Securing Two-factor Authentication for Smartphones in a Usable Way by Adding a Connected Token

Matthias Lange
Security in Telecommunications, Technische Universität Berlin
mlange@sec.t-labs.tu-berlin.de

ABSTRACT

Todays two-factor authentication solutions for smartphones either rely on a replaceable smartcard or a trusted execution environment such as TrustZone. The user has to enter a pin or passcode into the device to authenticate himself. Research has shown that this method is easy to break. An attacker can easily spy on the secret through logging the input, recording screen reflections [1] or deriving it from sensor readings [2]. After stealing the device the attacker is able to access data stored on the device without the owner's interaction. He may use a controlled environment (e.g. Faraday cage to shield the device from radiation) to evade remote wipe. The critical point in those attacks is that the possession factor is only limited to the smartphone.

In this work we combine a smartphone and an external, connected *smart token* to build a strong authentication mechanism that withholds existing attack vectors. This extends the possession factor beyond the mobile device. The token is connected (via Bluetooth or NFC) to the smartphone. During authentication a message is pushed to the token where the user has to approve or deny the authentication request.

Instead of using a proprietary gadget we want to use a smart watch. It combines powerful hardware with a rich OS. This will lead to broad acceptance among users as wearing a wrist watch is socially accepted behaviour. Further this approach provides high usability and protects the user's privacy by not revealing anything about the user's security status.

BODY

Two-factor authentication for smartphones is easy to break and can be secured by using a smart watch which acts as a connected token.

REFERENCES

[1] R. Raguram, A. M. White, D. Goswami, F. Monrose, and J.-M. Frahm. ispy: automatic reconstruction of typed input from compromising reflections. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS '11, pages 527–536, New York, NY, USA, 2011. ACM.

[2] Z. Xu, K. Bai, and S. Zhu. Taplogger: inferring user inputs on smartphone touchscreens using on-board motion sensors. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, WISEC '12, pages 113–124, New York, NY, USA, 2012. ACM.

Volume 1 of Tiny Transactions on Computer Science