Chapter

A Model for Auditing Smart Intrusion Detection Systems (IDSs) and Log Analyzers in Cyber Physical Systems (CPSs)

Joshua Ojo Nehinbe

Abstract

Suitable models that auditors can adopt to concurrently audit smart Intrusion Detection Systems (IDSs) and log analyzers in Cyber Physical Systems (CPSs) that are also founded on sound empirical claims are scarce. Recently, post-intrusion studies on the resilience of the above mechanisms and prevalence of intrusions in the above domains have shown that certain intrusions that can reduce the performance of smart IDSs can equally overwhelm log analyzers such that both mechanisms can gradually dwindle and suddenly stop working. Studies have also shown that several components of Cyber Physical Systems have unusual vulnerabilities. These key issues often increase cyber threats on data security and privacy of resources that many users can receive over Internet of a Thing (IoT). Dreadful intrusions on physical and computational components of Cyber Physical Systems can cause systemic reduction in global economy, quality of digital services and continue usage of smart toolkits that should support risk assessments and identification of strategies of intruders. Unfortunately, pragmatic studies on how to reduce the above problems are grossly inadequate. This chapter uses alerts from Snort and C++ programming language to practically explore the above issues and further proposes a feasible model for operators and researchers to lessen the above problems. Evaluation with real and synthetic datasets demonstrates that the capabilities and resilience of smart Intrusion Detection Systems (IDSs) to safeguard Cyber Physical Systems (CPSs) can be improved given a framework to facilitate audit of smart IDSs and log analyzers in Cyberspaces and knowledge of the variability in the lengths and components of alerts warned by Smart Intrusion Detection Systems (IDSs).

Keywords: intrusion, Intrusion Detection Systems (IDSs), Network Intrusion Detection System, smart IDSs, IDS audit, IS auditor, Cyber Physical Systems (CPS)

1. Introduction

Pragmatic studies have recently shown that Cyber Physical Systems (CPSs) must be adequately protected with security tools to reduce the rising cases of Cyber Physical attacks and the destructive impacts of these attacks on global economy, international security, digital services and means of livelihood of many ethnic and social groups across the globe [1–3]. Further studies have shown that components

of Cyber Physical Systems (CPSs) possess individual vulnerabilities that can endanger continuous usage of Cyber Physical Systems (CPSs) [4, 5]. The nature of the problems with different kinds of threats and cyber attacks on Cyber Physical Systems (CPSs) can correlate to severe disasters and complex confusion that may involve different stakeholders. The motives of some intruders may be complex to understand if they simultaneously attack the seamless integration of physical components and the computational elements of Cyber Physical Systems (CPSs) [6]. The impacts of some successful cyber attacks in this domain may corrupt or damage Cyber Physical data [2, 7]. Some intrusions can leak sensitive information to wider audience via social media with the aims to extort and discredit victims and service providers of Cyber Physical Systems (CPSs) [2].

The complexity and reoccurrence of threats and cyber attacks on the entire components of Cyber Physical Systems (CPSs) have made many organizations to develop the habit of deploying several categories of Intrusion Detection Systems (IDSs) within the peripherals and gateways of their connections to the entire Cyber Physical systems (CPSs) so that these devices can collect and analyze activities that signify evidence of intrusions against their corporate networks in real-time [8, 9]. Subsequently, analysts can quickly review the reports and respond to the attacks before the attacks achieve the objectives of intruders that launch them [10]. These issues have inevitably generated several challenges and concerns regarding the effectiveness of IDSs and analyzers of logs of IDSs in monitoring complex architectural systems peculiar to the above domains over the years. **Figure 1** illustrates Network Intrusion Detection System (NIDS) that is located in front of a firewall.

In other words, **Figure 1** demonstrates one of the two approaches organizations can adopt to position Network Intrusion Detection System (NIDS) in relation to firewall within the peripherals and gateways that connect them to the entire Cyber Physical Systems (CPSs) [7, 8]. Nevertheless, numerous studies often attest that Intrusion Detection Systems (IDSs) must always be upgraded to strongly help operators control the new dimensions and rising waves of intrusions against cyber physical resources across the globe. One of the pragmatic methods to achieve this security objective is to make IDSs smarter by connecting them to the Global Systems of Mobile (GSM) communication so that the toolkits can always send alerts to remote operators such that operators can promptly respond to cyber attacks at all time [11]. Thus, smart IDSs are IDSs that are configured such that operators can

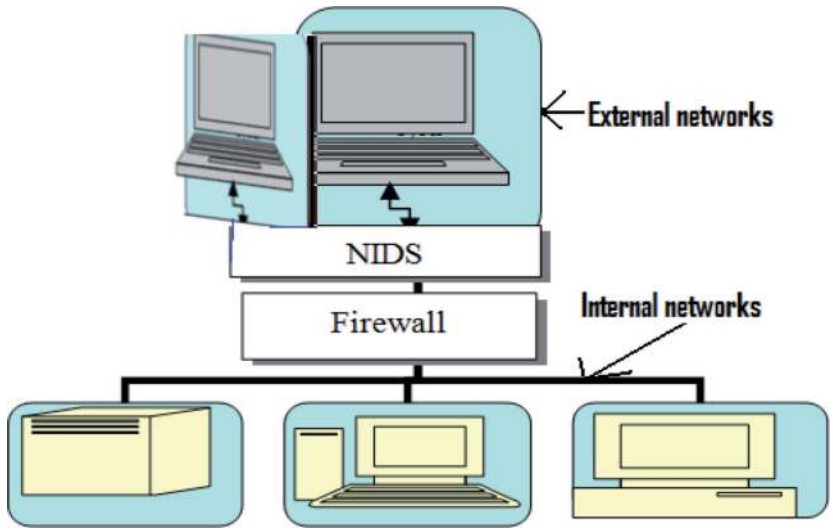

Figure 1.
NIDSs in front of firewall.

receive and respond to their alerts through Short Message Services (SMS) to the GSM or email addresses of the operators of IDSs in Cyber Physical Systems (CPSs). However, there are security and business requirements that underpin the framework upon which smart IDSs reside in private and corporate settings [2, 12]. The resilience and capacities of smart IDSs can be improved if operators can combine the information they gather from audit of log analyzers with the knowledge of the variability of lengths and components of alerts that smart Intrusion Detection Systems (IDSs) in the networks have generated. This can be used to ultimately design and improve the security policy on smart IDSs in the corporate elements of Cyber Physical Systems (CPSs) [3, 7, 13]. However, empirical studies on smart IDSs that specifically focus on audit of smart IDSs and log analyzers are inadequate over the years.

Basically, empirical studies on smart IDSs in the context of Cyber Physical Systems (CPSs) involve pragmatic examinations of specific experiments conducted with smart IDSs to concurrently correct security concerns and audit issues. These procedures can assist operators to improve the detection of intrusions against Cyber Physical Systems (CPSs) and cloud resources at large. The argument underpinning this chapter is that logs of smart IDSs should be concurrently audited during IDS audit. Otherwise, they may not be very useful for post-intrusion reviews. Similarly, lack of audit of logs of smart IDSs may render them ineffective for in-house training of newly recruited auditors and researchers exploring issues on identification, analysis, corroboration and mitigations of threats and security lapses in Cyber Physical Systems (CPSs) [5, 8].

