ShakeUnlock: Securely Transfer Authentication States Between Mobile Devices

ABSTRACT:

Many people already carry multiple mobile devices such as mobile phones, tablets, and smart watches. Other wearable computing gadgets (e.g. activity or fitness trackers) are on the rise as well. Most of these devices have access to, process and/or store sensitive information [2]. Well-known examples include, but are not limited to, communications (email, SMS, instant messaging), context information (location), access to non-public networks (WiFi, VPN), access to payment or identity management applications, photos, documents, and even health related information (e.g. heart rate). In addition, with the "Bring your own device" trend, employees start to store and process company data on private devices (cf. [3], [4]). To prevent attackers from gaining access to data stored on these devices, locking and unlocking mechanisms have been developed. Those lock devices while not being used (e.g. after a short idle timeout) and users have to unlock them before usage. While authentication conceptually is divided into knowledge-, biometrics-, and token based-authentication [5], [6], so far approaches for mobile devices mostly utilize either knowledge- or biometrics-based authentication.

SHIELD TECHNOLOGIES,

2232, 3RD FLOOR, 16TH B CROSS, YELAHANKA NEW TOWN, BANGALORE-64

Mail us: shieldtechnoblr@gmail.com / manager@shieldtechno.com

Contact: 9972364704 / 8073744810