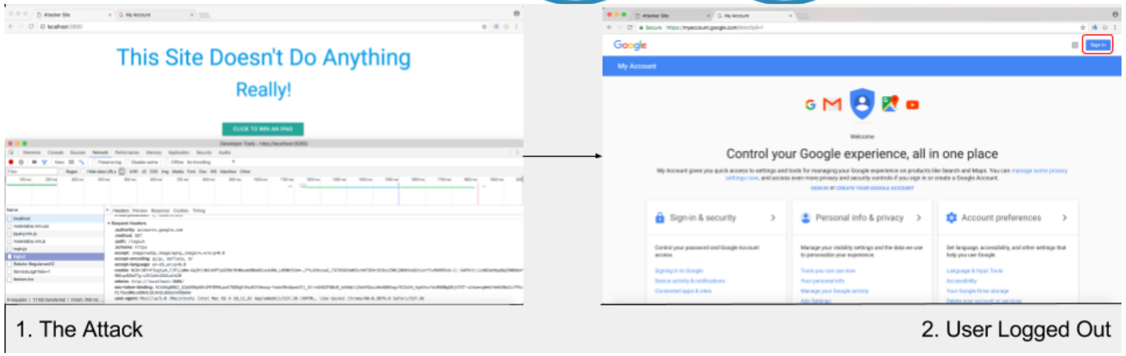
Modeling and Mitigating Cross Origin Attacks on FIM Based Services Using CORP

Aim

- To see if FIM is vulnerable to cross origin attacks through both modelling and experimentation.
- To understand and use CORP(a browser security policy) to mitigate these attacks through the browser.

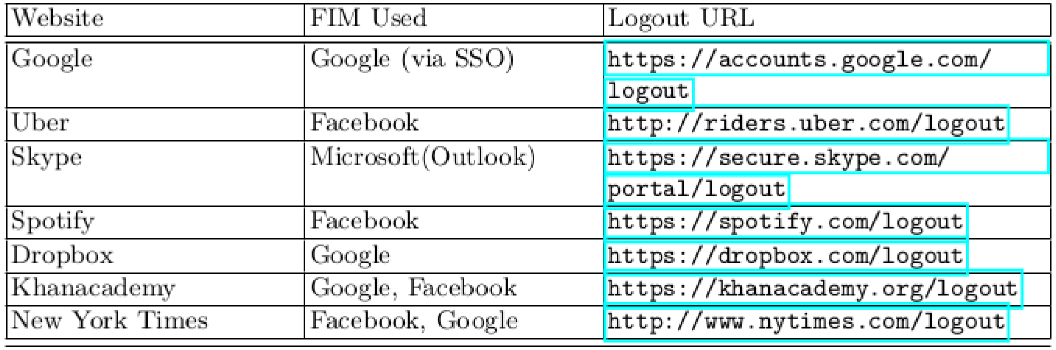


1. The Attack

2. User Logged Out

What We Did

- Created two models: Pre-CORP and Post-CORP, which were specifically defined on systems which use FIM and are affected by cross origin attacks.
- Mitigated the CORA in the Post-CORP model using CORP policy, in Alloy.
- Experimented with two main types of attacks: login detection and autologout.
- Succcesfully mitigated the CORA using CORP in the Chromium browser.



Website	FIM Used	Logout URL
Google	Google (via SSO)	https://accounts.google.com/logout
Uber	Facebook	http://riders.uber.com/logout
Skype	Microsoft(Outlook)	https://secure.skype.com/portal/logout
Spotify	Facebook	https://spotify.com/logout
Dropbox	Google	https://dropbox.com/logout
Khanacademy	Google, Facebook	https://khanacademy.org/logout
New York Times	Facebook, Google	http://www.nytimes.com/logout

Table 1. List of popular Websites, the FIM they are using and their Vulnerable Logout end-point

Conclusion

- FIM is not an all-encompassing security solution as it is vulnerable to CORA.
- CORP as a browser security policy would increase safety for users.

Software Engg Research Center

Akash Agrawall
Shubh Maheshwari
Projit Bandyopadhyay
Venkatesh Choppella