International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 299-314
http://dx.doi.org/10.14257/ijsia.2015.9.6.28

Secure and Trusted Environment as a Strategy to Maintain the Integrity and Authenticity of Digital Evidence

Yudi Prayudi[1] and Tri K Priyambodo[2]

[1]*Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia*
[2]*Department of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, Indonesia*
prayudi@uii.ac.id, mastri@ugm.ac.id

Abstract

The authenticity and the integrity of digital evidence are critical issues in digital forensics activities. Both aspects are directly related to the application of The Locard Exchange Principle (LEP), which is a basic principle of the existence of evidence in an event. This principle, not only applies before and at the time the event occurs, but also applies to the investigation process. In the handling of digital evidence, all activities to access the digital evidence are not likely to occur without the mediation of a set of instruments or applications, whereas every application is made possible for the existence of bugs. In addition, the presence of illegal access to the system, malicious software as well as vulnerabilities of a computer system are a number of potential problems that can have an impact on the change in the authenticity and the integrity of digital evidence. If this is the case, secure and trust characteristics that should appear in the activity of digital forensics may be reduced. This paper tries to discuss how the concept of a secure and trusted environment can be applied to maintain the authenticity and integrity of digital evidence. The proposed concept includes the unity of five components, namely standard and forensics policy, security policy, model and trusted management system, trusted computing, secure channel communication, and human factor. The ultimate purpose of this paper is to provide an overview of how the recommendation can be applied to meet the requirements of a secure and trusted environment in digital forensics for keeping the authenticity and the integrity of digital evidence. In general, this paper tends to explain a high-level concept and does not discuss low-level implementation of a secure and trusted environment.

Keywords: *Digital forensics, secure and trusted, Policy, security, trusted computing, Locard Exchange Principle*

1. Introduction

Authenticity according to [1] is the ability to maintain the initial identity when the digital evidence is obtained for the first time, as well as preserving the integrity in every stage of digital forensics process. In addition, integrity according to Vanstode in [2] is a property on which digital data are not changed by any party who does not have the authority to conduct the change. Only those with the authority could make any changes to and contacts the digital evidence. The authenticity and the integrity of digital evidence guarantee that the exploration, analysis, and information presented are complete and that the digital evidence has been unchanged since it was first discovered until it is finally used in the court or litigation process.

From another perspective, the authenticity and the integrity are directly related to the application of the Locard Exchange Principle (LEP), which is a basic principle on the handling of digital evidence. *i.e.*, "every contact between two different

ISSN: 1738-9976 IJSIA

parties will definitely leave a new trace [3]. In crime scene investigation practice, the implementation of LEP will convince the investigators that there must be evidence that will lead to case disclosure; it is in accordance with the main opinion of Dr. Edmond Locard, "*Every contact leaves a trace*". Further, [4] and [5] mention that Locard Exchange Principle also applies in the digital world; no matter how hard it is to leave a trace in a case, there must be other traces found which will lead to digital evidence that can disclose the case.

Locard Exchange Principle applies not only before and at the time of the case occurrence, but also at the time of the investigation process. Errors during the handling process of digital evidence and/or vulnerability of digital forensics system and environment used by the investigators can cause the emergence of new traces to be considered as digital evidence. When this happens, it will obviously reduce the authenticity and the integrity of digital evidence.

Digital evidence, is any valuable information that is stored or transmitted in digital form or information stored or transmitted in a binary form that can be used in the law enforcement and judicial process [6]. Digital evidence has a number of characteristics; it is easy to duplicate and transmitted, very susceptible to modify and to remove, easily contaminated by new data, and time-sensitive [7]. According to Schatz that cited in [6], in contrast to physical evidence, digital evidence is very dependent on the interpretation of its content. Therefore, the integrity of the evidence and the ability of the expert to interpret the evidence will be influential in sorting digital documents available to serve as evidence.

Based on the principle of "*every contact leaves a trace*", viewing, opening, changing a folder or file, as well as accessing or connecting a system to an external party can be considered as contacts in the context of digital evidence. The contact activities will cause changes in the authenticity and the integrity of digital evidence. Nonetheless, Kirschenbaum *et al.*, [5] revealed that in digital forensics, all activities to access digital evidence are not likely to occur without the mediation of a set of instruments or applications. Therefore, investigator should be able to ensure that whatever they do, starting from the acquisition stage, imaging, storage, exploration, and analysis of digital evidence, must retain the authenticity and the integrity of digital evidence. For example, the use of write blockers during the acquisition process and imaging of electronic evidence is a standard approach to ensure that the processes will not change the authenticity and the integrity of digital evidence. The utilization of proper tools and application, control access to the system, and the application computer security technique and model are several things that should be taken into account in undertaking digital forensics activities.

In the meantime, the presence of bugs in an application, illegal access, malicious software and vulnerabilities in a computer system are potential problems that could cast doubt the authenticity and the integrity of digital evidence. If this is the case, it will certainly affect “secure and trusted” characteristics of the investigation process carried out by law enforcement. It later becomes one of the challenges for practitioners and researchers in digital forensics to ensure that digital evidence obtained is completely trustworthy and the processes carried out during exploration and analysis stage are not disrupted by any application or system that can change the authenticity and the integrity of digital evidence.

The principles of secure and trusted in digital forensics should be the main concern of practitioners and researchers in this field. A variety of tools, particularly automated tools that can be used at each stage of digital forensics as well as the environments that are likely to be connected and networked, should be supported by advanced security mechanisms and higher form of trustworthiness of the system. This certainly requires an integrated effort to maintain the authenticity and the integrity of digital evidence. Unfortunately, until now there are not many studies

addressing this problem and providing a solution to the issues in a secure and trusted environment of digital forensics. Digital forensics activities must be guaranteed free of engineering efforts that will lead to a change in the authenticity and the integrity of digital evidence, and convince all parties that the digital forensics environment is secure and trusted, so that no party will question the investigation and analysis process.