Furthermore, smart IDSs are well-known for generating large quantities of alerts whenever they are configured to detect possible intrusions against Cyber Physical Systems (CPSs) [9, 11, 14]. It is inefficient to manually analyze massive alerts without incurring huge overheads and tradeoffs. Hence, data mining is often recommended as an underlying concept to automate tools that can reduce workload due to alerts from smart IDSs [14]. Another central issue here is that some companies use the reports obtained from the logs of smart IDSs to augment their networks security policies [8, 15, 16]. The necessity to audit smart IDSs alongside with log analyzers is not mandatory in the existing models for auditing Information Technology (IT). This generic audit framework seems to subsume IDS audit into security policy on computers and telecommunications [15, 17]. This weakness may eventually lead to lack of segregation of duties among internal auditors, IDS researchers and IDS operators. The human elements of the Cyber Physical Systems (CPSs) may place emphasize on Firewall and other forms of the Intrusion Prevention Systems (IPSs) over smart IDSs in the context of the organizational settings in the above settings. Moreover, it is plausible that some logs of regular IDSs that were archived might be relatively uninteresting details. One of the three central issues here is that the IDSs may be configured to send raw alerts to the mobile devices of the operators to analyze. This means that certain log analyzers that can analyze short messages must be installed in the Mobile phones of the operators of smart IDSs. Alternatively, remote log analyzers can send short text messages that indicate processed alerts of smart IDSs to the operators. Whichever the case, it is imperative to also audit programs that analyze logs of smart IDSs in Cyber Physical Systems (CPSs) to regularly establish the degree of information inherent in the archived logs at each time and to ascertain the patterns of packets intended to overload smart IDSs at certain period of time in the above settings [8].

Findings suggest that suitable realistic datasets that can be used to concurrently audit smart IDSs and logs analyzers are grossly inadequate for researchers due to security issues [17, 18]. Accordingly, the above domain of IDS audit in the security of networks and other components of Cyber Physical Systems (CPSs) continues to

suffer a major setback over the years. Therefore, by using alerts from Snort and C++ programming language, this chapter presents a comprehensive review of the above research issues and further proposes a feasible model that professionals can adopt to lessen the problems. One of the significant contributions of this chapter is its ability to practically provide clear review and guidelines that experts and trainees can adopt to ensure perimeter defense of mobile and computer networks. The chapter uses four datasets to practically illustrate a new framework for concurrent auditing of smart IDSs and log analyzers within corporations in the entire Cyber Physical Systems (CPSs). Also, the chapter broadly justifies the importance of conducting audit of log analyzers in smart phones together with IDSs audit. The remainders of this chapter are organized in the following order. Section 2 will present background research work that relates to IDS auditing. Section 3 explains the scope of IDS audit in Cyber Physical Systems (CPSs). Section 4 discusses challenges confronting IDS auditors in auditing Cyber Physical Systems (CPSs). Section 5 provides the proposed methodology for auditing smart IDSs and log analyzers while section 6 concludes the chapter.

2. Background information on audit of smart IDSs and log analyzers in Cyber Physical Systems (CPSs)

Studies have shown that Cyber Physical Systems (CPSs) are mergers of collaborative networks of automatic systems that are strongly built on sound theoretical and scientific principles and seamless integration of many disciplines [1, 6, 12]. Some of the disciplines that contribute to progressive growth and modernize Cyber Physical Systems (CPSs) over the years include informatics, computer and, mobile systems, Wireless Sensor Networks (WSNs), cyberspace, system designs, software, process, robotic, automobile and mechanical engineering [1, 6, 12, 19]. The underlying benefit of incorporating integrated components to drive Cyber Physical Systems (CPSs) is easy connectivity of many devices and systems to Cyber Physical systems (CPSs) across the globe. This capability has resulted into wider applications of Cyber Physical Resources (CPRs) in the areas of medical services, agriculture, electric installations, space engineering and other notable facets of human life [6, 19].

Critical issues begin to surface with the inexhaustible growth currently recorded in this domain in recent years especially on the numbers of service users, service providers and revenue accrued from sales of products and services that relate to Cyber Physical Systems (CPSs) [4]. Empirically, experts have argued that security, computational efficiencies and degree of helpfulness of complex architectural framework that underlying seamless integrations of physical and computation components of Cyber Physical Systems (CPSs) are serious doubts whenever these components are evaluated on the basis of performance, quality of service, users' satisfactions and robustness to counter threats and challenges [5, 20, 21]. Yet, emphasis over the years has focused on the computational capabilities of Cyber Physical Systems (CPSs) but less attention has been paid to the link between the computational and physical elements of this domain [20]. These flaws have raised series of technical and research issues on how to forecast traffic flow, optimize Mobile Cyber-Physical applications and how to achieve high performances of social services and healthcare facilities like wearable devices that run on Internet of a Thing (IoT) [1]. The correlations between social settings and industrial applications of cloud-based services that interact with Cyber Physical Systems' designs; innovation and manufacturing of digital resources continue to generate new paradigms in manufacturing and design's settings [6, 22]. These necessitate the importance of

measures to bridge the gap between the Cyber physical resources and social setting. Collaborative design of embedded systems and various algorithms that experts have designed to carry out co-modeling and co-simulation of novel innovations begin to emerge. However, majority of these algorithms often exhibit invisible flaws [19].

The above issues coupled with the alarming increase of intrusions against Cyber Physical Systems (CPSs) have resulted in the needs for organizations to adopt Intrusion Detection Systems (IDSs) [8, 10, 20]. These toolkits can then provide automated ways to monitor, analyze all incoming and outgoing network packets in their corporate networks, trigger and log alerts on suspicious packets they observe for security and decision purposes. Nevertheless, most of these mechanisms can only detect suspicious packets [9]. They have been criticized for lacking capabilities to make dependable decisions on suspicious activities of users that may signify security breach to Cyber Physical Systems (CPSs) [23]. Operators must carefully review alerts they generate to isolate false positives from realistic attacks. Alerts can be daunting and overwhelmingly difficult to manually analyze by operators. Series of log analyzers have been proposed over the years to compensate for these weaknesses [8, 9]. Studies have shown that significant numbers of log analyzers have limited capabilities required to categorize cyber attacks on the basis of all attributes of alerts [9]. A few numbers of researches has suggested that, the above devices should be upgraded so that they can intimate operators with alerts on real-time basis [11, 20]. The rationale is that operators should be able to remotely analyze intrusion logs and counter attacks on Cyber Physical Systems without the need to physically report to their offices.

These developments have led to the need to audit smart Intrusion Detection Systems (IDSs) to improve their efficacies. Audit of smart Intrusion Detection Systems (IDSs) or IDS audit involves comprehensive and thorough examination of the networking infrastructure and security controls upon which the management and operations of all smart Intrusion Detection Systems (IDSs) in an organization are established [18, 24, 25]. Ordinarily, one of the duties of IDS auditors is to thoroughly scrutinize IDSs, establish and report the efficacies of internal controls that the organization has implemented to safeguard each detector and resources related to these toolkits [26]. The evaluation and the reports of this kind of audit can go a long way to determine the level of compliance and operations of all intrusion detectors in the company with best global practices. Nonetheless, there are numerous challenges with research on audit of smart IDSs in corporate setting in the past years [18]. Studies advise that skilled intruders are common threats that are extremely disturbing corporate and private users of computer systems in Cyber Physical systems (CPSs) [2, 7, 10]. Unfortunately, researchers habitually ignore the audit of smart IDSs that should have established exploitable pathways, audit issues and novel paradigms on network security and perimeter defense since the inception of IDS technology. This neglect has countless impacts on digital resources that connect to cyber physical resources. This shortcoming is explicitly dangerous because it is generating warning signals service providers concerning data reliability and quality of service on local computing resources in many organizations. The impacts of some of these security concerns may appear negligible while significant numbers of them are grievous and hazardous to corporate existence considering the capabilities of demoralizing intrusions recently reported in some public media. Recently, the neglect of this aspect of IDS audit and lack of correlation of IDS audit with research findings have begun to subject sequence of findings from logs analyzers, integrity and compliance with professional standards and regulatory authorities to series of contentions [6, 21, 27].

