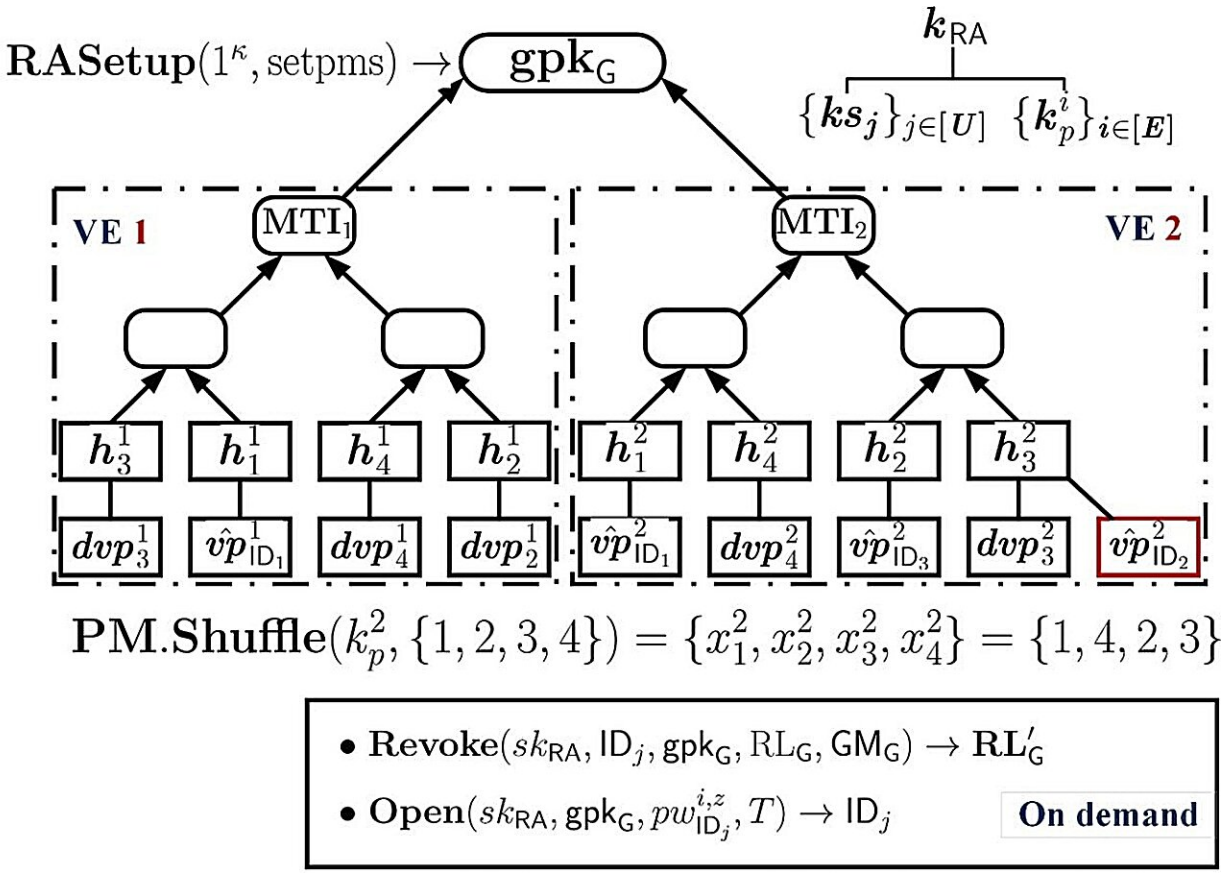
Enhancing cybersecurity with 'moving trees'

May 29 2024



High-level Merkle Tree Structure. Credit: *IEEE Transactions on Information Forensics and Security* (2024). DOI: 10.1109/TIFS.2024.3386350

"Please enter the code within the next two minutes." The concept of one-time passwords (OTPs) has become a mainstay in our procedures for secure user verification in sensitive applications, such as government and

financial services. Typically found in multi-factor authentication schemes, a standard OTP resists hacking attempts by imposing a time limit for users to input the given password.

However, in the face of increasing cyberthreats, current OTP protocols will be slowly rendered obsolete. Designing a better protocol to enforce the security and privacy of user information is no mean task.

Professor Zhou Jianying from the Singapore University of Technology and Design (SUTD) and his collaborators recently proposed a new scheme that addresses some of the shortcomings of existing OTP methods. Findings from this study are published in the paper "Dynamic group time-based one-time passwords," in *IEEE Transactions on Information Forensics and Security*.

There are several standard approaches to implementing OTP schemes. One approach, dubbed RFC 6238, stores symmetric keys to generate these transient passcodes which are supposed to be shared with the institution's server. Another, the Lamport'81 scheme, requires the user device and server to have separate password verification keys.

However, each approach comes with its own vulnerabilities—RFC 6238 is vulnerable to breaches to the server, while the Lamport'81 scheme cannot prevent the malicious tracking of each user's identity. This presents an alluring treasure trove for potential miscreants: if they can pry a crack open into the server, security information for all users are theirs for the taking.

Developments in the cryptographic scene have proposed various means to close the lid on this vulnerability. Prof Zhou highlighted one particular group time-based OTP (GTOTP) scheme which was proposed earlier with his collaborators. This scheme involves a random shuffling tree-like structure, with users tagged to each leaf on the tree for verification.

The arboreal algorithm structure, however, cannot be changed after it has been planted. All users that participate in the identity verification must be present from the start—they cannot leave nor can new users join.

Prof Zhou said, "The static nature of group structures assumed by previous schemes didn't reflect the fluidity often seen in memberships, whether in business contexts, collaborative projects, or community settings."

In the latest work, Prof Zhou and his collaborators studied a new scheme called dynamic GTOTP (DGTOTP) that can be implemented in practical situations. The researchers focused on two hurdles to overcome the difficulty of dynamic user environments: (1) fast and efficient algorithms for small devices, and (2) group management of the malleable pool of users.

Modern handheld devices are typically small and do not have large computational prowess. Any algorithm running on the device should be kept compact and efficient. The researchers suggest a three-fold approach to reduce computational overhead.

"The DGTOTP scheme employs outsourcing solutions for tasks like password generation and management to reduce the computational burden on group members. Furthermore, it addresses secure integration challenges by enhancing message authentication features," explained Prof Zhou, highlighting the lightweight anonymous client authentication approach.

As the pièce de résistance, the scheme uses an issue-first-and-join-later (IFJL) strategy which allows for the seamless handling of joining operations without disrupting other group members' local states.

This dynamic scheme can be applied to real-world scenarios where secure and efficient authentication within dynamic group settings is crucial. For instance, collaborative work environments where teams often change members or work with external partners would benefit from having a secure access to shared resources while facilitating secure onboarding and offloading. In online communities and forums, moderators may choose to restrict access to certain sections or features.

Prof Zhou's proposal is just the first step to enhancing privacy and security, with many paths to explore. There are still some ways to go before witnessing widespread adoption.

"For practical applications, an extension of our concept to securely integrate transport layer security (TLS) and DGTOTP could lead to the development of a protocol for mutual anonymous authenticated credential channel establishment," he concludes.

More information: Xuelian Cao et al, Dynamic Group Time-Based One-Time Passwords, *IEEE Transactions on Information Forensics and Security* (2024). DOI: 10.1109/TIFS.2024.3386350

Provided by Singapore University of Technology and Design