The solution proposed in this paper is to implement a secure and trusted environment-based concept as a strategy to ensure that the digital forensics environment is really secure, can be trusted by all the parties concerned, and is protected from system vulnerabilities and attacks against the contents of the evidence or other information [8]. This paper tries to discuss what strategy can be built to realize the concept of a secure and trusted environment to maintain the authenticity and the integrity of digital evidence in digital forensics activities. The main goal of this paper is to provide an overview of the requirement and give recommendations to realize a secure and trusted environment for digital forensics activities in maintaining the authenticity and the integrity of digital evidence. This paper is still on the high-level concept and does not include a discussion on the low-level implementation of a secure and trusted environment.

2. Digital Forensics Challenges

In the digital society era like today, Lin [9] believe cybercrime is a critical issue. This can be seen from the increasing number or victims and losses caused by cybercrime. In principle, [10] argues that cybercrime is a criminal activity where a computer or computer network is used as the primary means to violate prevailing law, rules, or regulations. Data and survey from PwC and RSA cited by Prayudi [7] show that cybercrime is a serious threat to individuals, institutions or countries and the amount of losses globally could be compared to the national income of a country.

Digital Forensics is a field that will have an increasingly widespread role and contribution for the years to come. This field is necessary to support the efforts of solving cybercrime cases that are commonly found in the society. In relation to cybercrime, digital forensics is also very necessary to resolve the dispute in litigation, involving individuals or institutions. Almost all individuals' and institutions' activities today are recorded through various electronic media and stored in various types of storage that can then be easily explored and analyzed; this is what so-called as the era of Electronics Stored Information (ESI) and e-discovery. This fact certainly can be the means for both parties in dispute to support their argument through exploration of a variety of potential digital evidence. This process obviously requires a digital forensics mechanism. According to [11], almost 67% litigation cases that happened are disputes between a company and its former employees who committed illegal access to corporate data which were then used for personal interests or even sold to its competitors.

Digital forensics is the use of science and methods for finding, collecting, securing, analyzing, interpreting and presenting digital evidence related to the case which is happening for the sake of reconstruction as well as the validity of the court [12]. Cybercrime and digital forensics, according to [13] bring major challenges that must be faced by law enforcements nowadays. This cannot be separated from the growing number of "*skilled technicians*" who use their ability and knowledge in information technology to transform conventional crime into cybercrime [14]. Another challenge is the presence of abundant applications that can be used as crime toolkits. In this case, [15] assume that currently to be able to conduct cybercrime, there is no need to have a strong background in computer technology; even someone

who has no knowledge in technology can easily conduct cybercrime by simply utilizing crime toolkits.

Along with the development of computer and information technology where networking, sharing, collaboration and connectedness become the main forces, cybercrime is becoming more complex these days. Based on the current technological development, [14] and [16] conclude that organized crime is one of the main characteristics of today's cybercrime activities. Furthermore, [17] elaborates that many of the current activities of cybercrime cannot be classified or identified when referring to conventional crime categorization. Cybercrime activities over time become more complex in terms of meaning and variation. This certainly raises a challenge for law enforcement.

According to [18], a growing number of electronic equipments which are able to store data, as well as the lifestyle of web based services and cloud computing, will be some challenges for digital investigators when either collecting digital evidence or exploring and analyzing it. Damshenas [19] argue that one of the challenges of digital forensics is how to deal with the development of technology storage and the dimensions of storage device that currently reach petabytes size and that must be acquired as digital evidence, too; those factors do have an impact on time and efficiency in searching and analyzing data. Then, the mobility trends of computer users as well as the possibility of connectedness between devices will also pose some challenges for the digital forensics in the near future.

The rapid growth of information technology, according to [20] will result in the growing number of potential digital evidence that must be acquired and analyzed since currently one person tends to have multiple devices that are interconnected and synchronized with each other. Flaglien [21] suggests the condition enables the birth of new characteristics of digital evidence called *correlated evidence*. Further, future investigation process tends to be a correlation, and linking criminal behavior using several datamining techniques from some different databases owned by law enforcement.

The protection of integrity and authenticity of digital evidence is only one part of the digital forensics process. All evidence must meet certain legal requirements before being presented in court. Braid as cited in [22] has defined five rules of evidence in order for evidence to be considered useful. Evidence must be admissible, authentic, complete, reliable and believable. Integrity and authenticity of digital evidence are the fundamental concept of digital evidence handling. According to [23], maintaining the integrity and authenticity of digital evidence throughout the process of examination presents different problems from those encountered when handling traditional physical or documentary evidence. Some common problems are exacerbated by the complexity of networked computers.

Digital forensics issues over time has been reviewed by several scholars, namely [18–20], [24, 25]. Based on their studies, there are a few things identified as the problems and challenges of digital forensics in the future, some of which have impacts on the integrity and the authenticity of digital evidence.

Moreover, based on the characteristics of digital evidence, handling of evidence should also consider the order of volatility of the digital evidence. In this case, Brezinski & Killalea in [26] mention the order of volatility of digital evidence as the following: register, memory, processor table, temporary file system, disk, remote logging, data monitoring physical configuration and network topology, and archived data. The development of digital technology enables the emergence of new variation of characteristics of digital evidence. Therefore, the order of volatility of digital evidence is very possible to change or to increase. Certainly, this is going to be the challenge for digital investigators to manage it.

Another challenge faced is the development of techniques categorized as anti-forensics. Ryan Harris in [27] defines anti-forensics as "*any attempts to compromise the availability or usefulness of evidence to the forensics process*". Meanwhile, Peron and Legarty as cited in [28] describe anti-forensics "*as a process of limitation of identification, collecting, comparing and checking of validity of electronic data, in purpose to obstruct a criminal investigation. Digital antiforensics can be called as a set of tactics and measures taken by a person who wants to prevent a process of digital investigation*". In this case, according to (Sant, 2014), a number of malware work to run anti-forensics activities. Thus, when referring to the opinion of [29] who extremely mention that there is no computer platform or environment that currently could withstand malware, then undoubtedly the same rationale also applies to the infrastructure of digital forensics.

