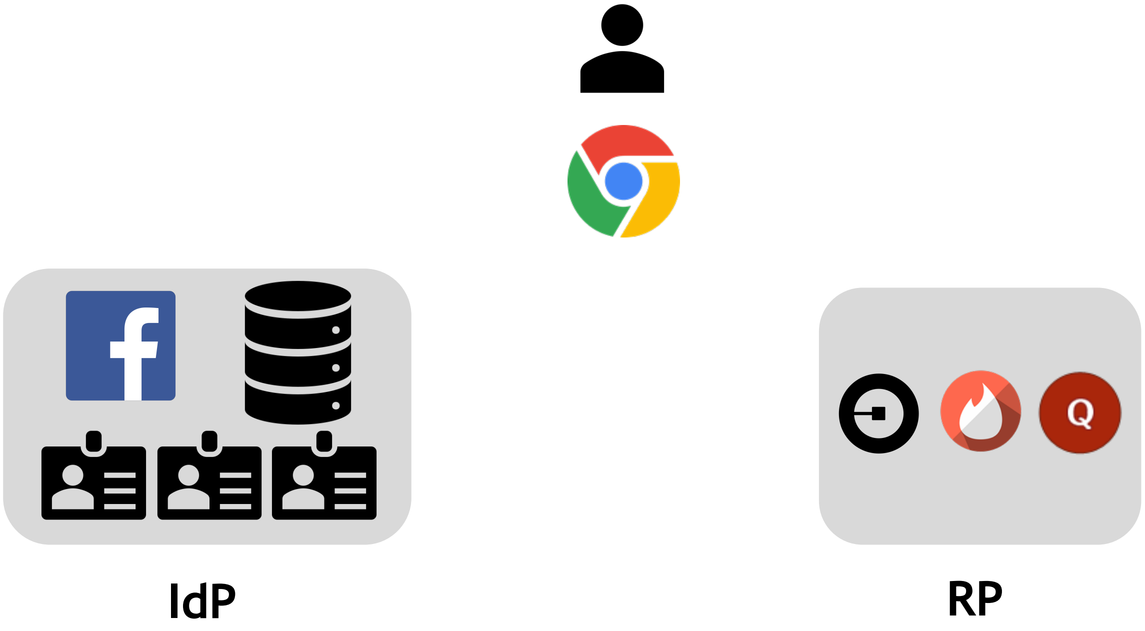
Preemptive Relying Party Account Takeover

Authentication Method	Account Already Exists	Account Doesn’t Exist
Traditional credential-based authentication	 victim@gmail.com •••••••••••••••••••••••••••••• User with e-mail victim@gmail.com already exists.	 victim@gmail.com ••••••••••••••••••••••••••••••
Single Sign-On	 Log in with Facebook (Login) Join with Facebook (Account Creation)	

Post-Compromise Remediation

- A two-link chain is created upon user authentication with SSO:
  - User and IdP
  - User and RP

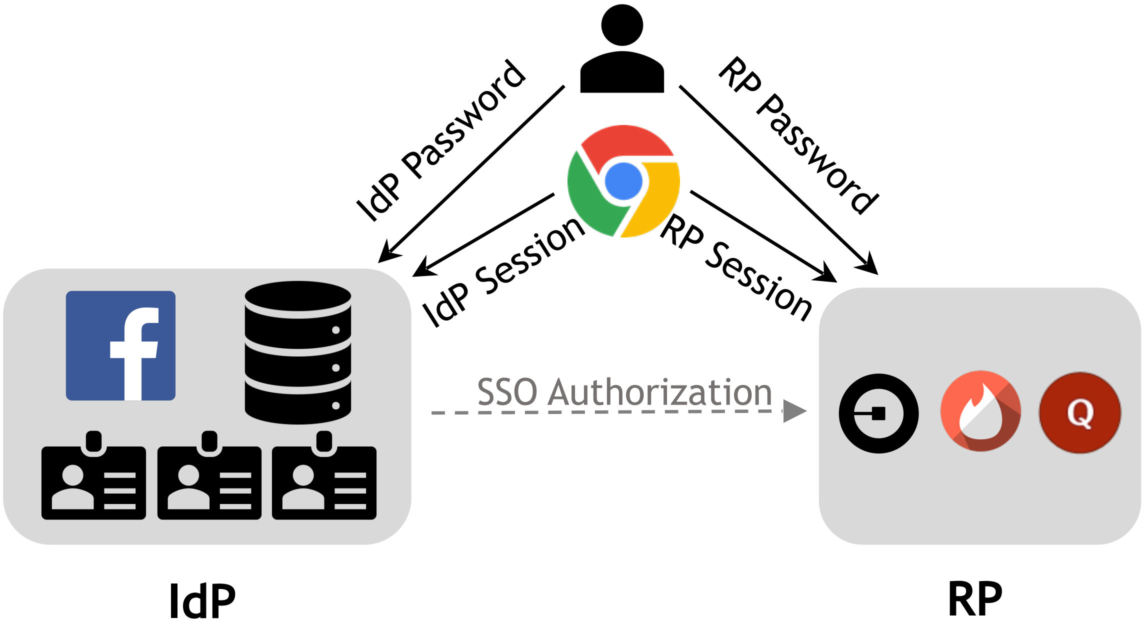
- What can victims do once they become aware of their account being hijacked?



