ABSTRACT

The increasing portability of computing devices combined with frequent reports of privacy breaches and identity theft has thrust data encryption into the public attention. While encryption can help mitigate the threat of unintentional data exposure, it is equally capable of hiding evidence of criminal malfeasance. The increasing accessibility and usability of strong encryption solutions present new challenges for digital forensic investigators. Understanding forensic analysis as a multidisciplinary field that searches evidence of crime, the authors focus their topic on particularity of cross-disciplinary issues arising in this area: Forensic analysis uses cryptology, information technology and mathematics in extracting encryption keys from memory. The chapter highlights the virtues of volatile memory analysis by demonstrating how key material and passphrases can be extracted from memory and reconstructed to facilitate the analysis of encrypted data. The authors show current methods for identifying encryption keys in memory and discuss possible defeating techniques and cryptosystem implementation strategies that could be used to avoid the key extraction.

INTRODUCTION

Currently, many organizations and government institutions have some experience, may be major or minor, of losing sensitive data. In May 2007, the Transportation Security Administration (TSA) lost a hard drive containing approximately 100,000 employee bank account details, while in October 2007 two laptops containing names and social security numbers of almost 4,000 employees were stolen.
In the same year, the government in the United Kingdom reported that two disks with personal information details of 25 million citizens had been lost. This forced many institutions to improve their data security procedures by implementing encryption mechanisms to protect their sensitive data.

Nonetheless, encryption is a double-edged sword. On one hand, it protects our sensitive data, on the other it allows criminals to hide data that would convict them of a crime.

Encryption has been used in relation to pedophilia, terrorism, organized crime and espionage (Denning, 1997).

In 2007, an incident happened when US Customs found child pornography on a Canadian citizen and legal US resident Sebastian Boucher’s laptop. The laptop was seized as the evidence and he was charged with transporting the pornography across borders. The problem appeared when examiners tried to open the incriminating drive Z and found out that it was a Pretty Good Privacy encrypted container. Although a forensic duplicate of hard drive was created after the shutdown of the notebook, the examiner could not open the encrypted container. Boucher refused to give the password on the grounds that it violated the Fifth Amendment right against self-incrimination.

The cooperation between the fields of cryptology, information technology, and forensic analysis is necessary in order to be able to obtain the encrypted evidence. In this chapter, we summarize possibilities, which individual fields of the forensic analysis offer to detect relevant information (evidence), and identify encryption keys, respectively. Moreover, we discuss the current state of and future trends in these areas.

FORENSIC ANALYSIS

Forensic Investigation Possibilities

Today, the forensic investigators cannot use the traditional, widely accepted computer forensic methodology of unplugging the power to a computer and then acquiring a bit-stream image of the system hard drive anymore. Investigators and incident responders are often seeing instances in which the questions they asked cannot be answered using the contents of an imaged hard drive alone. In many cases, the best source of information or evidence is available in computer memory. While the computer operates, RAM stores all the accumulated data for running applications and network communications. There is a great amount of information in RAM that exists only when applications are running. Most of this information cannot be easily obtained from a hard drive (Carvey, 2009).

Information that can be obtained from RAM includes:

- network connections, contents of the Instant Messenger client window, memory used by the Instant Messenger client process, decrypted versions of otherwise encrypted data, cryptographic key material, hard drive encryption keys, wireless keys, usernames and passwords, etc. (see short paper titled “The Value of Physical Memory Analysis for Incident Response” written by Hoglund (2008) (Hoglund, Greg is a Chief executive officer (CEO) of HBGary, Inc). Carvey (2009) also described more reasons, why the forensic investigator should collect the contents of RAM.

Volatile memory forensics has become increasingly prominent in the area of forensic analysis and incident response. Live forensics (on-line analysis) involves performing analysis at the same time the evidence is collected. And live systems also allow us to collect much more robust data. Another method used to analyze memory is off-line analysis. When forensic investigator performs the off-line analysis, they first collect digital evidence in live environment (usually a dump of all memory is created), and then that evidence is analyzed on another computer. Evidence must be analyzed on another computer because forensic analysis fights with similar limitations as rootkit detection: live detection can almost always be defeated by resident rootkits (Davis, 2009). On the other hand off-line