3. Secure and Trusted Issue

As an activity and a system that is always related to computer, digital forensics addresses some security issues that have also been studied by a number of researchers. Their main focus is on the efforts to cope with a big variety of cybercrime and hacking. For example, Rao [13] discusses how to anticipate digital forensics of various types of hacking activities (Hacktivism). Then Rekhis [30] has also conducted an investigative analysis toward security incident through formal language approach using the technique of TLA (Temporal Logic of Security Actions). Meanwhile, Flaglien [21] did an investigative analysis by applying data mining as well as looking for correlation between various machines for the purposes of analysis and identification of malware.

The second focus is on the study of to what extent security assurance in digital forensics process is. In this case, Saleem [31] have undertaken a study of algorithm and appropriate methods to support the security and integrity of digital evidence. Here, nine criteria were included as a filter to determine recommended methods and security algorithms. Here, nine criteria were security properties, identification and authentication, accuracy, binding of functionality, strength of mechanisms, attacks and vulnerability assessment, ease of use/ complexity or simplicity, computational efficiency, and time binding. Furthermore, a study done by [32] highlight the importance of safeguarding digital evidence as an important component in the investigation process and proceedings through the implementation of secure protocol logging. Then, Hsu [33] also carried out research on the application of hierarchical access control as a method to protect digital evidence.

The Issues of trust within the scope of digital forensics have been discussed by [34] through the concept of machine trust model to determine which digital evidence that meets the trust criteria. The model was proposed as a solution to problems that might be encountered by investigators when determining which digital evidence must be trusted if there is a contradiction between the evidence obtained. It is very possible to occur primarily in digital evidence obtained from an automatic process or output of an application.

However, there are things that still have not been much studied by the researchers, namely the importance of security on law enforcement/digital investigator infrastructure itself. Workstations or computers from the investigators are likely to connect to the Internet, either for the benefit of the acquisition and analysis of digital evidence, communication between law enforcement/investigator, for the purpose of case management, or accessing other sources. This, according to Thorpe [35] is open possibility of attacks or malware infection against the system. This risk should be taken into account by network managers in the law enforcement infrastructure.

It is in line with the opinion of Casey [36] that network-based attacks are now a major challenge for security on a number of strategic infrastructures in governments, healthcare, financial, electrical scope, and law enforcement. This statement is supported by the data from Moen (2007) as cited by [37] that nearly 80% of the web-based applications on several strategic infrastructures located in government institutions have vulnerabilities to attacks particularly cross-site scripting and SQL injection.

Furthermore, according to [38], the most important thing in digital forensics is to maintain the integrity of digital evidence. Preserving the integrity of digital evidence is a critical issue in digital forensics activities. To this end, [38] proposed a model as a framework for ensuring secure transmission of digital evidence from acquisition until storing it in a digital evidence database.

Related to trust issues, there are four terms that are almost the same but have different meanings, namely Trusted Networks, Trusted Computing, Trusted Computing Based, and Trustworthy Computing. Trusted Networks are all networks protected behind a firewall setting, which is the network in a security perimeter that has been created and protected. In this group, there are also other conditions known as Semi Trusted, Untrusted, and Unknown Networks. Semi Trusted is a network that allows access to certain services such as DNS and proxy but not for access to confidential or important information. Untrusted Network is a network that is outside the range of a security perimeter and beyond people's control, while Unknown Network is a network that is neither trusted nor untrusted. In this case, by default, all untrusted networks are unknown networks.

Trusted Computing is a set of technical specifications and guidelines issued by TCPA that include secure input and output, memory, sealed storage, and remote attestation. Trusted Computing is a technology built by the Trusted Computing Group. Through Trusted Computing, computer system will always be running consistently as expected, and the security of the activities is guaranteed with the support of hardware and software.

Trusted Computing Group (TCG) defines trust as "*the expectation that a device will behave in a particular manner for a specific purpose*" [39]. According to [40], trust is a "*degree of confidence*"; something is said to have gained the trust (trustworthiness) of people, organizations, applications, and systems when it meets the expectation as the service provided. Trust is an issue that is important in everyday life; trust will involve the management of various types of risk. A similar case also happens in computer systems and networks. Fisher [40] mentions that the use of authentication methods (*e.g.*, passwords, tokens, biometrics), digital signatures, cryptography, and identity management is a series of security mechanisms needed to get the trust in a computer system and network. However, it is not fully able to replace the trust with the provider, the quality or the functionality of the service itself.

Considering hardware solution to the security problem as an immediate need, in 1999 a number of large companies (i.e. Compaq, Hewlet-Packard, IBM, Intel, and Microsoft) formed Trusted Computing Platform Alliance (TCPA) as an initiation to establish new standards for the computer industry. The goal was to build standard for trusted clients (PC, PDA, Telephone, etc.) so applications that run over the network, telecommunication or e-commerce are trustworthy. This standard will be open in order to enhance the public's confidence and trust to use the platform. The terms of trustworthy computing and trusted computing have a different meaning. According to [41], a system may have trustworthy characteristics, but not trusted, and vice versa. Trustworthy Computing aims to build consumer confidence in computers, by making computers more reliable, more widely used and widely accepted.

Furthermore, [42] added that a system is said to be secure if it can anticipate these four categories of computer threats, as the followings:

- Interception, the availability of information to external parties that do not have authority to access it. External parties here can be a person, program or system.
- Interruption, which is the loss of connection to the main service system, both physically (*e. g.*, broken cable connections) or non-physically (*e.g.*, loss of connection to the main resource).
- Modifications, that is a modification to the system either directly or indirectly visible.
- Fabrication, the addition of objects from the party who has not had authority.

Meanwhile [39] says a system is found as having a trust if it meets three criteria, namely:

- Protected capabilities, there is a set of commands that have exclusive permission to access a specific location where sensitive data are stored or the location where a particular activity can be done.
- Integrity measurement, *i. e.*, the presence of metrics in the platform characteristics that contains things affecting the integrity of the platform.
- Integrity reporting is used for informing the specific storage location of integrity measurements as well as providing an authentication endorsement from the stored value based on trusted platform identities.