Importantly, sudden changes in the classifications and dimensions of intrusions that often aim to attack computer and mobile services operating within the

purview of Cyber Physical Systems (CPSs) are global concerns [7, 16]. Intruders have acquired more skills such that they can launch packets that have short and long datagram to achieve different motives in cyberspace. Studies of many trace files suggest instances whereby intruders have split some inbound and outbound packets into fragments. Some studies believe that attackers on Cyber Physical systems (CPSs) can suddenly varied the intensities of packets to smartly elude detections. Numerous audit and networking issues may begin to build up whenever new IDSs are installed in the perimeters of digital networks to complement existing IDSs that auditors have been previously audited. There are possibility that audit exercises may exclude auxiliary issues like log analysis on fragmented packets.

The location of IDSs relative to the firewall in an organization depends on their security policy. A growing numbers of opinions affirm that organizations can install Network Intrusion Detection System (NIDS) in the front or back of a firewall for different intentions [7, 16]. However, models that auditors can adopt to establish suitable approach to organizations are very scarce. Furthermore, current model of ICT audit restrict IDS auditors to the physical security, hardware and software components of smart IDSs [3, 24]. Auditors must use simulated attacks to investigate the initialization, configuration, interface, processing and performances of smart IDSs and to ascertain the tendency of the toolkits to dwindle after a prolonged usage. They must also evaluate the available disk spaces for both the toolkits and mobile devices that receive alerts from IDSs and log analyzers. They must assess the contingency plans in the organization to establish business continuity and preparedness of the toolkits to resume surveillance after intruders have attacked them or after downtime. Auditors must equally evaluate the internal and change controls designed to safeguard the smart IDSs from computer viruses and intruders. In addition, they will investigate the signatures, alert's mechanism, policies and possible rules that have been updated, their corresponding approvals and authorizers of the approvals to modify them [24, 25]. Nonetheless, the above procedures are flawed in the sense that both the experienced and inexperienced intruders may obfuscate and evade smart IDSs audited with the above model. Thus, intrusions on cyber components such as sensing, cyber communication mechanisms and physical resources like computer hardware, data center, employees and mobile devices that the detectors should have discerned and operators would have timely countered often achieve intruders' missions at long run.

One of the fundamental ways this chapter premises for operators and resident auditors to lessen the above problems is for both of them to periodically corroborate research with audit reports on smart IDSs in the perimeters of the organization. However, IDS audit is quite challenging nowadays because it is clearly different from the conventional IS audit process [18, 25]. Besides, IDSs audit requires the engagement of qualified IS auditors that also possess wide experience and knowledge in the above roles. Suitable IS auditors must also have practical experience on the installations of smart IDSs, logs' analyzers, reporting and countermeasures. Moreover, there are acute shortages of operators that also possess auditing skills. Besides, standard IDS audit templates and models that can serve as guiding principles to IDS auditors and operators in corporate environment in the context of Cyber Physical Systems (CPSs) are scarce [18, 24, 25]. Consequently, most IDS operators ignore the research aspect of their jobs that should be regarded as interim audit and concentrate on IDS operations.

Furthermore, approaches that most auditors frequently adopt to conduct IDS audit with generic Information System (IS) and audit process often exclude evaluation of the significance of log analyzers in the organization [27]. The dangers of the above methods are enormous especially if both reviews are inconclusive, unreliable and unsupported by empirical claims before major infringement occurs

in the digital networks of the organization. Organizations can experience infringements in critical and less critical areas of their business operations. Intruders may attack resources or areas of corporate systems that attract little or no attention of IT managers, inspection and internal control's managers with the aims to have enough time to achieve their objectives and to equally evade detection. Consequently, feelers premise that smart IDSs should be strategically installed in the segments that will make it difficult for intruders to bypass them. Smart IDSs that are located at the hearts of huge inbound or outbound traffic should be thoroughly verified by IS auditors from time to time. Traffic that migrates across spanning mode can overwhelm smart IDSs that are technically weak to compromise.

Generally, research findings and related work in the domains of IDS audit and log analyzers are novel issues in network security and Cyber Physical Systems (CPSs) [18, 24, 26]. Conventionally, experts have justified the significance of IDS policy in the perimeter defense of networks of corporate organizations [8, 13, 27]. An empirical study that examined risk-based systems and process audit method has been carried out as a strategy to bridge the gap between auditors and architectural designs of IT resources [18]. The model was able to detect the weaknesses of the process in terms of risk of material deficiencies and thirteen control patterns. However, the research was basically a generalized audit process that has a better performance whenever the model is adopted to audit financial data. Moreover, a study on how to debug Network Intrusion Detection Systems (NIDSs) has been explored [16]. The proposed model uses detection rules to debug NIDSs and eradicate defective rules that are well-known for triggering repetitive alerts. The model can assist IDS operators to reduce workload. However, the major flaw of this model is that it has the tendency to be operationally proprietary. The model will require routinely extension and upgrade before it can broadly relevant to other categories of smart IDSs in the market.

3. The scope of audit of smart IDSs and log analyzers in Cyber Physical Systems (CPSs)

A systematic review of IDS audit is a methodical review or examination of the operational conditions of IDSs with the aims to ensure their protection and to guarantee efficient, effective and reliable IDS operations within the perimeters of computers; cyber physical and sensing resources and mobile networks in an organization [13, 25, 28]. The scope of Cyber Physical Systems (CPSs) varies from organization to organization. Algorithms are the underpinning mechanisms that control and regulate collaborative networks of theories, concepts and embedded disciplines that constitute Cyber Physical Systems (CPSs) in each organization [19]. Audit review should reflect components of computer and mobile systems to be audited. It should state cloud resources such as networks of computers, mobile systems, Wireless Sensor Networks (WSNs), front-end and back-end of the networks, software, hardware, human element, work flow and process engineering [6]. Audit of smart IDS can be performed in conjunction with or separated from the conventional audit exercises in an organization. The audit time table, management, misgivings and repeated outbreak of intrusions can influence the necessity to conduct IDS audit and its scope of coverage. For Cyber Physical Systems (CPSs), the scope of the audit should include the security of sensing processing, storage of large alerts, performance of hardware and software and reliability of the systems. It should also extend to validation of algorithms, automatic systems, theoretical and scientific principles and seamless integration of disciplines underlying the systems with best practices. Hence, this type of IDS audit is eventful [14, 18]. Examiners

must carefully review and match the security policy of the organization with the implementations of smart IDS in the live and test environments to establish areas of compliance and noncompliance with best practice. Fundamentally, enterprise must have IDS policy. An IDS policy is a standard document stating a plan of actions an organization adopts regarding the administration and management of IDSs within their digital networks [8]. Besides, IDS policy should state IDS procedures, IDS rules and conditions that should be meant before rules can be activated, updated or deactivated [13]. The main challenge that IDS auditors often face is that most organizations do not have IDS policy [24]. Findings suggest that some companies do not isolate IDS policy from their security policies [8]. Hence, rather than separating both policies, some of them embedded a few sentences about IDSs in their security policies. Consequently, IDS audit and its ancillaries often lack exhaustive reviews over the years. Therefore, IDS auditor that wishes to conduct the above IDS audit must have well-established knowledge of IDS policy and major components of the smart IDSs within the networks.

In Snort for instance, the objectives of the audit must include critical review of IDS policy, physical security relating to the IDS (Snort in this case), the hardware component and software components of the toolkit. The audit must also include packet decoder, preprocessors, detection engine, logging and alerting system and output modules [8, 13]. Serious audit issues may arise whenever auditors lack strong knowledge of the above components and how they cooperatively work together to detect intrusions and to generate output in the required format.

4. Auditors' challenges in auditing smart IDSs in Cyber Physical Systems (CPSs)

Cyber Physical Systems (CPSs) lack the robustness to counter threats, challenges and cyber attacks due to weaknesses genetic to individual components that form these domains. Hence, there are critical challenges that face auditors and researchers of smart IDSs regarding IDS auditing and log analyzers in these domains. This section discusses and categorizes some of these issues into two groups; namely, the challenges with smart IDSs and challenges with log analyzers.

