

Chapter 7

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.

DOI: 10.4018/978-1-5225-0463-4.ch007

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 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.

40 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/forensic-investigation-of-digital-crimes-in-healthcare-applications/157459

Related Content

Decision Rule Extraction for Regularized Multiple Criteria Linear Programming Model

DongHong Sun, Li Liu, Peng Zhang, Xingquan Zhu and Yong Shi (2011). *International Journal of Data Warehousing and Mining* (pp. 88-101).

www.irma-international.org/article/decision-rule-extraction-regularized-multiple/55080

When Should We Ignore Examples with Missing Values?

Wei-Chao Lin, Shih-Wen Ke and Chih-Fong Tsai (2017). *International Journal of Data Warehousing and Mining* (pp. 53-63).

www.irma-international.org/article/when-should-we-ignore-examples-with-missing-values/188490

Hierarchical Hybrid Neural Networks With Multi-Head Attention for Document Classification

Weihao Huang, Jiaojiao Chen, Qianhua Cai, Xuejie Liu, Yudong Zhang and Xiaohui Hu (2022). *International Journal of Data Warehousing and Mining* (pp. 1-16).

www.irma-international.org/article/hierarchical-hybrid-neural-networks-with-multi-head-attention-for-document-classification/303673

Intelligent Text Mining: Putting Evolutionary Methods and Language Technologies Together

John Atkinson (2009). *Handbook of Research on Text and Web Mining Technologies* (pp. 37-59).

www.irma-international.org/chapter/intelligent-text-mining/21716

Mining Customer Knowledge for a Recommendation System in Convenience Stores

Shu-Hsien Liao, Chih-Hao Wen, Pei-Yuan Hsian, Chien-Wen Li and Che-Wei Hsu (2014). *International Journal of Data Warehousing and Mining* (pp. 55-86).

www.irma-international.org/article/mining-customer-knowledge-for-a-recommendation-system-in-convenience-stores/110386