Based on the explanation above, issues of secure and trusted in digital forensics are vital to maintaining the authenticity and the integrity characteristics of digital evidence. The existence of physical attacks either in the form of illegal use or unauthorized access to the digital forensics environment will cause changes in the authenticity and the integrity of digital evidence. This is similar to numerous attempts of computer attacks either through malware and trojans, vulnerability or bugs and errors in an application; those will reduce the authenticity and the integrity of digital evidence. This will be a challenge in dealing with secure and trusted environment issues in digital forensics.

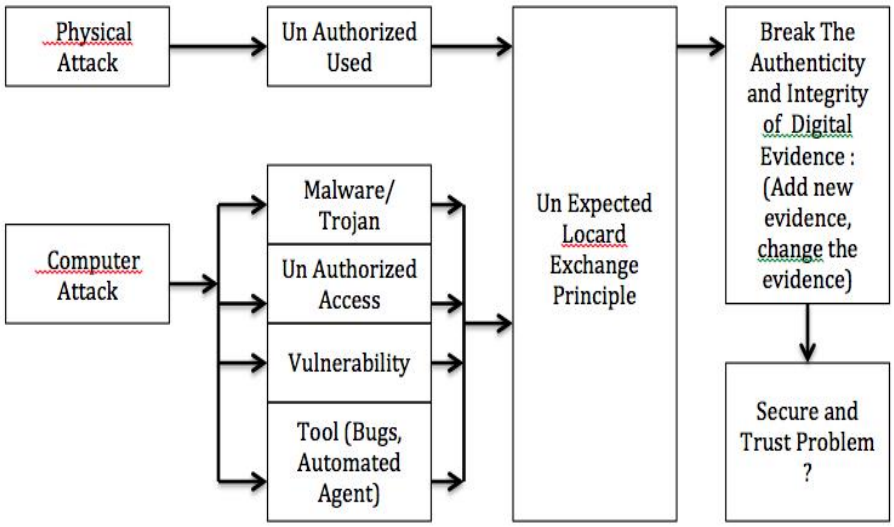

Figure 1 An Illustration of Authenticity and Integrity Problem in Digital Evidence

Figure 1 shows that after the acquisition process of digital evidence, the presence of physical or computer attacks on a computer system, investigator's system, or law enforcement system will trigger the emergence of a new trace as a consequence of the application of the Locard Exchange Principle. The addition of this new trail will certainly

have an impact on the change in the authenticity and the integrity of digital evidence. Therefore, a proper concept is required to keep and to preserve the authenticity and the integrity of digital evidence by protecting the evidence in a secure and trusted environment.

4. Proposed Strategy

Issues about the importance of a solution for secure and trusted system in a critical infrastructure has been discussed by [43] through cyber-physical security system (CPS Security). The proposed framework is through the approach of the three control fields namely: information field, controlling field and CPS risk assessment. The framework focuses on networked integrates computational resources into physical processes. The Framework cannot be specifically implemented in digital forensics environment because of more emphasis on interconnected between the physical components to improve the physical performance. Trusted issue is not addressed in that framework.

An environment that supports digital forensics activities must be guaranteed to meet the criteria of secure and trust characteristics. The proposed solution to meet those criteria is to apply trusted computing-based concept. In this sense, [40] reveal that trusted computing-based can serve as a solution to security problems of in the computer industry; even, through a project funded by Software Engineering Institute's Independent Research, a trusted computing has been proposed as a foundation for cybersecurity infrastructure.

Although there are multiple meanings of trusted computing-based, the one used in the this paper is the meaning as proposed by [41], that is, a unity of the aspects of hardware, software and procedural components that will guarantee the implementation of security policy. In other words, attackers can only penetrate a system when they have successfully taken down all of its security components. A system will only be able to implement Trusted Computing Base when there are awareness and cooperation from all the components involved in the system, either hardware, software, or human who runs security policy and operates the computer device.

In previous research, [37] have suggested five aspects as a strategy to increase security in mobile application-based eGovernment; those five strategies are selection of data and services, the appropriate policy, adoption of technology and the human education aspect. Next, [44] also proposed a strategy to improve a secure and trusted environment in the eGovernment system through 5 unit components, namely security and standard, security policy, trusted computing, defense-in-depth strategy and human factor. Strategy defense in e-Government is extremely important given that the eGovernment service frequently serves as a target for attacks from hackers or of cybercrime perpetrators.

Based on the concept described previously in [37] and [44], to satisfy the concept of a secure and trusted environment in digital forensics, an approach is suggested using five components, namely Security Standard And Forensics Policy, Security Policy, Model and Trust System, Trusted Computing, Secure Channel Communication and Human Factor. These five components are selected based on the following consideration:

4.1. Security Standard and Forensics Policy

Priyambodo [44] have cited the opinion of [45] regarding the importance of a policy within an institution. In this case, there are two main things in the importance of a policy, namely: being a guideline to communicate the primary goal of an institution that contains a set of basic principles as a reference for the technical and operational level; providing an overview of culture and value built into the institution. To support the concept of a secure and trusted environment, there are at least two aspects of policy, namely security standard

and forensic policy. Standard is the highest level of a policy that denotes transparency to the public and ensures that all the process undertaken in the institution have referred to the provisions. According to [46], using the standard will ensure a secure and trusted environment because it includes procedures, controls, and evaluations at every stage as well as the parties involved in the activities of digital forensics.

Meanwhile, [47] define a forensics policy as closely related to forensics readiness. Forensics policy and forensics readiness are policies that will encourage an institution to undertake activities which will ensure a minimum cost and maximum environment ability to get digital evidence. Thus, every data that is potential to be digital evidence and complies with behavior system and business model of the institution should be recorded and stored properly.

In a digital forensics process, a case investigation will be much easier to do when such a case occurs in an institution that has forensics readiness policy issued. This is because all necessary things in the investigation process will be provided. On the contrary, investigation processes will be much more difficult to do when the case occurs in an institution that does not have forensics readiness because the digital data and evidence required are not recorded, noted, and stored systematically. Thus, the institution that performs digital forensics processes needs to issue forensics policy and forensics readiness so that when a problem appears it can be easily tracked down since of all the activities in the system have been recorded, noted, and stored properly.