4.1 Research and audit issues on smart IDSs in Cyber Physical Systems

Different types of smart IDSs keep different categories of logs and alerts in different formats. The default settings of parameters that coordinate alerts of smart IDSs can enable the toolkits to trigger and log wordy and more explicit warnings than the setup that customize these parameters [25, 28]. **Figure 2** illustrates one

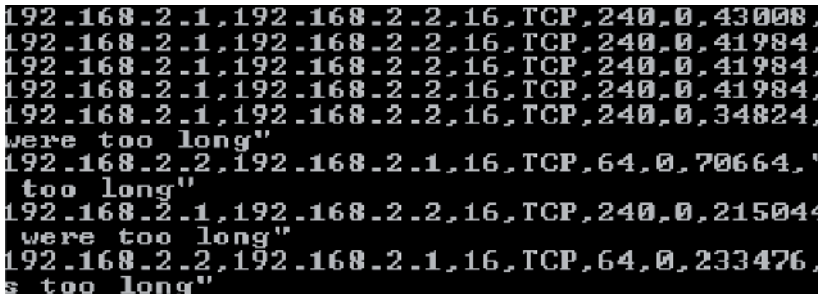

Figure 2.
A sample of alerts from Defcon11 in comma delimited format.

of the kinds of alerts that Snort can generate. The alerts are in comma delimited format because each attribute of an alert is separated by a comma. Operators of smart IDSs can implement the formats of alerts they want during implementation and before executing IDSs like Snort. The major issue is that the preferred formats of alerts cannot be reversed while the toolkits are working. This can create series of setbacks if operators if the formats they have implemented do not convey sufficient information operators will need to decide on the security matters of Cyber Physical Systems in the organization. **Figure 2** illustrates alerts that are expressed in comma delimited formats.

The alerts contain IP addresses to uniquely identify computers and their domain names on the Internet. The alerts are samples of comma delimited alerts extracted from Defcon-11 traces. Some of the attributes of the alerts were Transmission Control Protocol (TCP). However, further information is still required to ascertain attributes like the names, of the attacks to understand data transmission and exchange that occurred between sources and destinations of various attacks. **Figure 3** illustrates conventional kinds of alerts that the Snort would log whenever its default parameters on logs and alerts are implemented in Cyber Physical Systems (CPSs). This format is simple because each alert is explicit to human interpreters. For example, the signature generator (Sig_generator) of the first attack in **Figure 3**, the identification number (Sig_id) of the rule that triggered the alert and the number of times the rule has been reviewed or updated (Sig_rev) were 125, 1 and 1 respectively [25, 28]. The alerts are samples of default alerts extracted from Defcon-10 traces. The attack signified telnet's exploits. In other words, the Intrusion Detection System (Snort) detected telnet commands on the FTP command prompt or channel. The attack also indicated that someone used a computer with IP address 192.168.2.2 and port 21 to transfer file to a computer with IP address of 192.168.2.1 and port 1067 at 10:14 PM on 3rd of August. The problem with alerts that are formatted by comma delimiters is that auditors would require their documentations to properly understand them because they are not constantly explicit. **Figure 3** illustrates a sample of alerts of Snort in a default format.

It is imperative for the auditor to establish the directory where the alerts and systems files of the IDS are kept or recorded in the hardware before the beginning of the audit. By default, shows will Snort log alerts to */vary/log/snort/alerts*. However, the auditor begins to face further challenges if the directory is changed during implementation contrary to the conventional or documented standard. Additional challenges can occur due to the noncompliance of the organization to both the

Figure 3.
A sample of alerts of Snort in a default format.

recommended disk space and accepted format for alerts in the IDS policy [8, 10]. The implication is that it will be difficult to compare the sufficiency of the information conveyed in the IDS logs and short text messages that are extracted from different segments of the perimeters of the same organization if they have heterogeneous formats. In essence, the above sample of the raw alerts explains the link between research on smart IDSs and IDS audit.

4.2 Issues with detection rules or policies of smart IDSs in Cyber Physical Systems

Practical experience shows that the formats of detection rules vary from Intrusion Detection System to another. The rules within the detection engine of smart IDSs are many and they are mostly protected by copyright. The rules usually instruct smart IDSs to discriminate by logging and raising alerts on specific packets that migrate from specific networks into local subnets. Some rules are also designed to instruct smart IDSs to indiscriminately log and raise alerts on all suspicious packets that migrate from any network into local subnets [9]. These rules can also instruct the toolkit to always trigger an alert whenever the device observes any TCP packet that contains "USER root" in its header [8]. Rules can be localized, designed or configure such that they will report suspicious packets heading towards a computer in the subnets of Cyber Physical Systems [10]. Several audit issues arise regarding to best strategies to audit rules or policies of IDSs. These toolkits have several inbuilt rules or policies. There may be some discrepancies between the rules or policies that have been implemented in the organization and the security policy driving the implementation of rules or policies of the smart IDSs in the system. Discrepancies can also occur if some IDSs in the networks are not configured to operate as smart toolkits. Professionalism is required in adapting framework for auditing smart IDSs to audit IDSs that are not configured as smart toolkits in other to adequately safeguard the entire components of cyber physical resources in the organization. One of the reasons behind these challenges is that the security policy of the organization might not fully reflect the totality of the rules or policies in the detection engines of all smart IDSs in the networks. The IS auditor needs to evaluate if the IDS policy actually states specific rules or policies that should be activated or deactivated during implementations of smart IDSs. It is also necessary for auditors to establish the level of compliance of the organization with best security practice on the detection rules or policies approved by the management of the organization [8, 24].

New rules or policies can be added to the smart IDSs in other to improve their efficacies. However, some rules or policies may generate redundant alerts. Hence, it is often difficult to immediately establish the criticality of new and old rules or policies without a critical exploration of log analyzers that process alerts that correspond to these rules or policies. Also, session printable policies or rules are difficult to recommend for deactivation because they enable the detector to log everything attackers have typed [8, 10]. It is possible that all sections of the IDS policy will not fully capture the sensitivity of detection rules or policies in organizations. The chapter encourages auditors to thoroughly audit available IDS policy to ensure the policy is providing suitable standard that covers all components of Cyber Physical resources adopted in the organization.

4.3 Issues with maintenance of smart IDSs in Cyber Physical Systems

Smart IDSs must undergo regular maintenance so that they can adequately monitor very high traffic rates migrating into or outside the organization [15, 16, 23]. The maintenance of smart IDSs is the process of performing system tuning and routine

checks on all smart Intrusion Detection Systems in the organization; the directory of each configuration file, logs, text messages; available storage size, available disk space, disk space each toolkit has already utilized and the last time each toolkit was debugged to establish their readiness to promptly report intrusions that aim to exploit features of Cyber Physical Systems that provide opportunities for intruders to cause havoc without corrupting Cyber Physical data or leaking sensitive information from Cyber Physical Networks. Furthermore, constant maintenance of smart IDSs will enable their operators to correct new and past errors that were not recognized during the installations, configurations and testing phases of these devices. Usually, corrective maintenance is desirable because it will enable the operators of smart IDSs to perfect and improve the operations and performance of smart IDSs [15].

Intruders can compromise the mobile phones and email accounts of operators of smart IDSs [11, 21]. Therefore, the above maintenance will equally help operators of smart IDSs to fine-tune the toolkits so that they can effectively work in new environments and whenever the operators replace their mobile devices or renounce old email accounts. However, maintenance of smart IDSs requires extra efforts than the efforts required to configure and analyze their logs. Hence, most operators of smart IDSs often shy away from carrying out IDS porting, corrective and adaptive maintenance of these toolkits. From experience, IS auditor can perceive series of audit issues whenever the IDS policy does not recognize the significance of maintenance of smart IDSs in the enterprise networks.

