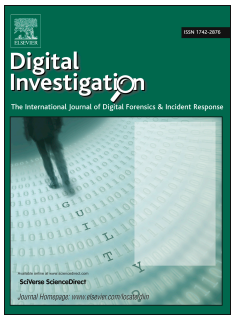
Accepted Manuscript



How to decrypt PIN-Based encrypted backup data of Samsung smartphones

Myungseo Park, Hangi Kim, Jongsung Kim

PII: S1742-2876(18)30176-2

DOI: 10.1016/j.diin.2018.05.006

Reference: DIIN 783

To appear in: *Digital Investigation*

Received Date: 19 April 2018

Revised Date: 30 May 2018

Accepted Date: 30 May 2018

Please cite this article as: Park M, Kim H, Kim J, How to decrypt PIN-Based encrypted backup data of Samsung smartphones, *Digital Investigation* (2018), doi: 10.1016/j.diin.2018.05.006.

How to Decrypt PIN-Based Encrypted Backup Data of Samsung Smartphones

Myungseo Park[a], Hangi Kim[a], Jongsung Kim[a,b,*]

[a] *Dept. of Financial Information Security, Kookmin University,77 Jeongneung-Ro, Seongbuk-Gu, Seoul, 02707, Korea*
[b] *Dept. of Information Security, Cryptology and Mathematics, Kookmin University, 77 Jeongneung-Ro, Seongbuk-Gu, Seoul, 02707, Korea*

Abstract

Smartphones, which are a necessity for modern people, have become important to forensic investigators, as they have a lot of user information which can be potential evidences. In order to obtain such evidences, forensic investigators should first extract the data from the smartphone. However, if the smartphone is lost or broken, it would be difficult to collect the data from the phone itself. In this case, the backup data can be very useful because it stores almost all information that the smartphone has. Nevertheless, since the backup data is basically encrypted by applications provided by vendors, the encrypted backup data which acts as anti-forensic is difficult to use. Therefore, it is crucial to decrypt the acquired encrypted backup data in order to effectively use it.

In this paper, we propose a method to decrypt the Samsung smartphone backup data which is encrypted by a user input called PIN (Personal Identification Number) and a Samsung backup program called Smart Switch. In particular, we develop algorithms to recover the PIN and to decrypt the PIN-based encrypted backup data as well. We have experimentally verified the PIN recovery backup data decryption up to 9 digits of PIN. Our implementation using a precomputed PIN-table with memory 30.51GB takes about 11 minutes

*Corresponding author.
Email addresses: pms91@kookmin.ac.kr (Myungseo Park), tiontta@kookmin.ac.kr (Hangi Kim), jskim@kookmin.ac.kr (Jongsung Kim)
URL: http://dfnc.kookmin.ac.kr/ (Myungseo Park)