4.2. Security Policy, Model and Trust System

A secure environment is strongly influenced by how security policy, security model, as well as trust management system is applied. In general, security policy is a set of statements and requirements of a system behavior that will ensure the realization of a secure system. Bishop (2004) in [47] argues that security policy is a statement that clearly specifies what should and what should not be in the sphere of security. On a lower level, security policy will include a set of policies about authority and secure states.

Furthermore, Clark and Wilson (1987) in [47] states that in the scope of law enforcement, security policy must also include policies about confidentiality of classified data. In this case, all classified data/information should be protected and only certain level users who have the right to access such data and information. Moreover, the policy must mention the rules and obligations that bind users who utilize the classified data.

Security Model is an abstraction that provides a conceptual language used by the administrator to implement the security policy. Commonly, security model will define the hierarchy of access or modification of rights that can be held by the users of the institution. Meanwhile, Trust Management System is a framework to decide whether the security policy expressed in logic and abstraction as well as implemented through programming or setting system has been completely in accordance with the policy that should be followed. Trust management system is run through policy language and compliance checker.

4.3. Trusted Computing

Priyambodo [44] have discussed the importance of Trusted Computing as a security solution that is hardware based. In this case, through the Trusted Computing system, a computer will always work consistently as expected, and the security of its activities is guaranteed with hardware and software support. Trusted computing approach is necessary because the current software approach applied as part of a security solution still possess a number of security gaps for certain parties. The approach undertaken by TCG begins with introducing the concept of "chain of

trust" from a system. In this concept, when a system starts booting activity, the chain of trust of modules that are uninterrupted are activated and perform its functions as checking stable security reference. If no problem is found, system activities will continue to the next level and so on so that every transaction and communication of data is trusted, reliable, secure and protected. During the implementation, according to [48], trusted computing would be supported by three main components, *i.e.*, Trusted Platform Module (TPM, Core Root Trust for Measurement (CRTM) and TCG Software Stack (TSS).

4.4. Secure Channel Communication

Two of the characteristics of digital workers are mobility and connectedness. Based on the opinion of [49], from the institutional viewpoint, digital workers must be facilitated through a secure connection mechanism via authentication and encryption that will protect existing information assets of the institution. Furthermore, [50] revealed that an example of digital workers is the first responders who are directly related to the crime scene. In certain situations, the first responders should mobilize quickly and at the same time, they still need to access the internal system.

According to [50], the infrastructure that supports the activities of police, firemen, and medical practitioners belong to the infrastructure that must be completely safeguarded. The use of commercial networks and public networks is a very risky option for such infrastructures. Thus, based on an internal study, [50] suggest the use of encrypted channels, especially virtual private networks (VPNs) as a solution to the infrastructures. Furthermore, [51] believe the implementation of a VPN through IPSec and SSL can be applied based on specific interests. For such cases, the use of a VPN technology either through SSL or IPSec protocol can provide a solution to fulfill the requirements of secure communication. Based on the characteristics, IPSec is more appropriate to used in connection link between law enforcement offices, which are co-located site-to-site, while SSL VPN can be used as a solution to the needs of remote access to support mobility of the first responders/digital investigators.

4.5. Human Factor

In any given system, human factor is the key factor in determining the success of system implementation. This is called as linking the human factor [42]. Even Mitnick and Simon (2002) in [52] states that "*Humans are the weakest connection in information security*". That is why human factor contributes to the emergence of system vulnerability that results in lower environment security. Human error; bad behavior in interacting with the system; low level of skill, knowledge and education emerge the gap that leads to human factor vulnerability.

In addition, [53] found the lack of knowledge and technology of human resources of law enforcement, and this has also posed some security problems mainly in information technology infrastructures. Unfortunately, all attempts done by each institution to enhance security are concentrated on hardware and software rather than peopleware. Therefore, there should be a mechanism in institution to focus on the handling of peopleware as a unity in the efforts to increase security and trust from the environment. Then, [54] suggest that efforts to improve security should be followed by increased feedback from human factor. The feedback can be obtained through various means, namely through modeling to determine the characteristics of the human factor in a security system.

These five components are proposed as a unified strategy to realize a secure and trusted environment to keep the authenticity and the integrity of digital evidence and

digital forensics activities. The interconnectedness of all five components can be seen in Figure 2.