4.4 Issues with configurations of smart IDSs in Cyber Physical Systems

There are hardware and software requirements for each smart IDS to exhibit performance that will always conform to best security practices. For NIDSs like Snort, the toolkit works on operating System like Linux, Windows 2003 Server Enterprise Edition and Microsoft Windows XP and hardware like Compaq 1600 Pentium III with dual Processor Server and Pentium IV workstation.

Using Snort as an example [7, 10], this premises that components such as Apache, Pretty Home Page (PHP), WinPcap and Analysis Console for Intrusion Databases (ACID) must be audited to ascertain their levels of compliance to best industrial practice [28]. The combination of Snort, Apache, database and ACID enable the NIDS to log alerts into a database. Two or more toolkits can be configured to centrally log alerts to unified database. Conversely, each toolkit may be setup to log its alerts to a different database. The above components also enable analysts to visualize and analyze alerts on web interface [8, 10]. Hence, the database (back-end) that may be MySQL must also be audited. IS auditors must always refer to the IDS policy for guidance. It is a good practice to complement the audit process by referring to the security policy of the organization to gain insightful evidence on degree of compliance and conformity of both documents.

The dangers are enormous whenever intruders compromise the back-end of the toolkit. Intruders can crash the entire toolkit, alter its cryptographic keys and render it bad and unintelligent [21]. Subsequently, they can illegally reconfigure the smart IDS to log no alerts or to suppress useful alerts [21]. New waves of stealthy attacks can shutdown IDSs; enable triggers and disable or re-start the back-end databases of the detectors. In the case of Snort, attackers can suddenly shutdown the Apache upon which the smart IDS runs. Hence, auditors must establish the level of control that safeguards all the components of smart IDSs in the firm. Usually, in Snort, Apache's server uses configuration file that is stored in the */etc/apache2/apche2.conf* [8, 24]. Therefore, auditors must also establish the last date the configuration's file was updated. Nonetheless, the above ideas are plausible whenever the auditors possess the needed skills to critically explore them.

4.5 Issues with IDS policy and security policy in Cyber Physical Systems

IDS policy is a document that is approved by top management in an organization [8]. This document reflects and states how all IDSs in the organization are implemented and managed. The document further reveals types of IDSs and their versions, configurations, license fees and expiry date and vendors. The document defines activities that managements of the organization have agreed to be regarded as normal and intrusive activities in their Cyber Physical Systems. It is expected to reflect the approved connectivity between log analyzers and logs of smart IDSs. It might be uneconomical to send overwhelming alerts directly to the operators of smart IDSs. Additionally, some smart IDSs can encrypt the email reports or alerts they intend to send to the operators or recipients. However, operators or recipients must install suitable tool in their mobile phones or computers to decrypt them. Thus, IDS policy should categorically state how the email addresses and mobile phones of operators of smart IDSs will receive concise and helpful alerts.

The security policy of an organization is the totality of security mechanisms that is approved by top management of the organization. This broad document usually states how the security's architecture of the organization should be deployed, monitored and managed annually. IDS policy is a segment of security policy. Auditors may find it difficult to challenge operators of smart IDSs in an organization whereby IDS policy is subsumed in security policy. In addition, the appropriateness of time that the organization must review their IDS policy will be difficult to criticize in this circumstance.

Most often, some intruders prefer to launch attacks that can probe or scan cyber networks to compensate for their inabilities to have access to the above policy's frameworks [7, 9, 10]. Information System auditors need to assess the security of the above policies in the organization to establish how they are kept, the custodian of both documents, access and procedures for granting approvals to the employees that have the rights to use and rights to know these documents.

4.6 Research and audit issues with log analyzers in Cyber Physical Systems

The quality of information that various log analyzers can derive from different formats of alerts that smart IDSs generate depend on many factors. Some analyzers of logs that originate from smart IDSs can process specific attributes such as Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), Type of Service (TOS) and Internet Protocol (IP) length. Intruders that compromise the TCP and IP of computer networks will distort network conversations or communications and the exchange of data through application programs [10]. The attacks will also affect apps that send packets of data from one computer to another. Similarly, the values held in the flags of parameters or attributes of alerts also differ from one attribute to another. For instance, log analyzer that analysis the parameters of ICMP in Cyber Physical Systems intend to discover actions of intruders that have requested for certain details about the systems [29]. The intention of the intruder may be to establish computers or mobile devices that signify echo reply and destination unreachable. The attack may also reveal weaknesses in the configurations of router within Cyber Physical Systems (CPSs). The attack can publicize details of routers, timestamp, timestamp reply; redirect message headers, domain name request, domain name reply, mobile registration request, mobile registration reply, errors in the conversion of datagram; address mask request and address mask reply. Intrusions on trace route can provide trodden paths for Distributed Denial of Service (DDoS) attacks in Cyber Physical Systems (CPSs) [29].

In addition, TOS is designed to categorize and prioritize networks' data so that digital devices will process critical data packets before they will process data packets that of less significant. However, intruders have many ways they can check the reliability of the networks. Attacks on TOS intend to undermine the quality of services rendered by the host and routers in the networks. This category of attacks can indiscriminately affect the migrations of different kinds of inbound and outbound data within the networks of Cyber Physical Systems (CPSs) [2, 7]. Intruders can insert fake data into the networks given the knowledge of TOS in the networks. The impacts of this attack can be severe if it occurs at the peak of operations whereby it coincidentally hinders the priority and migrations of data of higher importance than data of less importance in the networks. Moreover, attack on TOS can increase the numbers of fragmented packets that lost in transit. It can also cause significant delay of packets to complete computer and mobile communications, reassembling of fragmented packets and routing of multimedia data.

Each of the above attributes of alerts conveys different meanings to different organizations [9]. The mode that every log analyzer adopts to write their results into the output files (folders) is very important. Programs that append new records with old records would require enough disk space than programs that always clear all the content of old records in the output files during execution. For these reasons, IDS auditors often face many challenges from company to company in conducting thorough investigations on outputs of log analyzers and establish the significance of the output files in accordance to best practice.

4.7 Issues with theoretical frameworks for designing log analyzers in Cyber Physical Systems

There are several theoretical frameworks that programmers can adopt to design log analyzers to analyze logs of smart IDSs within Cyber Physical networks. Studies show that Statistical techniques, subjective logic, Visualization, Artificial Intelligence (AI), Neural Networks (NNs), Ensemble techniques and data mining have been used to design log analyzers in recent years [23]. Some analyzers may adopt priority of alerts, similarity of values held in the attributes of alerts, human observations, attack scenarios, hierarchical graphs, attacks that overlap, subjective reasoning and evidence of the damage the attack has caused as underpinning philosophies to design log analyzers [23]. Auditors must be thorough in this regards because features of non-related attacks may overlap and this will lead to mismatch of intrusions [26, 27]. The maximum error of log analyzer will increase if it mismatches intrusions. In other words, reports from log analyzer that mismatches intrusions are misleading and ineffective to design strong counter measures against intrusions in progress.

In addition, it is necessary for auditors to establish how each analyzer select minimum similarity and expectation of similarity in other to establish how the toolkits merge related alerts together. Also, different algorithms and metrics can compute weighted average of related alerts in different ways. Hence, it is challenging for auditors to be vast in different algorithms for comparing overall similarity of the alerts and how various algorithms isolate patterns of alerts that are false positives from real positives.

4.8 Issues with metrics for designing log analyzers in Cyber Physical Systems

Programmers can design log analyzers that adopt multiple metrics and different data mining concepts to analyze logs of smart IDSs [14]. It is easy to compare outputs of closely related metrics together. IDS auditors must conduct routine

research to ascertain strengths and weaknesses of statistical metrics that programmers have used to support intrusion detections in corporate organization that is under review. There are different ways to interpret and improve the quality of alerts from smart IDSs. Hence, the interface between log analyzer and logs of smart IDSs must be reviewed. These will enable auditors to establish suitable metrics for cross-correlation of alerts rather than interpreting uncorrelated attacks with heuristic methods. The instant that the design will update email addresses and mobile phones of operators of smart IDSs with new alerts should immediately IDS detects every suspicious event. Security issues begin to build up whenever there are networks failures such as poor Internet connection and poor mobile signals.

