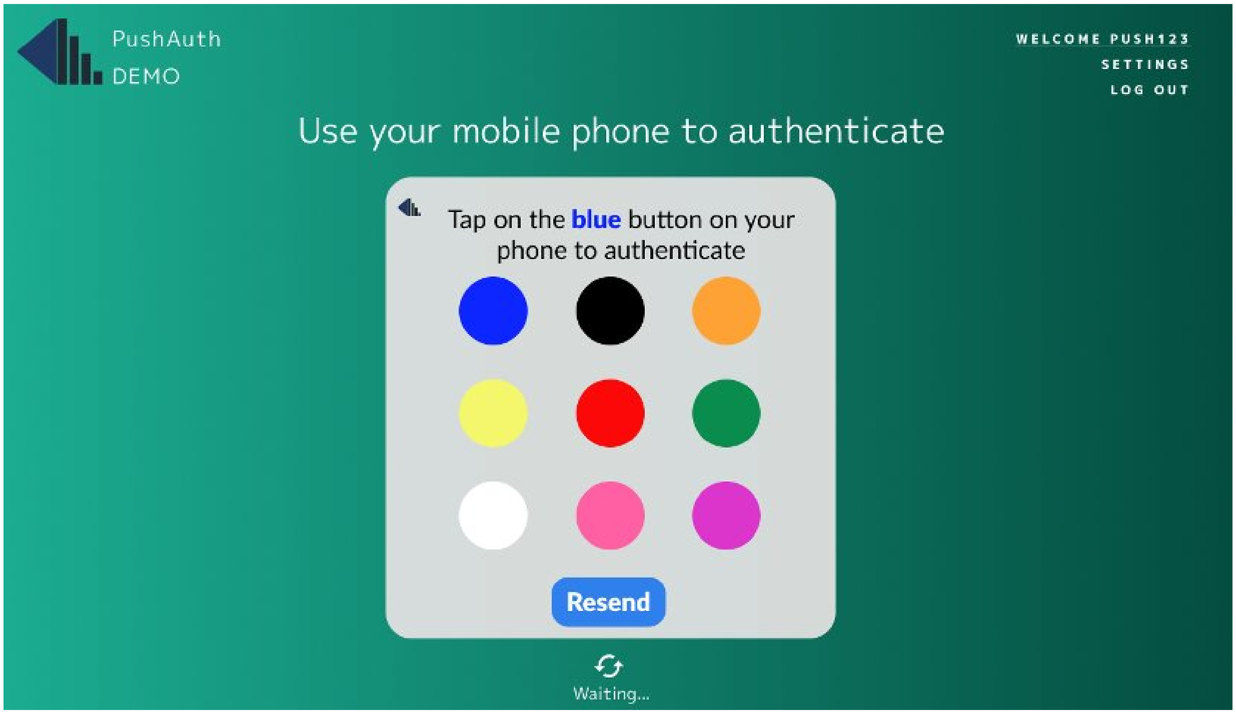
TechXplore

# New methods could improve security of two-factor authentication systems

April 14 2022, by Stephanie Jones



Use your mobile phone to authenticate

Tap on the **blue** button on your phone to authenticate

One of the interactions the researchers designed would require users to press the correct colored button to approve a login attempt. Credit: Nitesh Saxena, Texas A&M Engineering

As an extra layer of security, several online services have adopted push notification-based two-factor authentication systems, whereby users must approve login attempts through a mobile device. In current authentication systems, especially the "tap to approve" approach, there is no explicit link that indicates correspondence between the user's browser session and the notification they receive on their device. This vulnerability can be exploited by an attacker.

To address this issue, a team of researchers that includes Dr. Nitesh Saxena, professor in the Department of Computer Science and Engineering at Texas A&M University, has designed new, easy-to-use methods to counter the vulnerabilities in push notification-based two-factor authentication systems.

"The mechanisms we designed have a similar usability to the original push notification-based authentication method, but they improve security against concurrent login attacks," said Saxena. "If a user receives two notifications, the notification that corresponds to the browser's session of the attacker will differ. Therefore, the user should be able to detect that something is amiss and not accept the wrong notification."