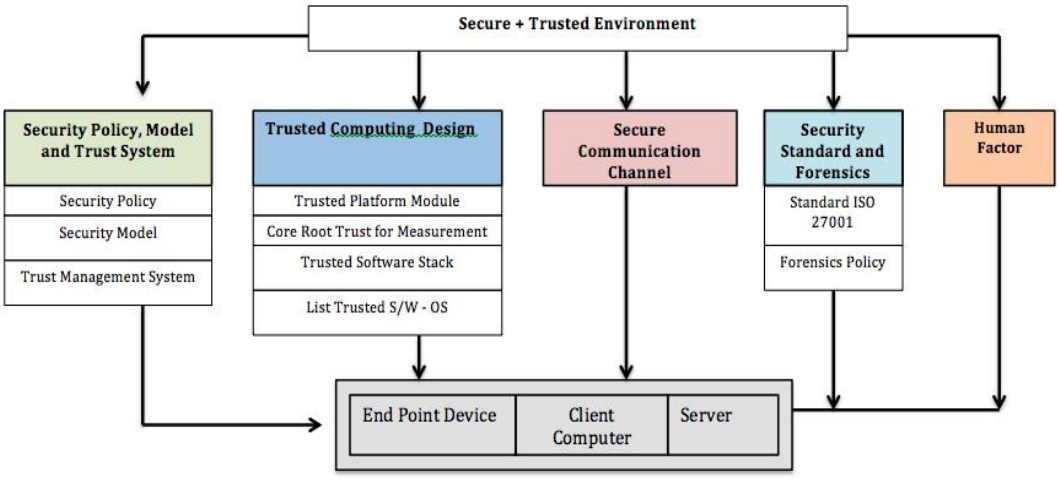

Figure 2. Secure and Trust Environment Strategy

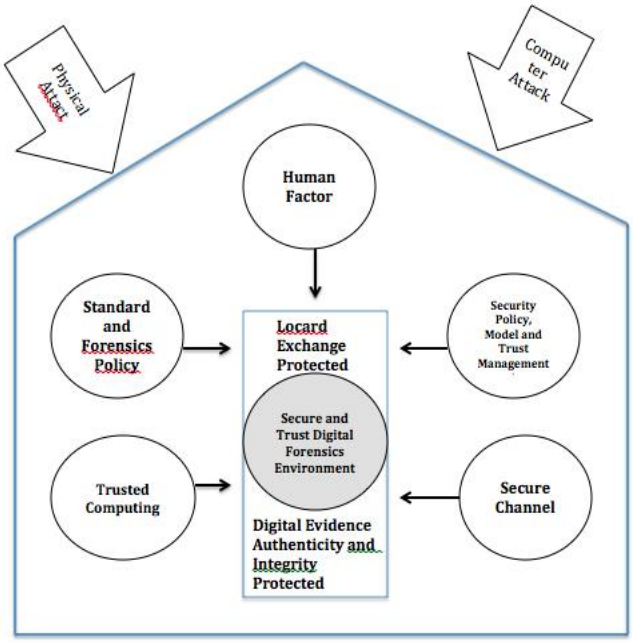

Figure 3 Secure and Trusted Environment Concept

5. Discussion

The concept of a secure and trusted environment cannot be realized solely in one solution but rather in an integrated unity. In this paper, five components are proposed as a strategy to realize a secure and trusted environment to maintain the authenticity and the integrity of digital evidence in digital forensics activity. The unity of the five components can be explained through an illustration in Figure 3.

Based on the illustration in Figure 3, the five components as a base for a secure and trusted environment will be able to preserve the authenticity and the integrity of digital evidence. In this case, all aspects that will be potential for the occurrence of changes in the authenticity and the integrity of digital evidence have been protected by implementing those five components. Thus, there will be no hesitation of all

parties in question regarding the activities of digital forensics. They are convinced with secure and trust characteristics in the digital forensics environment.

Conceptually, the five proposed components have the ability in performing detection and prevention toward the occurrence of four security threats as expressed by [42] as well as satisfying the three criteria of trust as suggested by [39]. The five proposed components principally would prevent the occurrence of security threats as well as meeting the criteria of trusted system through both technical and conceptual approach and standard policy.

The strategy that has been proposed is a common strategy that can be applied in an environment of digital forensics. This strategy is necessary, in particular, to handle digital evidence in a series of digital forensics activities. These five components is a comprehensive step to realizing a secure and trusted environment. Thus, it is safe to say that any activity that will cause changes in the integrity and authenticity of digital evidence is not going to happen. Handling digital evidence that is not supported by a secure and trusted environment will potentially bring unexpected interaction with digital evidence. A system that is not secure and trusted will cause the application of the principle Locard Exchange Principle (LEP) in digital forensics environment and will impact on the change of the integrity and the authenticity of digital evidence.

Based on the explanation, the role of a secure and trusted environment to maintain the authenticity and the integrity of digital evidence is shown in Figure 4.

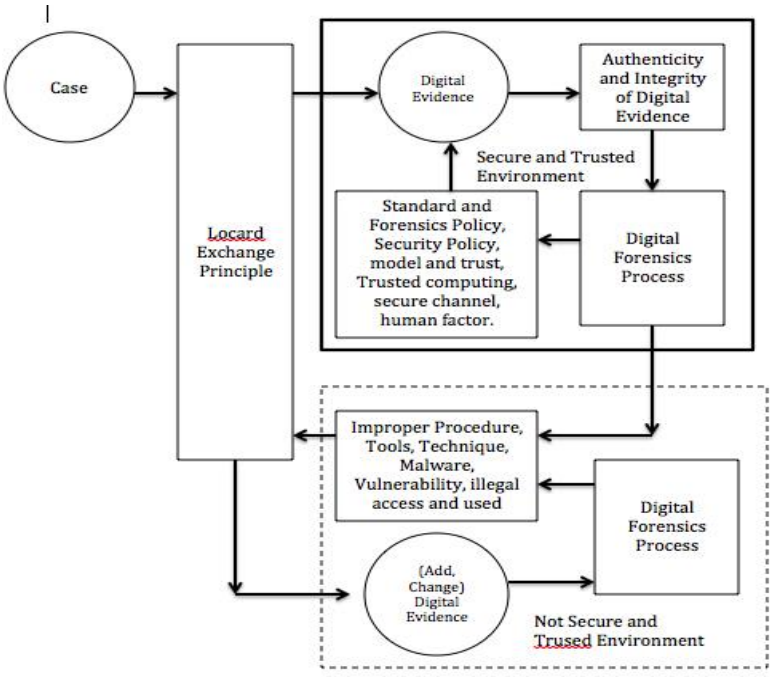

Figure 4 Secure and Trusted Environment for Maintaining Integrity and Authenticity of Digital Evidence

Through a secure and trusted environment strategy, it is expected that all parties associated with the handling of digital evidence will have the confidence that all processes related to the handling of digital evidence is done by someone who has the integrity and the competence of the appropriate expertise (human factor), in a security system with good authentication and authorization mechanism (security model), using a number of applications, tools and devices that are reliable (trusted computing), using secure communication and secure infrastructure (secure

communication) following a standard procedure and forensics activities (standard and policy).

Among those five components, two of them are hardware and software based (*i.e.*, trusted computing and secure channel communication), while the other three components are conceptual based, (*i.e.*, standard and forensics policy, security policy, model and trust management system and human factor). The five components of the strategy proposed in this paper is a recommendation. Ideally, all five components should be implemented to realize the concept of a secure and trusted environment in digital forensics. However, in case of not all five are feasible, at least one of the hardware and software based components, and one of the conceptual based components should be implemented. Secure channel communication and human factor component are recommended as the minimum strategy to reach the minimum level of a secure and trusted environment of digital forensics. Both are selected as the minimum strategy because some of the basic aspects of secure channel communication (for example, the use of SSL VPN) coupled with the fulfillment of some aspects of human factor will already improve the level of security and trust in an digital forensics environment.