Auditors must review operational logbooks to determine whether operators of smart IDSs keep track of cases of networks failures such as poor Internet connections, inability to access emails and poor mobile signals in the organization. These will give insightful evidence into the effectiveness of Internet and mobile service providers that are supporting the organization. The findings in this case may also guide the auditor in recommending to the organization to sustain or review the Service Level Agreements (SLAs) they agreed with their service providers. The new threats to cyber physical resources how to mitigate intrusions that can co-occur together without sharing the same impacts on the targets. Outputs of log analyzers may indicate graphical illustrations of alerts [8]. Some operators of smart IDSs may prefer to adopt visualizations to interpret alerts in the form of histogram, pie charts, bar charts and simple correlation graphs [8]. **Figures 4** and **5** demonstrate graphical illustrations of alerts from Snort whenever the valued held in the TCP and TOS are used to analyze alerts from the same dataset. For these reasons, IDS audit must be able to establish audit issues concerning attributes and metrics the organization are adopting to differentiate sequences or patterns of alerts that have tendencies to possess different interpretations from alerts that have regular patterns even if these alerts are analyzed with different attributes. Some interpretations of alerts may not impact directly on business operations that human element of Cyber Physical Systems (CPSs) transacts on daily basis. In addition, it is plausible that some intrusions are seasonal threats to Cyber Physical Systems (CPSs). **Figure 4** illustrates log analysis of alerts on the basis of the values held in TCP of intrusive alerts.

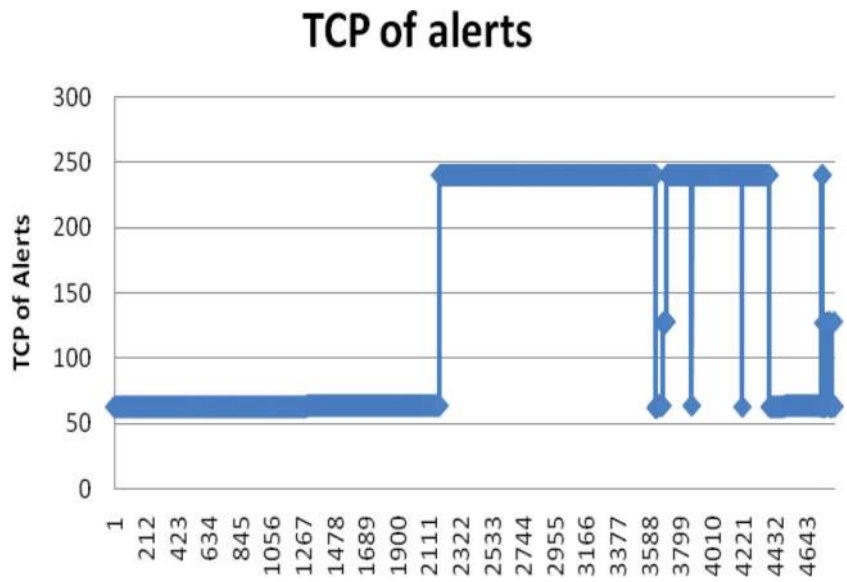

Figure 4.
Log analysis of alerts by values held in TCP of alerts.

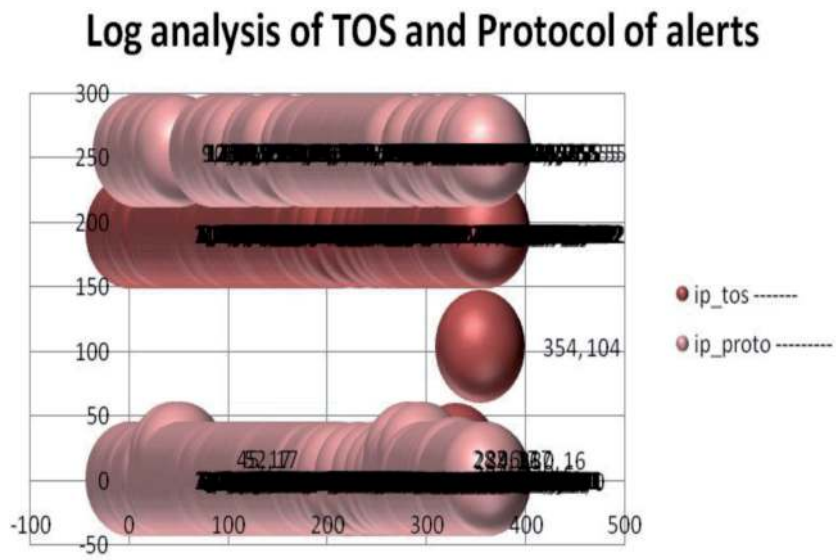

Figure 5.
Log analysis of alerts by values held in TOS and Protocol of alerts.

A seasonal rise in successful cases of cyber-attacks on corporate elements of Cyber Physical Systems (CPSs) can co-occur with a seasonal rise in unemployment and suspension of skilled workers. Therefore, IDS audit must establish the availability of inbuilt functionalities and capability of log analyzers in the organization to enable operators of smart IDSs to timely detect and mine frequent alerts from multiple sensors. Some IDS auditors can face challenges in recommending simple methods for graphical interpretations of IDS logs to organizations that do not include methods they prefer to illustrate intrusions against their Cyber Physical Systems in their IDS policy. **Figure 5** describes log analysis of alerts on the basis of the values held in the type of service (TOS) and Protocol of intrusive alerts.

5. Methodology for auditing smart IDSs and log analyzers in Cyber Physical Systems (CPSs)

Log analyzers are defined in this chapter as various programs that are designed to analyze logs of IDSs in a corporate setting [8]. Log analyzers have different objectives. The chapter proposes log analyzers that are interfaced with GSM to send short text messages after they have processed alerts of smart IDSs to operators. Log analyzers often have different objectives. For instance, log analyzers can be designed to debug NIDSs in the organization. There are log analyzers that determine the degree of predictability of attributes and information conveyed by attributes of alerts. Similarly, there are log analyzers that focus on correlation and aggregation of alerts. Sources of input data to each log analyzers in the same organization may also vary.

Some log analyzers may derive their input data from homogeneous logs of smart IDSs while significant numbers of them may receive input data from heterogeneous IDSs. By auditing them, operators and IDS auditors will be able to ascertain how the existing Log analyzers cluster alerts to arrive at the succinct texts they send to operators. For log analyzers that receive input data from several smart IDSs, it is necessary for the IS auditors to assess the locations of the contributing IDSs in relation to the log analyzers that aggregate or analyze their logs. Evaluators should ask questions like was the input modules of various log analyzers designed to override old alerts or append new alerts to previous ones and what programming language

was used to design them? The time to upload new alerts to the input modules of the log analyzers should also be audited. **Figure 6** is a sample of execution of log analyzer of alerts that is implemented in this chapter.

The results from the above enquiry can determine log analyzers that should be recommended for upgrade and new development that should be incorporated to improve intrusion detection in the organization. **Figure 6** illustrates samples of execution of four categories of log analyzers that are designed to support the aruments raised in this chapter. These log analyzers are implemented with C++ language and they are based on the attributes of alerts from Snort IDS. The input to three of the analyzers were alerts that Snort triggered on the DATA01, DATA02 and DEFCON-10 dataset in IDS and offline modes. The input to forth analyzer was alerts that Snort triggered on DDoS datasets supplied by the DAPRA to assist research community. The IDS triggered 4,919 alerts and dropped 250 packets after analyzing the packet capture (PCAP) file of the dataset. Typical IDS research can explore many concepts with the above alerts.

