Title: Identification of pressed keys by time difference of arrivals of mechanical vibrations

Author: Gerson de Souza Faria, Hae Yong Kim

PII: S0167-4048(15)00166-2
DOI: http://dx.doi.org/doi:10.1016/j.cose.2015.11.002
Reference: COSE 955

To appear in: *Computers & Security*

Received date: 1-7-2015
Revised date: 10-9-2015
Accepted date: 4-11-2015

Please cite this article as: Gerson de Souza Faria, Hae Yong Kim, Identification of pressed keys by time difference of arrivals of mechanical vibrations, *Computers & Security* (2015), http://dx.doi.org/doi:10.1016/j.cose.2015.11.002.

Identification of Pressed Keys by Time Difference of Arrivals of Mechanical Vibrations

Gerson de Souza Faria[a,1,]*, Hae Yong Kim[a,1]

[a]*Departamento de Engenharia de Sistemas Eletrônicos, Escola Politécnica, Universidade de São Paulo, Av. Prof. Luciano Gualberto, tr. 3, 158, CEP 05508-010, São Paulo, Brazil*

*Corresponding author

Email addresses: gerson.faria@usp.br (Gerson de Souza Faria), hae@lps.usp.br (Hae Yong Kim)

Highlights

- We show a new physical vulnerability of commercial pinpads.
- We could infer the pressed PIN number within 96.4% of success.
- The certification processes does not address this new side-channel attack.
- Design flaws responsible for the vulnerability are spotted and explained.

Abstract

The possibility of finding the sequence of pressed keys in a mechanical keyboard is a serious