6. Conclusions and Further Research

One important issue in the field of digital forensics is to maintain the authenticity and the integrity of digital evidence. In other perspectives, the authenticity and the integrity are directly related to the application of the Locard Exchange Principle (LEP), which is a basic principle in the handling of digital evidence which reads: Every contact between two different parties will definitely leave a new trace. Errors in the process of handling digital evidence that has been obtained, system vulnerability, and/or digital forensics environment can lead to the presence of new traces as digital evidence. Besides, a number of potential physical and computer attacks on the computer system used by investigators or law enforcement will emerge new traces that will reduce the authenticity and the integrity of digital evidence. In the implementation, all activities accessing the digital evidence are not likely to occur in the absence of a mediation, such as a set of instruments or applications. Therefore, investigator should be able to ensure that whatever they do with the digital evidence will not tamper its authenticity and integrity.

The solution proposed in this paper is to run a secure and trusted environment strategy. This strategy is the development concept that is proposed earlier by [37] and [44]. The proposed strategy includes five components, namely: standard and forensics policy, security policy, model and trusted management system, trusted computing, secure channel communication, and human factor. Those five components of strategy proposed in this paper are only a recommendation. Ideally, those components should be implemented to realize a secure and trusted environment concept in digital forensics. In the case of not all components can be satisfied, there have to be one of the hardware and software based components and one conceptual based component to be implemented. Secure channel communication and human factor components are the minimum strategies that must be carried out for satisfying the minimum level of a secure and trusted environment of digital forensics.

References

[1] F. Cohen, Digital Forensic Evidence Examination, 5th Edition, no. c. 2013, p. 517.
[2] J. Cosic and M. Baca, "(Im) Proving Chain of Custody and Digital Evidence Integrity with Time Stamp," in MIPRO,Proceedings of the 33rd International Convention International Conference, 2010, no. Im, pp. 1226 – 1230.
[3] S. Raghavan and S. Raghavan, "The Digital Forensic Landscape," SecureCybers, pp. 1–9, 2012.

[4] K. Zatyko and J. Bay, "The Digital Forensics Cyber Exchange Principle," Forensics Magazine, 2011. [Online]. Available: http://www.forensicmag.com/articles/2011/12/digital-forensics-cyber-exchange-principle.
[5] M. G. Kirschenbaum, R. Ovenden, and G. Redwine, Digital Forensics and Born-Digital Content in Cultural Heritage Collections, no. December. Washington DC: CLIR publication, 2010, p. 101.
[6] Y. Prayudi and Azhari, "Digital Chain of Custody : State Of The Art," IJCA, vol. 3, no. 1, pp. 1–8, 2015.
[7] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody," Int. J. Comput. Appl., vol. 109, no. 9, pp. 30–36, 2014.
[8] M. Burmester, "A trusted computing architecture for critical infrastructure protection," in 4th International Conference On Information, Intelligence, Systems and Applications (IISA), 2013, pp. 1–6.
[9] I.-L. Lin, Y.-S. Yen, and A. Chang, "A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime," in Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011, pp. 543–548.
[10] N. Kshetri, The Global Cybercrime Industry. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, p. 267.
[11] J. E. Davis, "Computer Forensics in IP Theft Litigation and Investigations," New York, USA., 2011.
[12] A. Agarwal, M. Gupta, and S. Gupta, "Systematic Digital Forensic Investigation Model," Int. J. Comput. Sci. Secur., vol. 5, no. 1, pp. 118–134, 2011.
[13] S. Rao, "Hacktivism Trends , Digital Forensic Tools and Challenges : A Survey," in IEEE Conference on Information and Communication Technologies (ICT 2013), 2013, no. Ict, pp. 138–144.
[14] R. Broadhurst, P. Grabosky, M. Alazab, and S. Chon, "Organizations and Cyber crime : An Analysis of the Nature of Groups engaged in Cyber Crime," Int. J. Cyber Criminol., vol. 8, no. 1, pp. 1–20, 2014.
[15] A. Alazab, J. Abawajy, M. Hobbs, R. Layton, and A. Khraisat, "Crime Toolkits: The Productisation of Cybercrime," in 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 1626–1632.
[16] M. A. Tariq, J. Brynielsson, and H. Artman, "Framing the Attacker in Organized Cybercrime," in European Intelligence and Security Informatics Conference Framing, 2012, pp. 30–37.
[17] D. J. Neufeld, "Understanding Cybercrime," in 2010 43rd Hawaii International Conference on System Sciences, 2010, pp. 1–10.
[18] M. Pollitt, "A History of Digital Forensics," in Advances in Digital Forensics VI, K.-P. Chow and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 3–15.
[19] M. Damshenas, A. Dehghantanha, and R. Mahmoud, "A Survey on Digital Forensics Trends," Int. J. Cyber-Security Digit. Forensics, vol. 3, no. 4, pp. 209–234, 2014.
[20] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, and N. F. Binti, "Digital Forensic Trends and Future," Int. J. Cyber-Security Digit. Forensics, vol. 2, no. 2, pp. 48–76, 2013.
[21] A. O. Flaglien, "Cross-Computer Malware Detection in Digital Forensics," Gjovik University Collage, 2010.
[22] J. Richter and N. Kuntze, "Securing Digital Evidence," in Fifth International Workshop on Systematic Approaches to Digital Forensic Engeneering, 2010, pp. 119–130.
[23] A. R. Gonzales, R. B. Schofield, and D. W. Hagy, "Digital Evidence in the Courtroom : A Guide for Law Enforcement and Prosecutors," 2007.
[24] S. Raghavan, "Digital forensic research: current state of the art," CSI Trans. ICT, vol. 1, no. 1, pp. 91–114, Nov. 2012.
[25] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digit. Investig., vol. 7, pp. S64–S73, Aug. 2010.
[26] S. Dossis, "Semantically-enabled Digital Investigations," Master, Department of Computer and Systems Sciences, Stockholm University, Swedia, 2012.
[27] K. Shanmugam, "Validating Digital Forensic Evidence," Brunel University Uxbridge, UK, 2011.
[28] J. Ćosić, Z. Ćosić, and M. Bača, "(Il) Legal Aspects of Digital Antiforensic," in The 22nd Central European Conference on Information and Intelligent Systems, 2011, vol. 147, no. Il, pp. 147–151.
[29] C. Valli and M. Brand, "The Malware Analysis Body of Knowledge (MABOK)," in The 6th Australian Digital Forensics Conference, 2008.
[30] S. Rekhis, "Theoretical Aspects of Digital Investigation of Security Incidents," Engineering School of Communications, Tunisia, 2007.
[31] S. Saleem, O. Popov, and R. Dahman, "Evaluation of Security Methods for Ensuring the Integrity of Digital Evidence," in International Conference on Innovations in Information Technology, 2011, pp. 220–225.
[32] R. Accorsi, "Safekeeping Digital Evidence with Secure Logging Protocols : State of the Art and Challenges," 2009 Fifth Int. Conf. IT Secur. Incid. Manag. IT Forensics, no. 1, pp. 94–110, 2009.
[33] C. Hsu and Y. Lin, "A Digital Evidence Protection Method with Hierarchical Access Control Mechanisms," in IEEE International Carnahan Conference on Security Technology (ICCST), 2011, pp. 1–9.
[34] M. Wojcik, H. Venter, J. Eloff, and M. Oliver, "Applying Machine Trust Models to Forensics Investigations," in IFIP Advances in Information and Communication Technology, 2006, pp. 55–65.