Post-Compromise Remediation

- A two-link chain is created upon user authentication with SSO:
  - User and IdP
  - User and RP

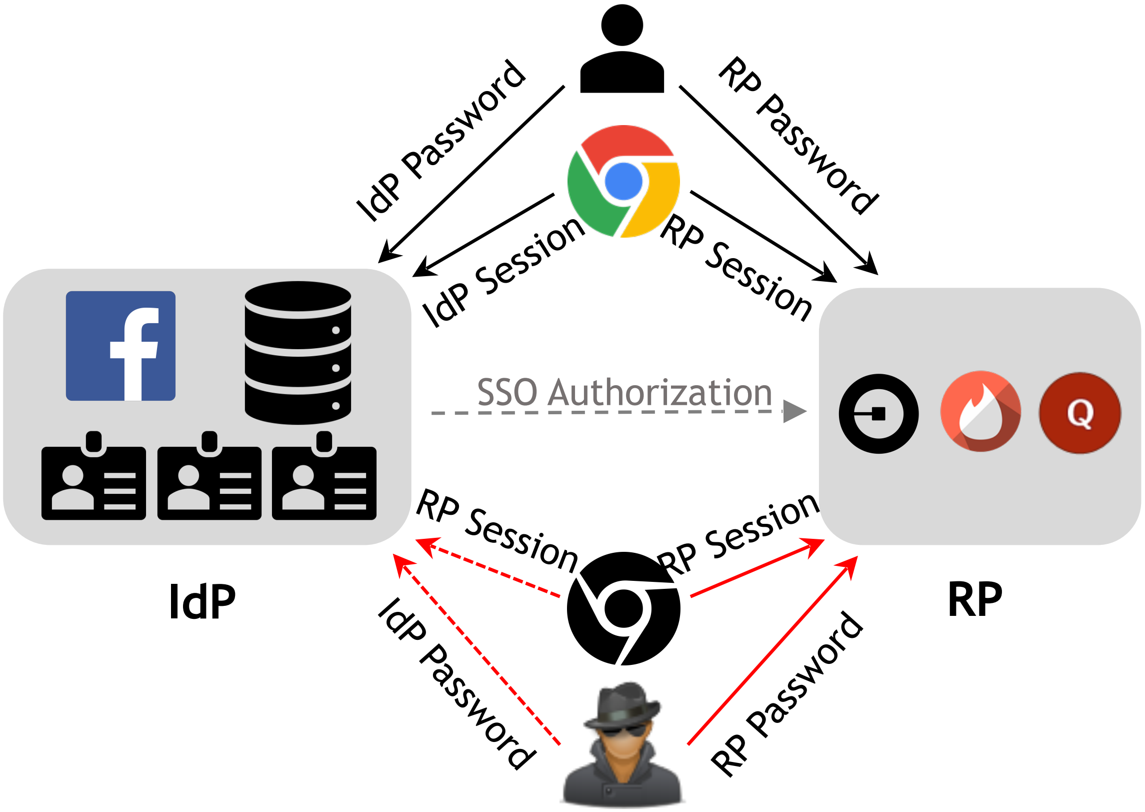
- What can victims do once they become aware of their account being hijacked?



