Decoupling data-at-rest encryption and smartphone locking with wearable devices

Ildar Muslukhov, San-Tsai Sun, Primal Wijesekera, Yazan Boshmaf, Konstantin Beznosov

PII: S1574-1192(16)30088-8
DOI: http://dx.doi.org/10.1016/j.pmcj.2016.06.016
Reference: PMCJ 722

To appear in: *Pervasive and Mobile Computing*

Please cite this article as: I. Muslukhov, S.-T. Sun, P. Wijesekera, Y. Boshmaf, K. Beznosov, Decoupling data-at-rest encryption and smartphone locking with wearable devices, *Pervasive and Mobile Computing* (2016), http://dx.doi.org/10.1016/j.pmcj.2016.06.016

Decoupling Data-At-Rest Encryption and Smartphone Locking With Wearable Devices

Ildar Muslukhov*, San-Tsai Sun, Primal Wijesekera, Yazan Boshmaf, and Konstantin Beznosov

The University of British Columbia

4085-4224 Main Mall, Vancouver, BC, Canada

{*ildarm, santsais, primal, boshmaf, beznosov*}*@ece.ubc.ca*

Abstract

Smartphones store sensitive and confidential data, e.g., business related documents or emails. If a smartphone is stolen, such data are at risk of disclosure. To mitigate this risk, modern smartphones allow users to enable data encryption, which uses a locking password to protect the data encryption key. Unfortunately, users either do not lock their devices at all, due to usability issues, or use weak and easy to guess 4-digit PINs. This makes the current approach of protecting confidential data-at-rest ineffective against password guessing attackers. To address this problem we design, implement and evaluate the Sidekick system – a system that uses a wearable device to decouple data encryption and smartphone locking. Evaluation of the Sidekick system revealed that the proposal can run on an 8-bit System-on-Chip, uses only 4Kb/20Kb of RAM/ROM, allows data encryption key fetching in less than two seconds, while lasting for more than a year on a single coin-cell battery.

Keywords: smartphone loss and theft, data-at-rest encryption, smartphone locking, wearable devices, encryption keys management

*Corresponding author: Ildar Muslukhov (ildarm@ece.ubc.ca)