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

University of Illinois at Chicago

USENIX Security Symposium, August 2018
Single Sign-On

Continue with Facebook

Quora
A place to share knowledge and better understand the world

Continue with Google
Continue with Facebook

Continue with Facebook

Discover more with Pinterest
Find new ideas to try

Email
Create a password
Continue

First time on VK?
Sign up for VK

Your first name
Your last name
Date of birth
Day, Month, Year

Your gender
Female, Male

Continue registration

GET STARTED
By clicking log in, you agree with our Terms, Privacy Policy and Cookies Policy.

LOG IN WITH FACEBOOK

LOG IN WITH PHONE NUMBER
Single Sing-On Authentication Flow

Relying Party (RP or client)

End User

Identity Provider (IdP or OP)
Single Sing-On Authentication Flow

End User

Authorization Endpoint

Identity Provider (IdP or OP)

Relying Party (RP or client)

GET STARTED

LOG IN WITH FACEBOOK

LOG IN WITH PHONE NUMBER

LOGIN TO RP

HTTP 302

Authorization Endpoint

Identity Provider (IdP or OP)
Single Sing-On Authentication Flow

End User

Login to RP

HTTP 302

Identity Provider
(IdP or OP)

Relying Party
(RP or client)

Is User Agent logged in?

Authorization Endpoint
Single Sing-On Authentication Flow

Relying Party (RP or client)

End User

Identity Provider (IdP or OP)

Login to RP

HTTP 302

Authorization Endpoint

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

Continue as Me
Single Sing-On Authentication Flow

Relying Party (RP or client) → End User

- Login to RP
- HTTP 302
- Authorization code

Identity Provider (IdP or OP) → Authorization Endpoint

- Authorization code
- Authorization Endpoint
Single Sing-On Authentication Flow

1. **Identity Provider (IdP or OP)**
   - Authorization Endpoint
   - Token Endpoint

2. **Relying Party (RP or client)**
   - Login to RP
   - HTTP 302
   - Authorization code

3. **End User**
   - Retrieve Tokens
   - HTTP 302
   - Authorization code
Single Sing-On Authentication Flow

Relying Party (RP or client)

End User
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

<table>
<thead>
<tr>
<th>Good</th>
<th>Bad</th>
</tr>
</thead>
</table>
| • Ease of use  
• Integrated experience  
• Eliminates burden of multiple account creation | • Attackers can leverage the same functionality to increase access coverage even when it is implemented correctly |

![Social Media Logos](image1.png)  
![Social Media Logos](image2.png)
Single Sign-On, the Good, the Bad and the Ugly

<table>
<thead>
<tr>
<th>Good 🌈</th>
<th>Bad 😞</th>
<th>Ugly 😞</th>
</tr>
</thead>
</table>
| • Ease of use  
• Integrated experience  
• Eliminates burden of multiple account creation | • Attackers can leverage the same functionality to increase access coverage even when it is implemented correctly | • Very hard/impossible to recover from IdP account compromise |

![Social Media Icons](image1.png)

![Social Media Icons](image2.png)

![Social Media Icons](image3.png)
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 Account Takeover

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

![Image of a phone with a map and HUD app interface]
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
Long-term Access (variation 2)

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

Victim’s RP
Attacker’s FB

Victim’s FB

Facebook

LinkedIn

YouTube

Twitter

Bing

Quora

Reddit

4chan
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
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: 
     - Log In
     - Forgot account?
     - Create New Account

3. Facebook
   - Connected to Facebook
   - Use your Facebook account to log in
What if the victim doesn’t yet have an RP account?
## Preemptive Relying Party Account Takeover

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Account Already Exists</th>
<th>Account Doesn’t Exist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional credential-based authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single Sign-On</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Preemptive Relying Party Account Takeover

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Account Already Exists</th>
<th>Account Doesn’t Exist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional credential-based</td>
<td><img src="image1" alt="Victim email and password fields with warning" /></td>
<td><img src="image2" alt="Victim email and password fields" /></td>
</tr>
<tr>
<td>authentication</td>
<td><strong>User with e-mail <a href="mailto:victim@gmail.com">victim@gmail.com</a> already exists.</strong></td>
<td></td>
</tr>
<tr>
<td>Single Sign-On</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Preemptive Relying Party Account Takeover

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Account Already Exists</th>
<th>Account Doesn’t Exist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional credential-based authentication</td>
<td><img src="image" alt="Username and Password Form" /></td>
<td><img src="image" alt="Username and Password Form" /></td>
</tr>
<tr>
<td></td>
<td>User with e-mail <a href="mailto:victim@gmail.com">victim@gmail.com</a> already exists.</td>
<td></td>
</tr>
<tr>
<td>Single Sign-On</td>
<td><img src="image" alt="Login with Facebook Button" /> (Login)</td>
<td><img src="image" alt="Account Creation with Facebook Button" /> (Account Creation)</td>
</tr>
</tbody>
</table>
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?

SSO Authorization
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 **74.7%** RPs
• **89.5%** RPs **do not** offer session management
  • Complete remediation: revoking RP access and invalidating active sessions
• Until RP cookie expires
  • short-lived sessions in **only 5** Web RPs
• **GoodReads:**
  • revoke access only affects Web access
• **Kayak:**
  • partial read access always remains
Single Sign-Off

- User Devices
- Identity Provider
- Relying Parties

- User access
- Hijacking
- Authentication revocation
Single Sign-Off

• Steps 1 - 4: IdP account compromise
Single Sign-Off

- Steps 1 - 4: IdP account compromise

User Devices

Identity Provider

Relying Parties

User access
Hijacking
Authentication revocation

Steps:
1. IdP account compromise
2a. User access
2b. Hijacking
3. Identity Provider
4a. Authentication revocation
4b. Relying Parties
Single Sign-Off

- Steps 1 - 4: 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 reauthorizes 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