Post-Compromise Remediation

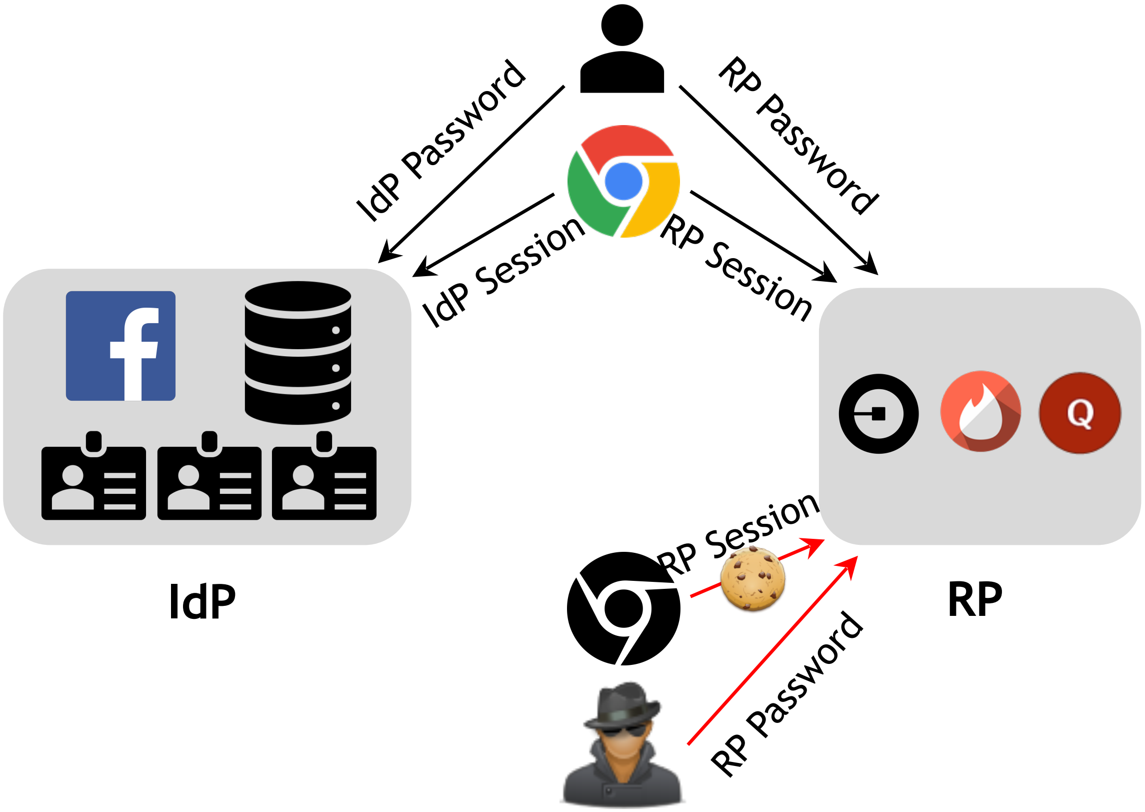
- A two-link chain is created upon user authentication with SSO:
  - User and IdP
  - User and RP

- What can victims do once they become aware of their account being hijacked?



Post-Compromise Remediation

- A two-link chain is created upon user authentication with SSO:
  - User and IdP
  - User and RP
- What can victims do once they become aware of their account being hijacked?



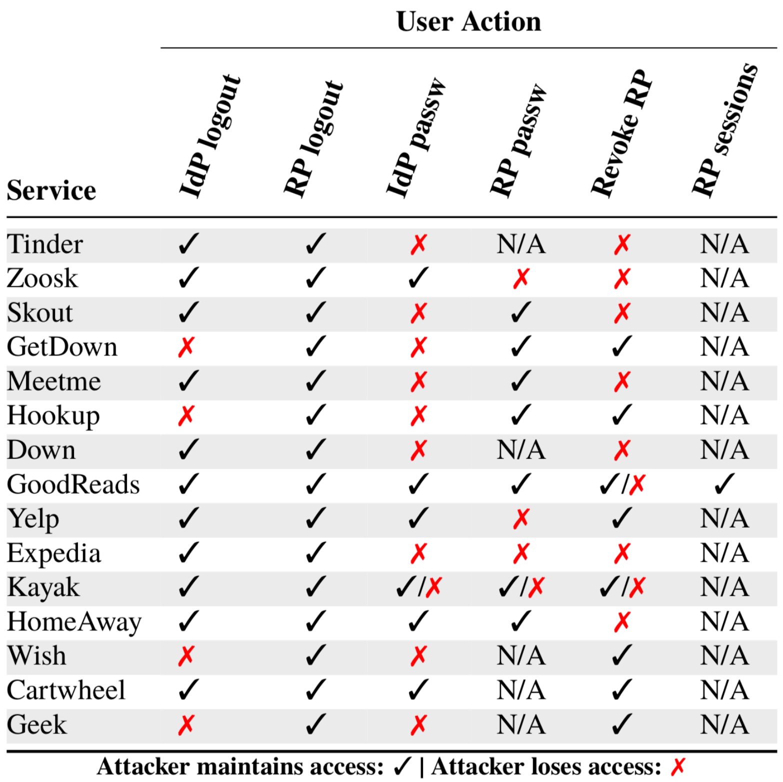
Post-Compromise Remediation

- *What session management options are available?*
- *How effective are they?*

- Possible remediation actions:
  - Logout from IdP
  - Logout from RP
  - Reset/change IdP password
  - Add/change RP password
  - Revoke RP access from IdP
  - Invalidate active RP sessions from RP
- Examined each action independently on 95 RPs

