Modeling and Mitigation of Cross Origin Attacks on FIM Based Services Using CORP

AIM

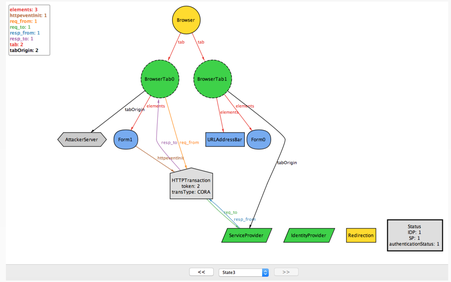
To study the impact of Cross Origin Attacks on systems using Federated Identity Management to handle authentication.
To create models representing CORP's interaction with web browsers and to identifiy current risks.
To test CORP's implementation and mitigate cross origin attacks using it.

INTRODUCTION

With ever-increasing cyber threats we look for ways to improve the security of our systems. FIM is a system by which authentication is handled by 3rd parties, thus increasing security. However even when FIM protocols are implemented, systems may not necessarily be completely secure. Current browser secuity policies like Same Origin Policy(SOP) still have many issues and lack complete coverage. Thus through modeling and experimentation we must test how systems using FIM react to cross origin attacks.
Cross Origin Reqest Policy(CORP), a proposed browser security policy which aims to bridge the gaps in current policies, may be used to mitigate them.

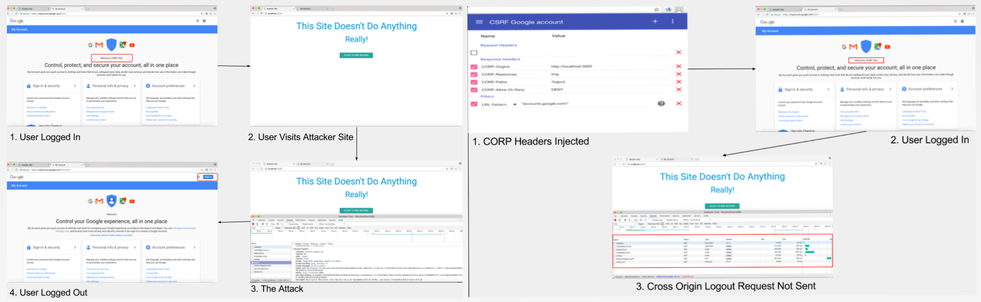
MODELING

We used alloy to show cross origin attacks on a finite state model.



EXPERIMENTATION

We conducted cross-timing and autologout attacks on sites which used FIM protocols. We also attempted ot mitigate these attacks using CORP



The Logout Attack

The Logout Attack Mitigation

RESULTS

We modeled CORP and its interaction with the browser and used the alloy model to show risks of cross origin attacks. Experimentation on systems using FIM yielded the fact that they too are vulnerable to these attacks. However they are safe if in the presence of CORP.

CONCLUSIONS

FIM is not an all-encompassing security system. Current browser security policies have many defects which causes services to be vulnerable to cross origin attacks even if they have FIM. Implementing a CORP browser security policies protects the user through the browser from attacks like cross-site timing, csrf, etc.

Software Engg Research Center

Akash Agrawall
Shubh Maheshwari
Projit Bandyopadhyay
Venkatesh Choppella