Chapter 3
Cryptography for the Forensics Investigator

Thomas Martin
Khalifa University, UAE

ABSTRACT

There are many challenges for a forensic investigator when it comes to digital evidence. These include the constantly changing technology that may store evidence, the vast amounts of data that is stored, and the increasing use of cryptography. This last problem can prevent any useful information being retrieved and is encountered in the use of communication protocols, whole-disk encryption, and individual applications. Cryptography is a field of great depth and breadth, encompassing both complex mathematics and cutting-edge technology. A forensics investigator does not need to be aware of all aspects of this field, but there are certain areas that are vital. The knowledge described in this chapter can assist an investigator in obtaining information that may otherwise be obscured, and also prepare them to defend the integrity of any evidence obtained.

INTRODUCTION

Computer Forensics, the study of digital evidence relevant to legal matters, has long been considered solely the domain of law enforcement. And while this has been true in the past, there is an increase in the use of forensics in other areas. Outside of criminal cases, forensics can be relevant to Industrial Tribunals, E-Discovery and Incident Management. Information Systems need be designed to support the forensics investigator in satisfying these legal procedures. But beyond mere satisfying obligations, good forensics capabilities can strengthen the security of Information Systems. Gone is the notion that any system can be completely secure. When a breach does happen, a

DOI: 10.4018/978-1-4666-4030-6.ch003

well designed forensics capability (supported by staff trained to perform the analysis) can quickly determine the cause of the incident without major disruption. The sensitive nature of such investigations that require unrestricted access, as well as the potentially damning conclusions, has lead many organizations to develop such capabilities in-house.

Cryptography is seeing increased usage, in response to problems of data leakage, both commercial and personal. Criminals have also been known to use encryption to hide the details of their crimes. As encryption products become more easy to use and freely available, they are going to be encountered in more investigations. Encryption is a potential barrier to a forensics investigator. The physical media may be successfully captured, but encryption can prevent any information from being retrieved.

In this chapter, we will describe those aspects of cryptography that are vital to a forensics investigator. First, we describe the fundamental goals of cryptography and briefly describe the algorithms that achieve them. Second, we explain all the steps necessary to protect the integrity of any information collected. Finally, we propose a set of best practices that can be conducted when an investigator encounters encrypted evidence.

BACKGROUND

Ideally, a forensics investigator would have a back door to any cryptography encountered. Such mechanisms have long been proposed (Denning, 1996) but have not seen widespread adoption. Occasionally there are mistakes in the implementation of cryptography that have lead to weaknesses (e.g. a software bug caused predictable keys in the Debian Openssl package (Bello, 2008), or low entrophy causing repetition of RSA primes (Lenstra et al., 2012)), but the number of cases is small, and one cannot rely on them being present.

In spite of the obstacles, a good deal of research has been undertaken on what can be done by a forensics investigator in the face of encrypted evidence. The majority of the work to date has focused on capturing keys from live memory. Shamir and Someren proposed a method for looking for the high entropy as a tell-tale aspect of RSA keys (Shamir & Van Someren, 1999). Klein instead looked for the common formats and syntax of keys and certificates (Klein, 2006). Halderman extended the timeframe that keys could be captured in memory by freezing the memory and using error-correction techniques (Halderman, Schoen, Heninger, Clarkson, Paul, Cal, Feldman, & Felten, 2006). The work of (McGrath, Gladyshev, & Carthy, 2010) identified many useful artefacts from the use of PGP/X509 public key encryption, including file headers, times, dates, identities, etc. Tromer demonstrated that inter-process information leakage can allow an unprivileged process to gain access to AES keys of processes running in parallel (Tromer, Osvik, Shamir, 2010).

FUNDAMENTALS

Forensics investigators require at least a superficial knowledge of cryptography. In this section we will describe the specific objectives of integrity and confidentiality aspired for in cryptography. We will briefly cover some of the algorithms currently used to achieve these objectives. We will also mention some of the upcoming advances in cryptography (fully homomorphic encryption, quantum computers) and the impacts they will have.

Confidentiality

Cryptography has been primarily been used to ensure the confidentiality of information. Encrypted information whether stored or in transit, must be prevented from being accessed by all but authorized parties. Encryption can be either