Journal of Global Information Management
Volume 30 • Issue 2

Designing and Evaluating an Automatic Forensic Model for Fast Response of Cross-Border E-Commerce Security Incidents

Chia-Mei Chen, Department of Information Management, National Sun Yat-sen University, Taiwan

Zheng-Xun Cai, Department of Information Management, National Sun Yat-sen University, Taiwan

Dan-Wei (Marian) Wen, Guilin University of Electronic Technology, China

ABSTRACT

The rapid development of cross-border e-commerce over the past decade has accelerated the integration of the global economy. At the same time, cross-border e-commerce has increased the prevalence of cybercrime, and the future success of e-commerce depends on enhanced online privacy and security. However, investigating security incidents is time- and cost-intensive as identifying telltale anomalies and the source of attacks requires the use of multiple forensic tools and technologies and security domain knowledge. Prompt responses to cyber-attacks are important to reduce damage and loss and to improve the security of cross-border e-commerce. This article proposes a digital forensic model for first incident responders to identify suspicious system behaviors. A prototype system is developed and evaluated by incident response handlers. The model and system are proven to help reduce time and effort in investigating cyberattacks. The proposed model is expected to enhance security incident handling efficiency for cross-border e-commerce.

KEYWORDS

Digital Forensics, E-Commerce Forensic System, E-Commerce Forensics, E-Commerce Forensics Framework, E-Commerce Security, Forensic Process, Forensics Framework, Incident Response

INTRODUCTION

The explosive expansion of information technologies offers unprecedented opportunities for businesses to expand their markets through cross-border e-commerce, which accounted for roughly 20% of total global online transactions in 2015 (MEDICI Team, 2015) and continues to increase rapidly. The use of ICT is a critical factor in improving service productivity in e-commerce (Rabeh, Islam, Samer, Adnan, & Mustafa, 2019), and the growth of cross-border multi-national e-commerce has set trends for a major overhaul of the online industry (Sanjeev et al., 2019). Many governments consider now cross-border e-commerce as a new dimension of trade (Lianos, Mantzari, Durán, Darr, & Raslan, 2019). However, this increase in cross-border e-commerce activity has been accompanied by a commensurate increase in cyber-crime (Lau, 2018; Shrivastava, 2016). Not only have financial firms suffered serious losses due to cyberattacks (Ismail, 2018), governments, academic institutions, and high-tech firms have also experienced severe information breaches, with significant impacts on policy, research results, and competitive advantage. It is suggested that a serious cyberattack occurs

DOI: 10.4018/JGIM.20220301.oa5

every 39 seconds and that cybercrime could cost businesses up to $5.2 trillion over the next five years (Bera, 2019).

Privacy and security have emerged as two key requirements for successful cross border e-commerce (Karwatzki, Dytynko, Trenz, & Veit, 2017; Sung, 2006; Sutton, Khazanchi, Hampton, & Arnold, 2008). To prevent cyberattacks, businesses promote security awareness through information security education, training and awareness programs which have shown to improve employee security behavior (Winfred, Daniel Okyere, & Peace, 2019). In addition to national regulatory frameworks to promote user privacy protection, trans-national measures have been implemented to ensure cross-border e-commerce security. For instance, in 2016 the Organization for Economic Cooperation and Development (OECD) published its "Consumer Protection in E-commerce" (OECD, 2016) to stress the importance of consumer data security, especially for cross-border e-commerce. In addition, beginning in 2018, EU member states have implemented the General Data Protection Regulation (Tikkinen-Piri, Rohunen, & Markkula, 2018) and the European Data Protection Regulations to harmonize data privacy laws.

In addition to these overarching guidelines for securing e-commerce safety, new attention has focused on measures related to responding to security incidents. As defined in the RFC 2350 ("Expectations for Computer Security Incident Response") (Brownlee & Guttman, 1998), a security incident is any adverse event which compromises some aspect of computer or network security. Generally, it is related to the compromise of confidentiality (e.g., user privacy), integrity (e.g., alteration of confidential information) or availability of information (e.g., Denial of Service attacks). The security incident response process includes evidence collection to facilitate rigorous investigations to protect cybersecurity (Baryamureeba & Tushabe, 2004), entailing evidence acquisition, collection and preservation, analysis, examination, and result reporting (Ademu, Imafidon, & Preston, 2011) using multiple forensic tools and technologies and comprehensive security domain knowledge. This makes identifying and tracking cyberattacks a time- and cost-intensive task for businesses. Moreover, prompt incident response is essential to reducing damage and loss from cyber-attacks.

Digital forensics is a prominent component of incident response and handling that involves collecting and analyzing digital evidence, detecting suspicious patterns of attacks, and presenting an analysis report after a cyberattack incident (Lianos et al., 2019; Shrivastava, Kumar, Gupta, Bala, & Dey, 2018). The goal of digital forensics is forensically examine computerized media to distinguish, protect, recuperate, investigate and express realities and suppositions about advanced data (Shrivastava, Sharma, Khari, & Zohora, 2018). In doing so, evidence reconstruction is achieved after a crime committed by a standalone computer and evidence interpretation from any digital sources (Shrivastava, Sharma, & Dwivedi, 2012).

To fight cyber-crime, digital forensics should acquire as much relevant evidence as possible. Digital evidence (Novak, Grier, & Gonzales, 2018) is stored or transmitted in binary form in various storage media including hard drives, flash memory, random access memory, system logs, application logs, process information, network traffic, etc. The amount of data generated and stored due to our daily activities is increasing rapidly. An IDC study estimated that, in 2020, the world produced more than 5,200 gigabytes of data for each person alive (Gantz & Reinsel, 2012). With the rapid increase of digital evidence, digital forensic investigators have to search through massive amounts of evidence to identify suspicious behavior, raising the need for sophisticated automatic digital forensic tools and procedures (Pollitt, Caloyannides, Novotny, & Shenoi, 2004).

For most e-commerce cyber-attacks, incident handlers require a forensic model to assess a reported incident and prioritize it before initiating a potentially costly and lengthy formal or legal procedure. A digital forensic investigation is often initiated to ascertain certain facts in response to an incident. Prioritizing incidents is critical in the incident response process as well as for damage control. The legal foundation focuses on the use of forensic tools and techniques for the recovery, handling, analysis, and preservation of digital evidence, as opposed to firewalls, antivirus, routing, or intrusion detection. However, the incident response process takes much time and effort (Ryan &