Post-Compromise Remediation

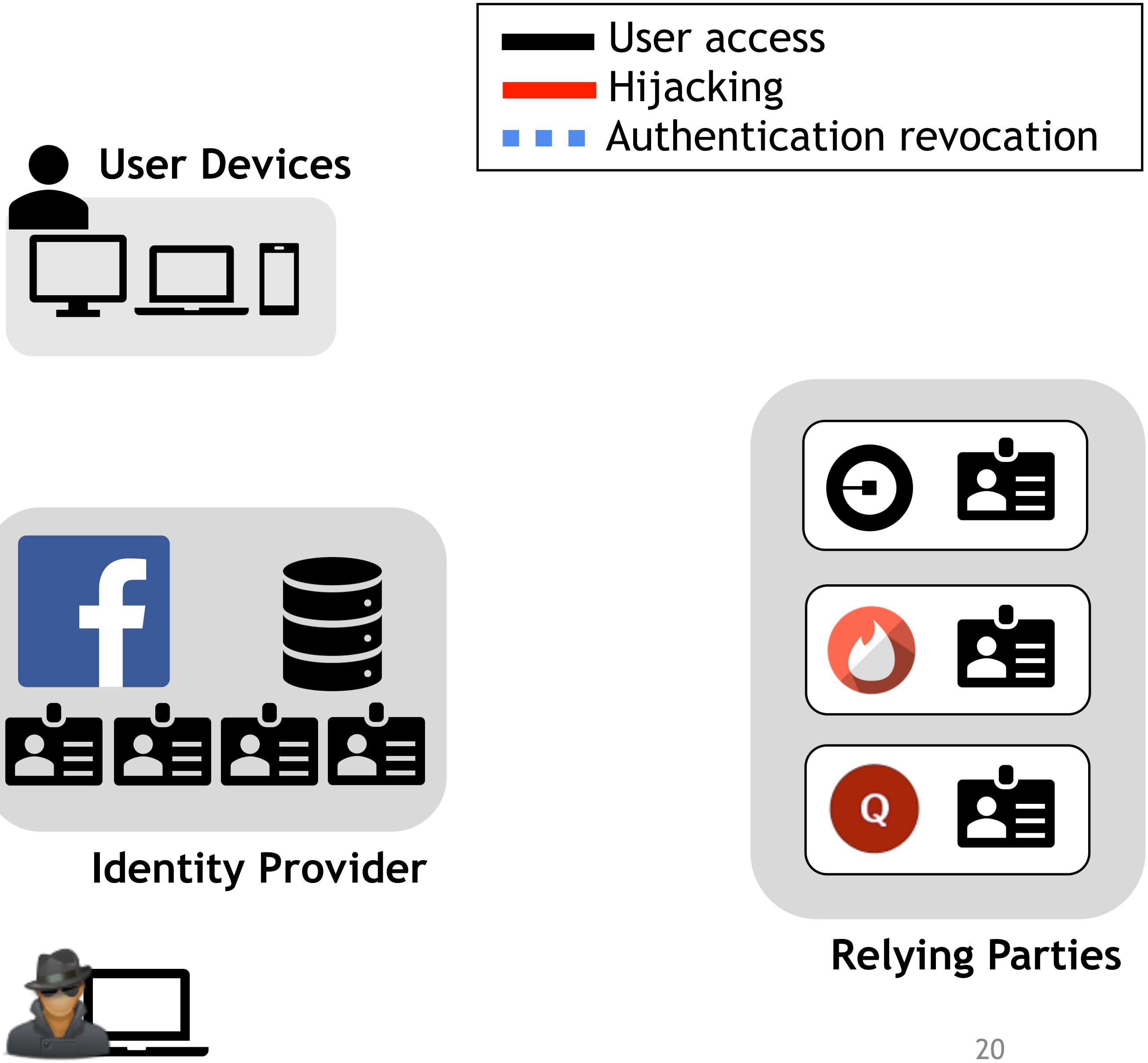
- No effective recovery action for **<u>74.7%</u>** RPs
- **<u>89.5%</u>** RPs **<u>do not</u>** offer session management
  - Complete remediation: revoking RP access and invalidating active sessions
- Until RP cookie expires
  - short-lived sessions in <u>only 5</u> Web RPs
- GoodReads:
  - revoke access only affects Web access
- Kayak:
  - partial read access always remains



