Theme: Security & Privacy

- Sub Theme: Continuous Authentication (Contextual intelligence driven continuous and implicit authentication)

Existing authentication systems for mobile and IoT devices impose huge burden on users (who own multiple devices) in terms of configuring and managing credentials (authentication secrets), and entering credentials 50+ times a day on multiple devices, apps, and websites. Due to such usability issues, users end up creating weak credentials across devices and apps, exposing themselves to various guessing attacks. Since most devices implement all or nothing type of access control, attackers could potentially access everything on users' devices by successfully guessing passwords (explicit authentication secrets).
To address such usability and security issues, the security community has been intensively developing implicit and continuous authentication schemes, to (a) ensure that a single password compromise cannot lead to compromise of the entire device, and (b) minimize the number of times users have to explicitly authenticate themselves on multiple devices and apps.

We are aiming to find and explore new implicit and continuous authentication factors that are driven by contextual, situational, and environmental intelligence. An example factor is the use of trustable locations – continuously checking that devices are physically located within pre-defined trustable locations (e.g., homes or workplace), and automatically unlocking devices in such contexts. Another example is the use of trustable (pre-defined) devices, allowing a primary device to be unlocked continuously when a known, trustable device is physically nearby. Our goal is to explore such

authentication factors that are novel and practical, and could facilitate more usable and secure authentication environments for mobile and IoT device users.

- User’s proximity based authentication that does not heavily rely on possession of trustable devices
- Human body’s signal / human body’s response to external stimulus (e.g. electric pulse) based authentication
- Mobile app usage behavior based authentication
- Tiny (almost unnoticeable) wearable based authentication (e.g., very thin smart ring)
- Authentication / secure communication using a human body.
- Identification and authentication of a user/thing among multiple users/things.

※ The topics are not limited to the above examples and the participants are encouraged to propose original idea.

※ Funding : Up to USD $200,000 per year