The first log analyzer explores the rules that triggered the above alerts and a sample of its results is shown in **Table 3**. The second log analyzer explores the sources of the intrusions and all the addresses of computers they attacked and categorize them on the basis of date, time, sequence number, source IP address, source port number, destination IP address and port number of destination address. The third log analyzer explores the sources and destinations of the intrusions captured in the dataset. To ascertain the variability and quality of the alerts, the analyzer went further to compute Gini Index on the basis of sources and destnations of the attacks to further classify the alerts as shown in **Table 1**.

Given the probability of each cluster $[p(c_t)]$ and for each attribute (SIP or DIP), the Gini Index is expressed as [14]:

$$GIndex(SIP / DIP) = 1 - \sum_{t=1}^{n} (p(c_t))2 \quad (1)$$

The fourth analyzer uses alerts from DATA01 and DATA02 to compute the lengths of alerts and the pattern within them.

5.1 A model for auditing smart IDSs and log analyzers in Cyber Physical Systems

The auditors of smart IDSs must have audit plan and feasible audit time table. The audit time table should categorically state the annual frequency proposes for conducting audit of smart IDSs and log analyzers in the organization [4, 24, 25, 27]. **Figure 7** describes a model for auditing Smart IDSs and Log analyzers in CPSs.

The audit plans can be an annual arrangement or a short-term plan that itemize the procedures the auditors will adopt to conduct IDS audit in the organization at the due dates. **Figure 7** illustrates the schematic diagram of a new framework for auditing smart Intrusion Detection Systems (IDSs) and log analyzers in this chapter. Accordingly, IDS auditors should preview the entire processes they will follow to carry out the audit of smart IDSs and log analyzers in advance. This is called the planning phase. This is the stage at which the auditors must delineate the objectives, scope, budget and resources they would require to comprehensively accomplish the audit [4, 5, 24]. The auditors will also need to establish the methods they will adopt to carryout fact-finding; the duration or time frame they will spend on each stage and the total time they will generally spend to conduct the review. The IDS audit team should categorically state the format of the IDS audit reports, potential challenges they envisage and the period they schedule to conduct exit meetings with the management of smart IDSs in Cyber Physical Systems (CPSs).

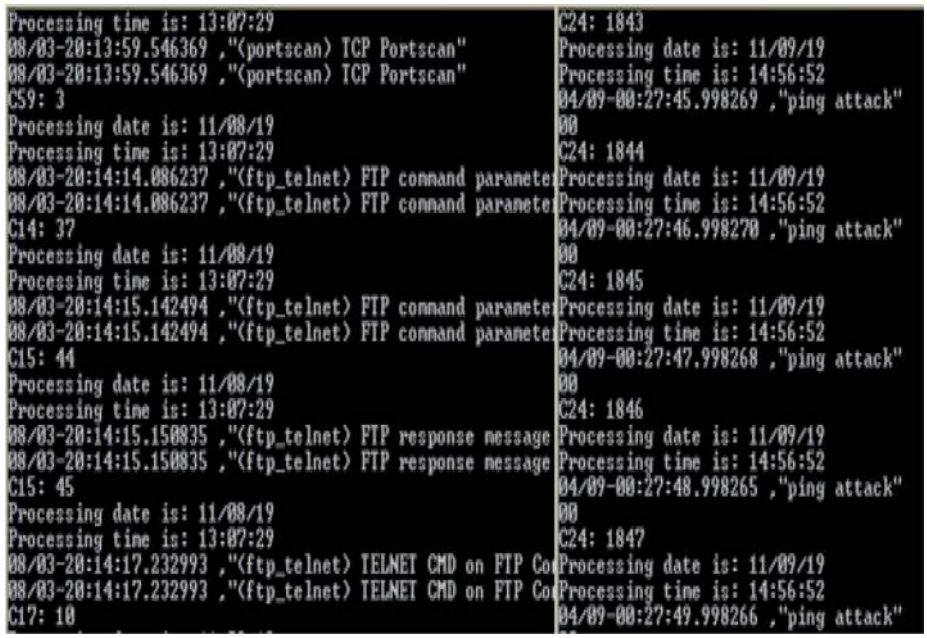

Figure 6.
A sample of execution of log analyzer of alerts.

Dataset	Attribute	Number of cluster	Gini Index
DDOS-1-SIP	Source IP	408	0.998
DDOS-1-DIP	Destination IP	1	0.000
DDOS-2-SIP	Source IP	265	0.996
DDOS-2-DIP	Destination IP	1	0.000

Table 1.
Log analysis of online trace files.

The second stage of this model is the preliminary examination of smart IDSs' controls and Log analyzers. In this stage, the IDS auditors ought to carry out initial assessment of the existing IDS resources, all related components of the IDS; operational procedures and the controls that were implemented in the enterprise to safeguard the smart IDSs and log analyzers. The auditors should interview or send questionnaires to main employees that are responsible for the management of different smart IDSs and all log analyzers in the organization [17, 18]. The review should cover all the IDSs in the organization together with infrastructure in the organization that relates to them, logical access and physical security of each smart IDS. The directory of each smart IDS, access to the root directory, procedure to log on to the root, permissions granted to read, write, execute and modify files and log analyzers; operating systems; hardware requirements including security, usage and available disk space; configuration files (signatures, profiles, etc) and respective logs kept by each smart IDS and log analyzer must be requested from the dedicated IDS operators. The review of the log analyzers and other programs that interface with the logs of the smart IDS should also be carried out at this stage using simulated attacks.

Furthermore, at the third stage of this model, the IDS auditors begin to critically examine Service Level Agreement (SLA) on the smart IDSs and verify the SLA for

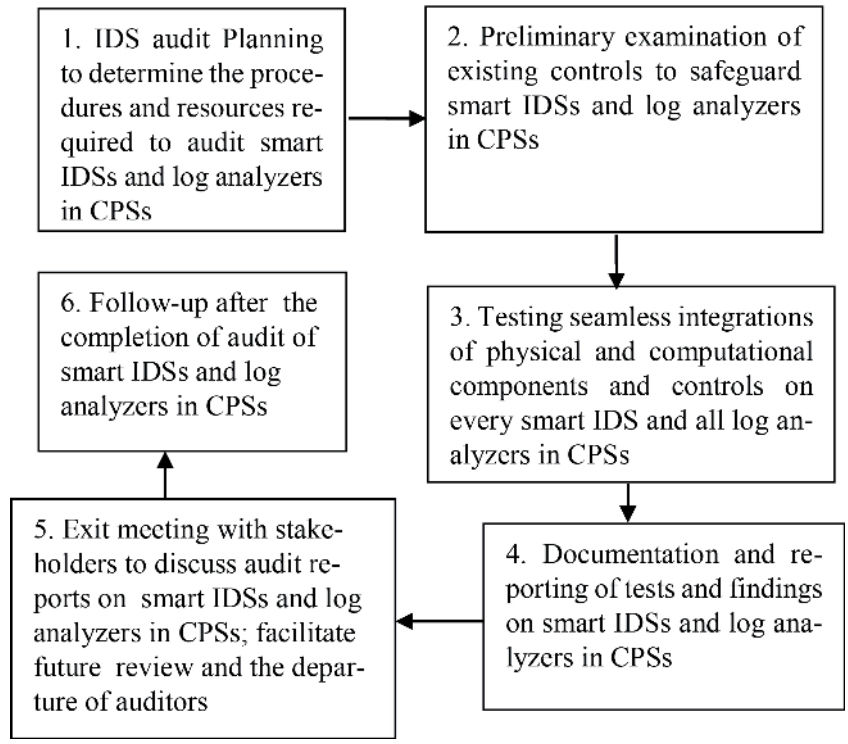

Figure 7.
A model for auditing smart IDSs and log analyzers in CPSs.

proprietary log analyzers [18]. They will scrutinize process flow, incident reporting procedures; relevant features of physical and organizational structures; training and users manuals in the organization that is using Cyber Physical System to support their business operations. They must test and validate the level of security and controls that have been implemented to counter likely threats and attacks on smart IDSs and related infrastructure in the networks [7, 13, 25]. Auditors must examine the seamless of the entire components of the engineered systems and quantify the level of protection smart IDSs in the organization can render to them. They must review controls and configurations of operating systems, security of smart IDSs and database access controls. The review at this stage should include various strategies the organization has implemented to hardening the host computer(s) and the networks so that auditors can establish the levels of compliance of operations of smart IDSs in the company with best practices [5, 21, 25].