	User Action					
Service	**IdP logout**	**RP logout**	**IdP passw**	**RP passw**	**Revoke RP**	**RP sessions**
Tinder	✓	✓	✗	N/A	✗	N/A
Zoosk	✓	✓	✓	✗	✗	N/A
Skout	✓	✓	✗	✓	✗	N/A
GetDown	✗	✓	✗	✓	✓	N/A
Meetme	✓	✓	✗	✓	✗	N/A
Hookup	✗	✓	✗	✓	✓	N/A
Down	✓	✓	✗	N/A	✗	N/A
GoodReads	✓	✓	✓	✓	✓/✗	✓
Yelp	✓	✓	✓	✗	✓	N/A
Expedia	✓	✓	✗	✗	✗	N/A
Kayak	✓	✓	✓/✗	✓/✗	✓/✗	N/A
HomeAway	✓	✓	✓	✓	✗	N/A
Wish	✗	✓	✗	N/A	✓	N/A
Cartwheel	✓	✓	✓	N/A	✓	N/A
Geek	✗	✓	✗	N/A	✓	N/A

Attacker maintains access: ✓ | Attacker loses access: ✗

Single Sign-Off



▬ User access
🟥 Hijacking
■ ■ ■ Authentication revocation

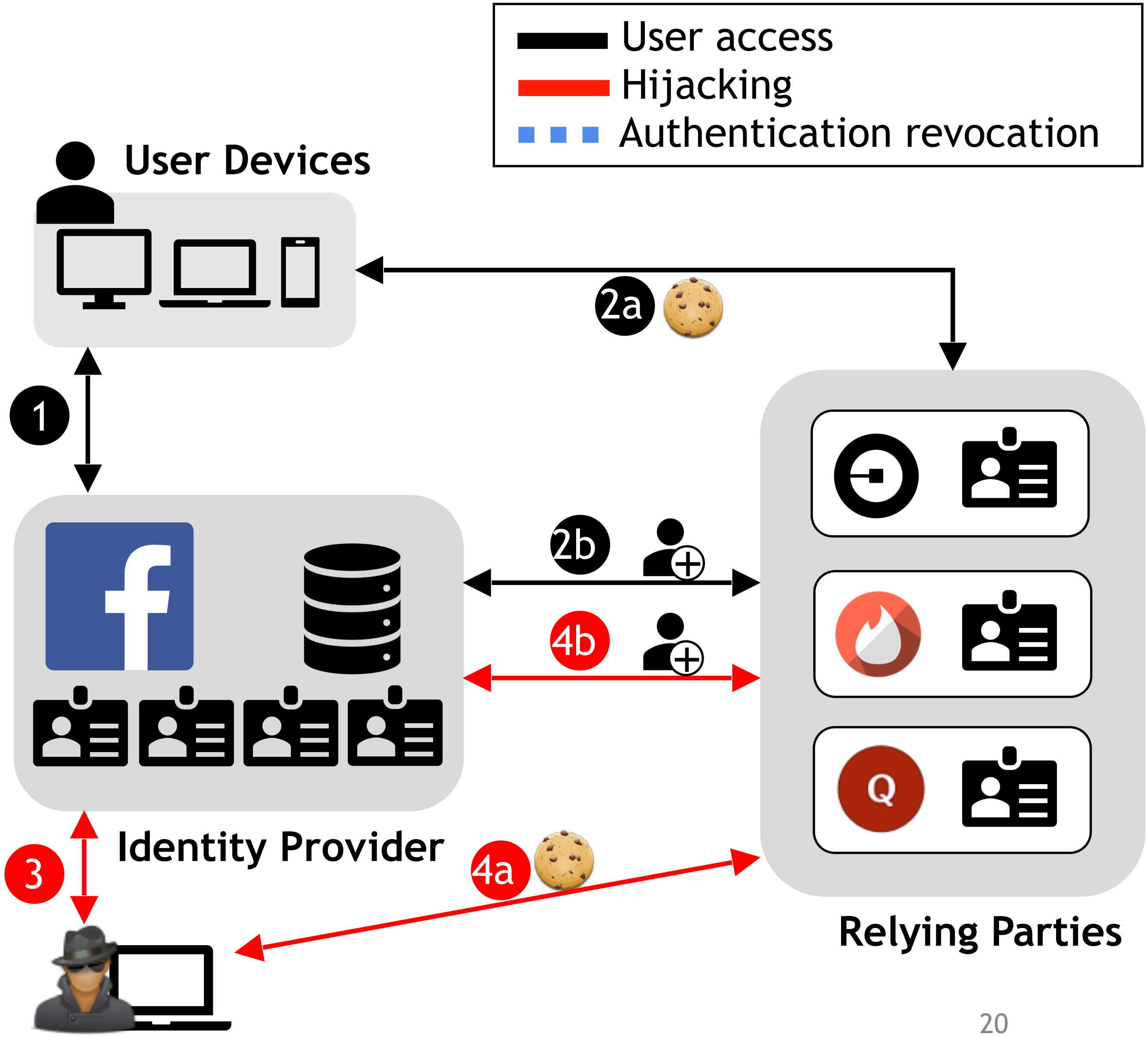
User Devices

Identity Provider

Relying Parties

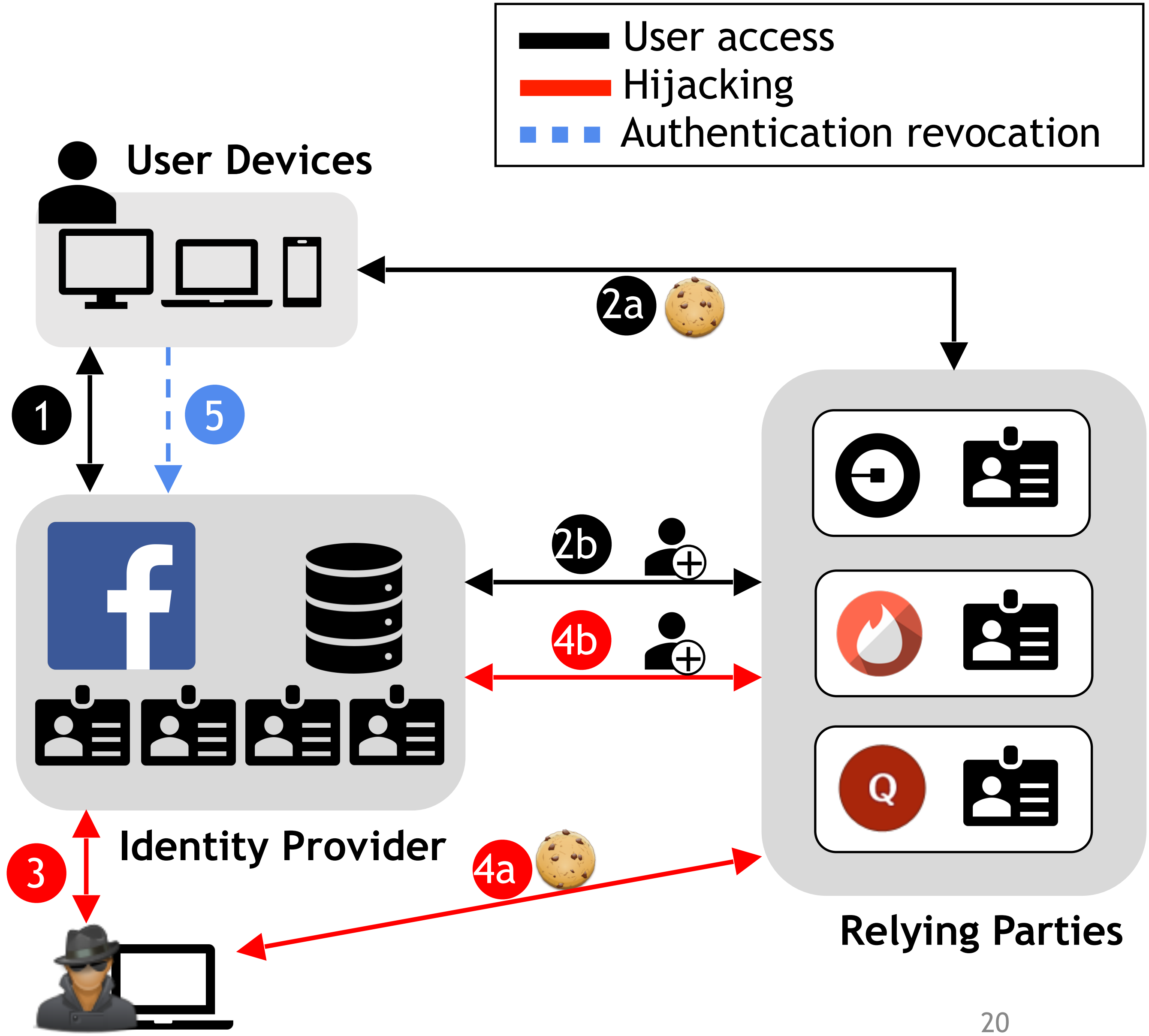
Single Sign-Off

- Steps 1 - 4 : IdP account compromise



Single Sign-Off

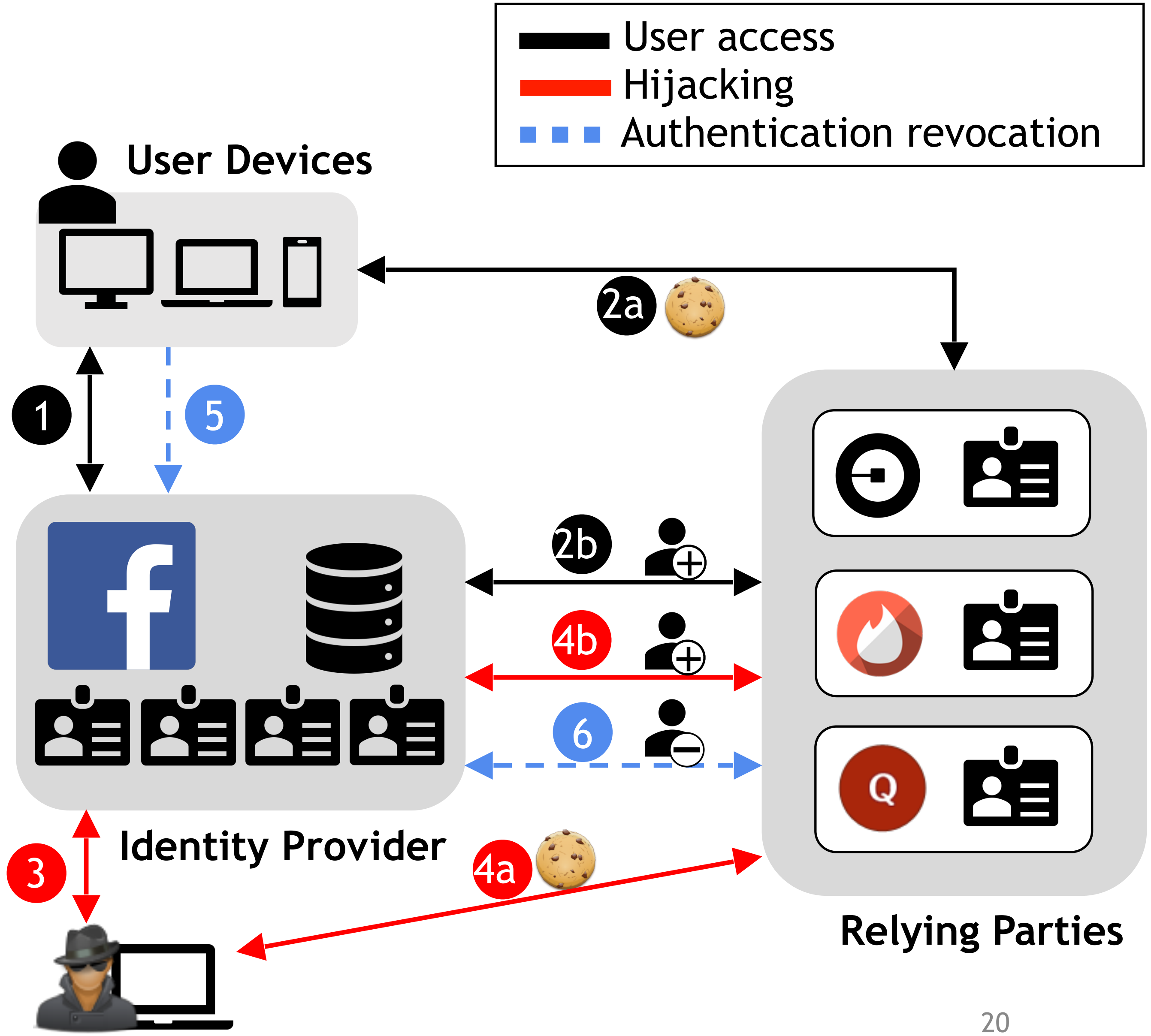
- Steps ❶ - ❹ : IdP account compromise



