Chapter 17
Forensic Investigation of Digital Crimes in Healthcare Applications

Nourhene Ellouze
University of Carthage, Tunisia

Slim Rekhis
University of Carthage, Tunisia

Noureddine Boudriga
University of Carthage, Tunisia

ABSTRACT

Healthcare applications are increasingly being used due to the safety and convenience brought to patients' life and healthcare professionals, respectively. Nevertheless, the use of weak authentication techniques and vulnerable communication protocols makes these applications threatened by specific classes of security attacks and e-crimes. The latter threaten the privacy, the safety and even the life of the persons using these applications, due to the fact that they handle sensitive information and implement complex and critical features. This chapter focuses on postmortem investigation of crimes on healthcare applications. After classifying crimes targeting healthcare applications, the requirements for the design of appropriate postmortem investigation system, are discussed. A literature review of proposals related to the investigation of crimes in healthcare applications together with a discussion of the advanced issues are also provided in this chapter.

INTRODUCTION

The advances in Information and Communications Technologies have led to the release of a wide set of healthcare applications, including, but are not limited to, remote monitoring of patients in hospitals, real time detection of emergency situations threatening chronically ill patients, and continuous monitoring of

DOI: 10.4018/978-1-7998-3025-2.ch017

elderly people. Healthcare applications are increasingly being used owing to the great efficiency and quality of service they offer to elderly persons, patients, and healthcare professionals. They have contributed to the enhancement of patients' autonomy, and the improvement of clinical treatment and remote health surveillance through the development and implementation of several technologies and equipment like, Wireless Sensor Networks (WSN), Implantable Medical Devices (IMDs), and cloud services.

Healthcare applications exhibit significant security weaknesses including the use of weak authentication techniques and the lack of appropriate security mechanisms. These weaknesses make them unprotected and subject to several criminal attacks threatening the safety and the privacy of patients, especially as these applications handle sensitive medical data and provide life-sustaining functions. Among the most common crimes targeting healthcare applications, we cite the unauthorized access to the medical records. Such type of attacks may induce serious threats on the privacy of the victims through the disclosure of their medical records, or even may threaten their life through the malicious modification of their medical records to make further medical prescription by physicians erroneous. In this context, the design of a system for postmortem investigation of criminal incidents threatening healthcare systems is becoming a key requirement.

A set of challenging issues should be addressed during the design of a postmortem investigation system tailored to healthcare applications. The first challenge is related to the storage of the huge amount of evidential traces that can be provided by healthcare systems, as these traces require an unlimited storage space when collected over a long period of time. The second challenge is related to the integrity and the trustworthiness of the provided evidence, especially as healthcare systems are connected to open environments (e.g., internet) through vulnerable communications protocols. The third is related to the complexity of medical evidence collection and processing, especially as healthcare systems implement different technologies and equipment that may provide heterogeneous evidence. The fourth challenge is related to the need that an investigation on healthcare digital crimes collects and analyzes two types evidence collected from the IT system under investigation. The first type contains information related to authentication, access, sensitive events execution, while the second type contains the medical information related to the victim health status.

Several research works have focused on the identification of criminal attacks targeting healthcare applications, and the development of security techniques protecting them from security attacks. Other research works focused on the development of secure audit and accounting tailored to healthcare applications to prepare for a postmortem investigation. A set of postmortem investigation techniques were also proposed in the literature to address medical and physical crimes. An overview of these research works will be provided in this chapter.

The remaining part of this chapter is organized as follows. The next section provides an overview of e-health systems. In Section 2, we identify and classify crimes targeting healthcare systems. Section 3 discusses the main requirements for the design of postmortem investigation of e-crimes on healthcare applications. In Section 4, we review the literature related to the design of techniques and methodologies for the checking of audit logs and the analysis of incidents on Wireless Body Area networks. We also discuss in this section digital investigation scope and techniques considering attacks on Implantable Medical Devices. Section 5 reviews investigation techniques tailored to physical crimes. In Section 6, we discuss advanced issued related to the investigation of criminal attacks on healthcare applications.