Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 116 (2017) 381–392

Procedia Computer Science

www.elsevier.com/locate/procedia

2nd International Conference on Computer Science and Computational Intelligence 2017, ICCSCI 2017, 13-14 October 2017, Bali, Indonesia

A review of collisions in cryptographic hash function used in digital forensic tools

Zulfany Erlisa Rasjid[a*], Benfano Soewito[b], Gunawan Witjaksono[b], Edi Abdurachman[c]

[a]*Doctor of Computer Science, School of Computer Science, Bina Nusantara University*
[b]*Binus Graduate Program, Bina Nusantara University*
[c]*Binus Graduate Program, School of Statiatics, Bina Nusantara University*

Abstract

Digital forensic tool is a software used by digital evidence investigators to extract data and information from a digital evidence. The integrity of the digital evidence must be maintained through the chain of custody in order to be admissible in court. Most digital extraction tool use either MD5 (Message Digest) or SHA (Secured Hash Algorithm) hashing to check the integrity of digital evidence. The hashing algorithm has been found to have a weakness known as collision in which two different messages have the same hashing values. Although the probability of producing such weakness is very small, this collision can be used to deny the usage of the evidence in court of justice. After the first collision has been found, many cryptanalysts have tried to explore various methods to detect the collisions with shorter and efficient time. This paper is to review the existing methods in digital forensic tools that have been used to create a collision attacks in digital evidence.

© 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the scientific committee of the 2nd International Conference on Computer Science and Computational Intelligence 2017.

Keywords: MD5; digital evidence; hash function; collision; digital forensic; cryptography

[*] Corresponding author.
E-mail address: zulfany@binus.ac.id

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the scientific committee of the 2nd International Conference on Computer Science and Computational Intelligence 2017.
10.1016/j.procs.2017.10.072

1. Introduction

Cryptographic hash function is a function that converts a message of any length to a data of fixed length. The purpose of cryptographic hash is to ensure the integrity of data. Digital forensic tool is a tool to extract evidence data from different storage media, such as hard Drive, Memory, file system etc. There are several open source tools that are widely used to carry an investigation. Those tools include EnCase, SanSift Kit and many more. Most digital forensic tool use SHA (mostly SHA-1 because of its performance) and MD5 (Message Digest) hashing function to proof the data integrity. The problem with these digital forensic tools is a collision which has been reported by many researchers to indicate a weakness in this cryptographic has function. Collision is a condition whereby two or more files that has differences in contents and behaviors but having the same hash value. After the discovery of MD5 collision by Wang et al. [1], more and more cryptanalyst try to discover more collisions in more efficient time, for both MD5 and SHA hashes. The purpose of this review paper is to gain extensive knowledge on how collision attacks were performed using various methods, and how different strategies are proposed to improve hash algorithms.

2. Digital Forensics Tools

Six popular tools based on the information from http://resources.infosecinstitute.com/computer-forensics-tools/#gref that are commonly used in Digital Forensics which is summarized in table 1. It shows that top widely used Hash function that is used in Digital forensics is MD5 algorithm and some uses SHA algorithm, even though other algorithms are available such as RIPEMD and HAVAL. FTK Imager uses both MD5 and SHA. Normally investigators choose one instead of using both hashing methods as it involves additional time when using two different hash algorithms. Due to the fact that most Digital Forensics Tools uses MD5 and SHA hash algorithm to check the integrity of files, this paper reviews the two algorithms in terms of collision attacks. Collision attacks compromises the integrity of the digital evidence.

Table 1: List of most widely used Digital Forensic Tool

No.	Digital Forensic Tool	Hash Function	Features
1	EnCase	MD5	Remote Forensic Capability Evidence Processor Manager Smartphone and Table support Case Analyzer Email Review
2	San Sift	MD5	Network Forensics Computer Forensics Cloud Forensics Memory Forensics
3	Sleuth Kit	MD5	Contains a collection of unix commands for volume analysis and file systems
4	FTK Imager	SHA1 and MD5	Acquire and Preserve data from different media Forensics for computer and mobile Detect and validate suspected Malicious activities
5	Bulk Extractor	MD5	Forensic Scanner Feature Extraction Files, images and emails

Download English Version:

https://daneshyari.com/en/article/4960466

Download Persian Version:

https://daneshyari.com/article/4960466

Daneshyari.com