Single Sign-Off

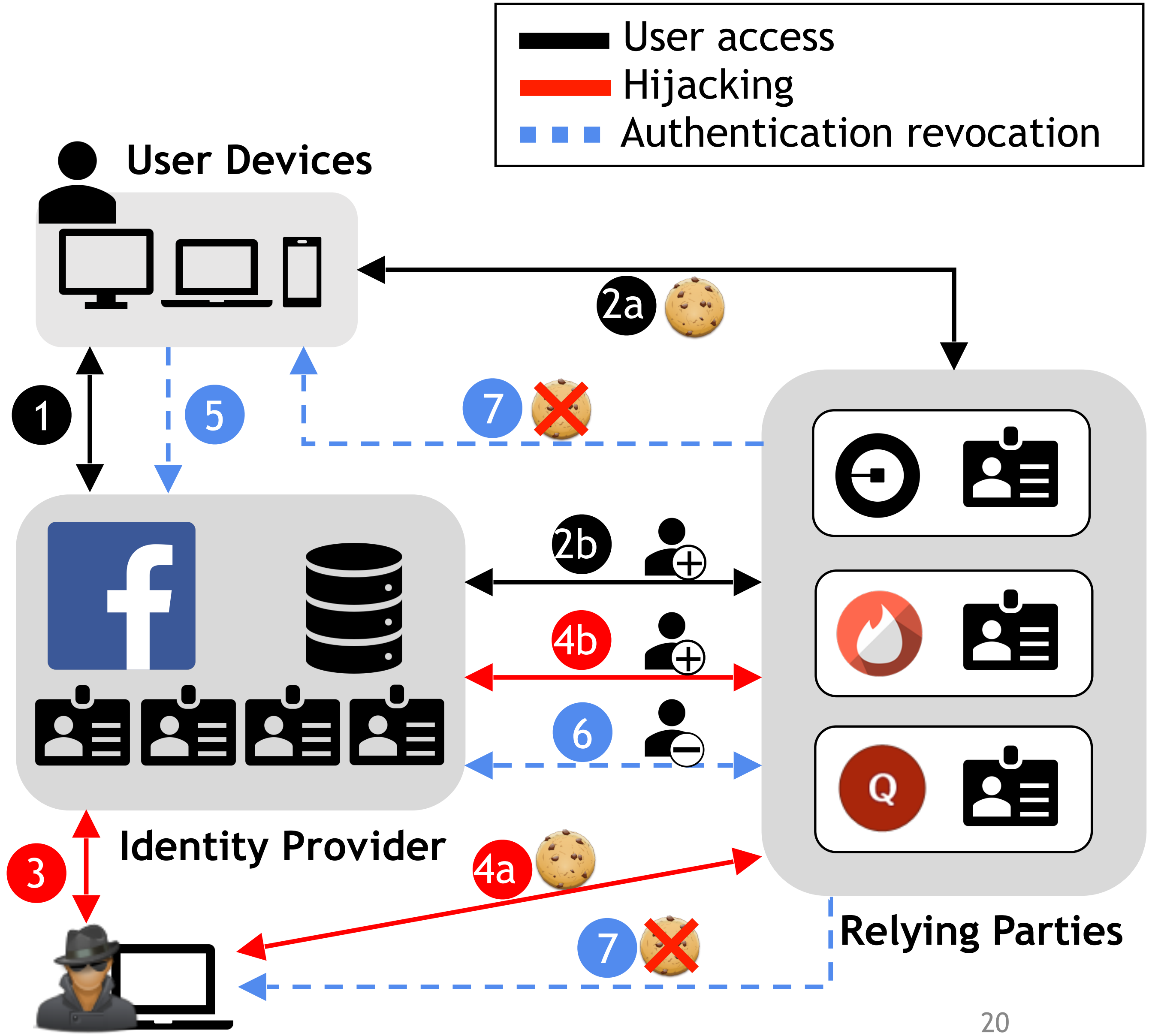
- Steps ❶ - ❹ : IdP account compromise

- Revoke all tokens and notify all RPs



Single Sign-Off

- Steps 1 - 4 : IdP account compromise
- Revoke all tokens and notify all RPs
- RP accounts should be frozen until the victim reauthenticates through SSO



Takeaways

- SSO magnifies the scale and persistence of attacks, and also enables novel attacks not feasible with traditional credential-based authentication.
- No options for remediating account compromise in most services. Due to SSO prevalence, remediation infeasible in practice.
- We propose a strict universal revocation scheme that addresses the attacks enabled by SSO.

Questions

- Please read the paper for all the missing details
- Feel free to contact me:
  - mghas2@uic.edu
- Dataset: http://cs.uic.edu/~sso-study