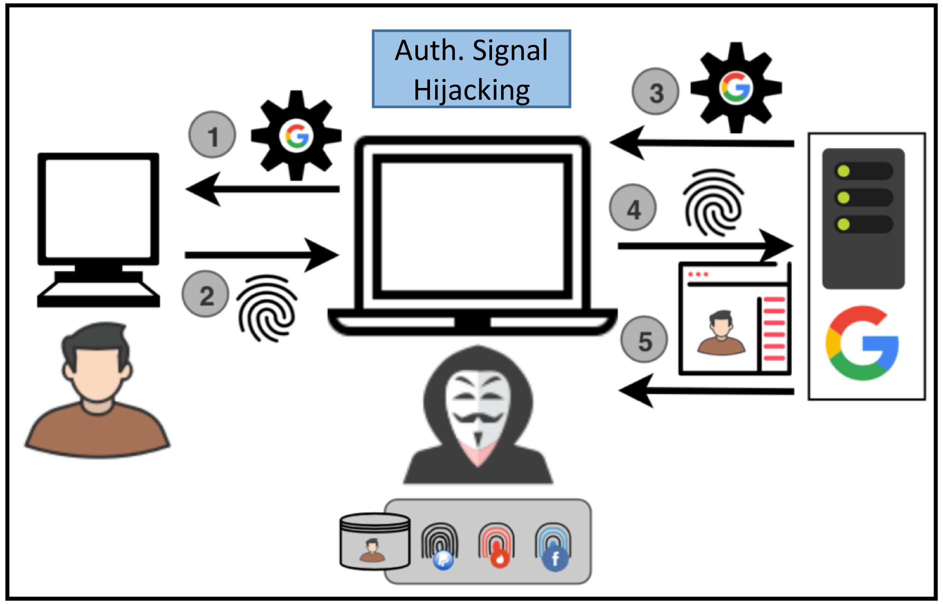
SaTC: CORE: Small: Black-Box Flaw Discovery in Web Authentication and Authorization Mechanisms

UIC UNIVERSITY OF ILLINOIS AT CHICAGO

Challenge

- Authentication and authorization mechanisms lie at the core of high-value and critical web services and applications. They are frequently the target of both cyber-criminals and nation-state adversaries.
- The complexity and scale of modern web services, coupled with the ad-hoc nature of web development and the fragmented structure of development teams, leads to incomplete or ineffective internal security testing.
- Deployment of proprietary mechanisms that haven't been audited by the security community.



Solution

- Develop a modular, website-agnostic, auditing framework for the automated black-box analysis of authentication and authorization mechanisms in modern web services and applications.
- Explore how auxiliary authentication factors are leveraged by modern authentication systems, and how attackers can bypass defenses by replicating them.
- Develop novel systems for detecting the lack of security-guideline compliance in modern authentication environments and investigate the feasibility of authentication mechanisms that employ replay-resistant auxiliary signals.

Broader Impact

- Identify existing flaws in web services that expose users, organizations, and government employees to attacks.
- Release software prototypes to streamline the automation of authentication-related auditing and to help practitioners and researchers with the detection of flaws or security-guideline violations in modern web apps.

Scientific Impact

- Advance the community's understanding of the pitfalls in emerging web practices in authentication, authorization, and account session management.
- Differential analysis for automated, large-scale auditing for detecting authentication flaws and authorization bugs that leak private information.
- Investigation of a novel class of attacks against authentication mechanisms and bot-prevention systems that rely on auxiliary authentication signals.
- Exploration and design of robust authentication mechanisms to enhance the protection of user accounts.

Award Number: 1934597 (2019-2022)

Institution: University of Illinois at Chicago
Jason Polakis (polakis@uic.edu)