The team's paper describing the research was published in the proceedings from the 2021 Institute of Electrical and Electronics Engineers' European Symposium on Security and Privacy (EuroS&P).

Push notifications are clickable pop-up messages sent directly to a user's mobile or desktop device via an installed application. They can appear at any time and show various things such as the weather, breaking news, missed calls or text messages, reminders, etc.

They can also be utilized as second-factor authentication (or password-free authentication), which works as an additional layer of security to protect users' online accounts from attackers. With push notification authentication, a push notification is sent directly to a mobile device—usually a smartphone—registered to an online account, alerting the user that a login attempt is taking place. The user can then review the notification details and either approve or deny the request by tapping a button.

One of the main advantages of this method is that it's a simple way to authenticate login attempts that don't require the users to remember and manage complex passwords for their accounts. Over the past few years, there's been a sharp increase in the adoption of push notification-based authentication systems like Duo-Push and Authy. They have also been commercially adopted by major software and service companies like Google, Twitter and several academic entities.

While this method is fundamentally more user-friendly than the one-time password method, it contains several security risks, one of which is called a concurrency attack, introduced in Saxena's research.

During this type of attack, a malicious actor will acquire a user's password and launch a login session simultaneously as the primary user, gaining access to the user's login credentials. If the attacker and user log in simultaneously, the user's device will receive two "push to approve" notifications. Because there is no fundamental difference between the two notifications, they could unknowingly accept the attacker's notification, giving them access to sensitive information (banking, school, etc.).

An early solution the researchers developed, which is mentioned in their European Symposium on Security and Privacy paper, consisted of using a random four-digit number the user would have to compare and match to accept the notification. With this type of approach, however, there's a high chance that they will not look at it close enough and accept the attacker's notification.

"There is a large amount of literature in the usability security community showing that people don't pay attention to these security notifications, warnings and things of that nature," said Saxena. "They bypass them by pressing the OK button so that they can connect and pursue their main task. They don't anticipate an attack, so we didn't want to use this method."

To address this design flaw, the researchers designed a new method called REPLICATE. With REPLICATE, users need to approve the login attempt by replicating a randomized interaction presented on the browser session over on the login notification, explicitly binding the notification to the user's browser session. For example, the user would be instructed to drag a key icon in a particular direction in one interaction. In another interaction, the user would be shown colored buttons and press the correct one.

While the interactions are simple to perform, they will prevent a concurrency attack from occurring because the interaction required to validate the user's session will differ from the interaction the attacker will be required to perform to approve their session.

To test the effectiveness of the interface, the team conducted a usability study with 40-50 participants, where they evaluated and compared its efficacy to the "just tap" method. They found that the study participants could successfully carry out the simple tasks efficiently with little to no errors.

"If the attacker were to log in at the same time to carry out an attack against this method, they wouldn't succeed because the user is matching their browser session with the notification and wouldn't be able to accept the attacker notification," said Saxena.

In addition to studying REPLICATE's effectiveness with a larger study group to better measure its usability and adaptability in practice, the researchers want to increase the randomness of the process of matching the browser session with the notification.

"For example, when you look at the number of options for the key drag interaction, the randomness involved in this process is very low. If the user receives two notifications, one saying, 'drag it up' and the other 'drag it down,' the user could pick the attacker's notification, perform that operation, and accept it. Although we did not see it in the study, there's still a small possibility that it could happen, so that would be one thing we need to solve."

**More information:** Jay Prakash et al, Countering Concurrent Login Attacks in "Just Tap" Push-based Authentication: A Redesign and Usability Evaluations, 2021 IEEE European Symposium on Security and Privacy (EuroS&P) (2021). DOI: 10.1109/EuroSP51992.2021.00013, ieeexplore.ieee.org/document/9581191

Provided by Texas A&M University College of Engineering

Citation: New methods could improve security of two-factor authentication systems (2022, April 14) retrieved 9 April 2024 from https://techxplore.com/news/2022-04-methods-two-factor-authentication.html