[35] S. Thorpe, "An Experinmental Survey Towards Engaging Trustable Hypervisor Log Evidence Within a Cloud Forensics Environment," Int. J. Comput. Sci. Inf. Technol., vol. 4, no. 6, pp. 125–141, 2012.
[36] E. Casey, Digital Evidence and Computer Crime. London, UK: Elsevier Academic Press, 2011, p. 590.
[37] T. K. Priyambodo and Y. Prayudi, "Information Security Strategy on Mobile Device Based eGovernment," ARPN J. Eng. Appl. Sci., vol. 10, no. 2, pp. 652–660, 2014.
[38] Y. Zhang and Y. Lin, "Research on the Key Technology of Secure Computer Forensics," in 2010 Third International Symposium on Intelligent Information Technology and Security Informatics, 2010, pp. 649–652.
[39] M. Burmester and J. Mulholland, "The Advent of Trusted Computing : Implications for Digital Forensics," in SAC, 2006, pp. 23–27.
[40] D. A. Fisher, J. M. Mccune, and A. D. Andrews, "Trust and Trusted Computing Platforms," 2011.
[41] M. Amin, S. Khan, T. Ali, and S. Gul, "Trends and Directions in Trusted Computing : Models , Architectures and Technologies," in International Multiconference Of Engineers and Computer Scientist, 2008, vol. I, pp. 19–21.
[42] T. Nikolakopoulos, "Evaluating the Human Factor in Information Security," University of Oslo, 2009.
[43] P. Dong, Y. Han, X. Guo, and F. Xie, "A Systematic Review of Studies on Cyber Physical System Security," Int. J. Secur. Its Appl., vol. 9, no. 1, pp. 155–164, 2015.
[44] T. K. Priyambodo and Y. Prayudi, "A Proposed Strategy for Secure and Trusted Environment in eGovernment," IJEGR, vol. 10, no. 1, 2015.
[45] K. Wada and P. King, "IT Policy: An Essential Element of IT Infrastructure," Educause Review, no. June, pp. 14–15, Jul-2001.
[46] C. Gikas, "Information Systems Security : A General Comparison of FISMA , HIPAA , ISO 27000," 2010.
[47] C. Taylor, B. Endicott-Popovsky, and D. a. Frincke, "Specifying digital forensics: A forensics policy approach," Digit. Investig., vol. 4, pp. 101–104, Sep. 2007.
[48] D. Schellekens, "Design and Analysis of Trusted Computing Platforms," Katholieke Universiteit Leuven, 2012.
[49] S.-H. Sun, "The advantages and the implementation of SSL VPN," in 2nd IEEE International Conference on Software Engineering and Service Science (ICSESS), 2011, pp. 548–551.
[50] A. R. McGee, M. Coutière, and M. E. Palamara, "Public Safety Network Security Considerations," Bell Labs Tech. J., vol. 17, no. 3, pp. 79–86, Dec. 2012.
[51] Y. Prayudi and A. Ashari, "A Study on Secure Communication for Digital Forensics Environment," Int. J. Sci. Eng. Res., vol. 6, no. 1, pp. 1036–1043, 2015.
[52] S. Soltanmohammadi, S. Asadi, and N. Ithnin, "Main Human Factors Affecting Information System Security S," Int. J. Contemp. Res. Bus., vol. 5, no. 7, pp. 329–354, 2013.
[53] F. Cohen, "The State of the Art and What We are Missing," in 1st Chinese Conferemce on Digital Forensics, 2012, pp. 1–21.
[54] J. J. Gonzalez and A. Sawicka, "A Framework for Human Factors in Information Security," in WSEAS International Conference on Information Security, Hardware/Software Codesign, E-Commerce and Computer Networks, 2002, pp. 1871–1877.

Authors

Yudi Prayudi, currently he is a PhD Student at Department of Computer Science and Electronics Gadjah Mada University and also senior lecturer at Department of Informatics Universitas Islam Indonesia Yogyakarta, Indonesia. His research interests include digital forensics, cybercrime, watermarking, steganography, malware analysis and network security.

Dr. Tri Kuntoro Priyambodo, M.Sc., currently he is an Associtate Professor at Department of Computer Science and Electronics Gadjah Mada University. He is a member of IEEE. He is also hold a position as a Secretary of Satellite and Aerospace Electronics Research Group, Gadjah Mada University. His research interests include Computer Network Security, eGovernment Systems, and Autonomous Unmaned Systems.