CICI: UCSS: Towards Secure and Usable Push Notification Authentication for Collaborative Scientific Infrastructures

Nitesh Saxena, Texas A&M University, College Station, USA

The goal of the project is to enhance the security of push-based and related authentication systems in science infrastructures (e.g., Just-Tap-2FA) by addressing fundamental design vulnerabilities while preserving usability, research questions being:

1. Are existing methods secure and how we can redesign them for better security?
2. Are users able to complete the authentication process successfully without assistance?
3. Do users find the proposed authentication methods more user-friendly than existing solutions?
4. Which authentication method (among those that we have proposed) result in improved security and usability?

Research Challenges

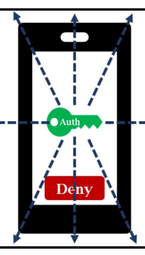
- Solutions must provide strong security against concurrent and ambiguous authentication attempts without relying on user vigilance or attention to multiple notifications.
- Solutions must preserve low-effort, fast interactions without cognitive burden, and ensure clear, distinguishable authentication feedback for correct session association.
- Solutions must be modular and compatible with real-world constraints, enabling seamless integration across existing scientific cyberinfrastructure and its associated devices, platforms, and accessibility settings.

Broader Impact

- Investigating security of widely deployed 2FA schemes
  - Investigating security issues in widely used push authentication systems (e.g., universities, government like NSF, and private organizations) and communicating findings through peer-reviewed publications.
- Inclusive authentication for public use in cyberinfrastructure
  - Developing usable and secure authentication system for public use.
- Collaboration with Industry (e.g., Cisco, Google)
- Student mentoring in Areas of National Importance
- Curriculum Enhancement & Inclusive Outreach
  - Offer advanced coursework in secure authentication while engaging minority and high school students through inclusive outreach

Security Investigation of Real-world (scientific infrastructure) Push Notification Authentication Systems

In depth Security & Usability Investigation in the Lab



Design and Implementation of Secure Push-based Authentication Method

<u>Security Investigation via Systemic Analysis</u>

- Measure effectiveness of designed attacks
- Investigate important insights on systemic's behavior on attack's response.
- Evaluate detectability of attack entry points through user's response

<u>Authentication Clarity & Effectiveness Through Systemic Analysis</u>

- Evaluate how well methods communicate authentication steps and support successful completion
- Compare ease of understanding with existing authentication
- Analyze effectiveness across all proposed authentication methods

Intellectual Merits

- **Investigate Security Challenges in real-world Push Notification Authentication Deployments** (AsiaCCS'21, Mobicom'23, WWW'25, TMC'25)
- **Design and Implementation of New Push-based Authentication Methods** (Euro S&P'21)
- **Rigorous Security and Usability Studies in Lab Settings** (Euro S&P'21, Mobicom'23, AsiaCCS'21, ACM CCS'24)

Notable Publications

- Countering Concurrent Login Attacks in "Just Tap" Push-based Authentication: A Redesign and Usability Evaluations [Prakash et al.] (**Euro S&P 2021**)
- Bypassing Push-based Second Factor and Passwordless Authentication with Human-Indistinguishable Notifications [Jubur et al.] (**AsiaCCS 2021**)
- Breaking Mobile Notification-based Authentication with Concurrent Attacks Outside of Mobile Devices [Mahdad et al.] (**Mobicom 2023**)
- SoK: A Comprehensive Evaluation of 2FA-based Schemes in the Face of Active Concurrent Attacks from User Terminal [Mahdad et al.] (**WiSec 2023**)
- Breaching Security Keys without Root: FIDO2 Deception Attacks via Overlays exploiting Limited Display Authenticators [Mahdad et al.] (**ACM CCS 2024**)
- Usability and Security Analysis of the Compare-and-Confirm Method in Mobile Push-Based Two-Factor Authentication [Jubur et al.] (**IEEE MC 2025**)
- Broken Access: On the Challenges of Screen Reader Assisted Two-Factor and Passwordless Authentication [Akanda et al.] (**WWW 2025**)
- An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools [Jubur et al.] (**ACM Computing Surveys 2025**)
- Comparing a Store-less Password Manager with Traditional Password-Only Authentication [Jubur et al.] (**IEEE Internet Computing 2026**)