In the fourth stage, proper documentation and reporting are critical elements that auditors must carryout to achieve comprehensive auditing of smart IDSs and log analyzers [4, 18, 25]. Hence, it is imperative for the IDS auditors to document key findings they observe at each stage of the audit. This chapter proposes that the IDS auditors should appoint dedicated scribers among the audit team to document tests and respective findings as the audit progresses. IDS audit reports should include executive summary, suitable headings, controls investigated during the audit and corresponding findings the team of auditors have observed in the organization [17, 24]. They must include remarks, recommendations and practical suggestions on how IDS operators and designers of existing log analyzer can fix audit issues they have identified in the review. Thus, this chapter proposes that documentation and reporting of findings should be incorporated into stage 4 of a comprehensive audit of smart IDSs and Log analyzers in Cyber Physical System.

Exit meeting is the fifth stage for a comprehensive audit of smart IDS and log analyzers in the context of Cyber Physical Systems. The auditors and audit team from the organization that is under review must gather together in interactive conferencing to discuss the audit reports before the audit team will exit the organization [17, 25]. The meetings are avenues for both teams to agree on the date and how various audit issues raised on the smart IDSs, log analyzers; computational and cyber physical infrastructure in the organization will be fixed. The meetings should state the date the representatives of audit team will revisit the unit of the organization to check that issues raised in the IDS audit reports have been fixed.

Finally, follow-up is the sixth and last stage of the above framework. The representatives of the IDS audit team must revisit the organization to examine documents like visitor's diary and access log to the above resources. They need to also report on the status of all the issues that have been raised in the audit reports they recently submitted to the organization [25]. To conclude the audit, the reports of this team should categorically state audit issues on smart IDSs and log analyzers that have been fixed, pending issues and reasons behind the delay on audit issues that end-users have not fixed. We suggest that auditors must advise the organization to develop a suitable IDS policy whenever they have none.

5.2 Results and discussions

The attacks illustrated with the DDOS-1 and DDOS-2 datasets in **Table 1** did not vary on the basis of their respective destinations' IP addresses when compared with the sources' IP addresses of the attacks. The results sugest that the entire alerts that originate from the dataset are mostly repeated information that belongs to one group of destination's IP address. Hence, the Gini Index was 0.000.

Figure 8 illustrates log analysis of lengths of alerts in DATA01 dataset.

Therefore, IDS auditors must as well audit codes and Log analyzers to establish the input data, their functions and capabilities in other to establish the strenghts and limitations of each analyzer. Such systematic review will enable the auditor to establish Log analyzers that analysts should optimize either by splitting them or by merging two or more codes together. **Table 2** illustrates cumulative length of attributes that Snort has used to report 4919 and 75,390 alerts on DATA01 and DATA02 respectively. **Table 3** interprets the attacks from the above evaluation and the rules that detected them. Thus, auditors can adopt information in **Tables 2** and **3** to conduct risk assessments and identify strategies of some intruders in Cyber Physical Systems (CPSs).

Figure 9 is a description of log analysis of lengths of alerts in DATA02 dataset.

Essentially, **Figures 8** and **9** illustrate the patterns that lengths of alerts from both datasets can generate. Thus, the chance that intruders can overload smart IDSs over time depends on the quantity of alerts the detectors can trigger on daily basis. The results further suggest that automated strategy for forecasting length of alerts smart IDSs generate is critical to auditors in conducting audit of smart IDSs in the context of Cyber Physical Systems (CPSs). This can assist operators to forecast patterns of attacks, workload and how human aspects of security and privacy can link to Cyber Physical Systems (CPSs).

5.3 Suggestions for improving security in Cyber Physical Systems

The above models have practical implementations in protecting computational, human, mechanical and physical components that are fundamental to Cyber Physical Systems (CPSs). IDS policy must state the configurations and various types

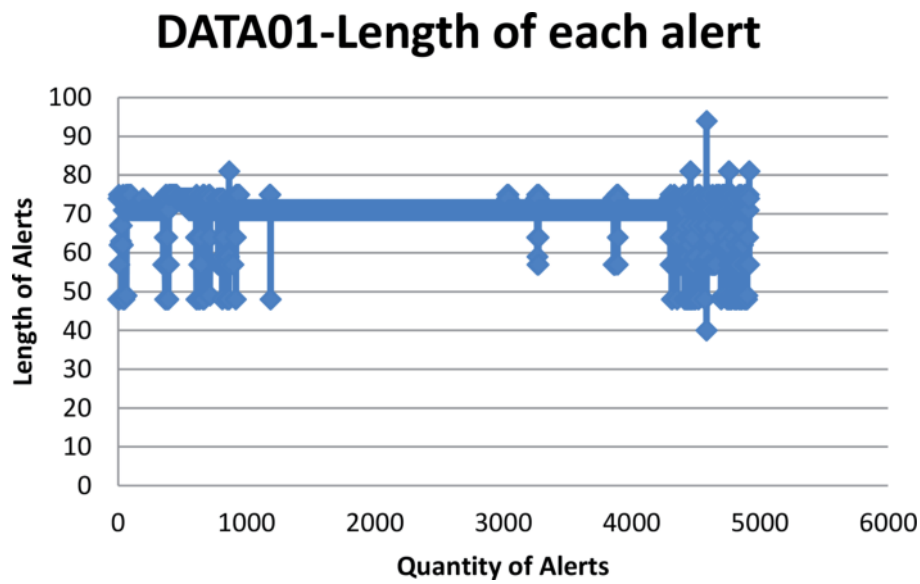

Figure 8.
Log analysis of lengths of alerts (DATA01).

Dataset	Total alerts	Total attributes
DATA01	4919	345375
DATA02	75390	2893183

Table 2.
Log analysis of components of alerts.

of smart IDSs in the above settings. This document should state the vendors of Network Intrusion Detection Systems (NIDs) and Host-based Intrusion Detection Systems (HIDSs) installed to safeguard all entities in Cyber Physical Systems (CPSs). Auditors must verify whether the policy approves software-based IDSSs or hardware-based IDSs, or combinations of both detectors. Among other things, auditors should further investigate this document to ascertain if it contains information regarding license fees, number of users, expiration date for the payment of license fees and bank accounts of the vendors of smart IDSs procured in these settings.

IDS policy must reflect operators of smart IDSs responsible for the administration and monitoring of various smart IDSs and Log analyzers in the organization. Recently, intruders keenly probe source codes to establish their limitations. Therefore, it is imperative for IDS auditors to carefully scrutinize IDS policy. The document must categorically state allowable length of time to train supervised learning algorithms as well as the acceptable level that log analyzers must reduce workload due to IDS alerts in other to undermine the generality of intrusions IDSs have warned. What is the acceptable way to classify similar alerts and similar intrusions? Should similar intrusions be classified on the basis of temporal relationships, intrusive objectives, capabilities to support subsequent intrusions or values held in the attributes of alerts? The audit must be able to match IDS policy with the above questions for the document to be useful for mitigating problems of alert correlations that have raised serious concerns among security experts in recent time. IDS policy document should not reflect ambiguity in any aspect. The document should be simple and explicit. It should also include the incident and reporting team; processes of escalating cases of intrusions and response strategy approved by the

Sig_generator	Sig_id	Sig_rev	Description of alert/attack	Summary of attack
119	2	1	Double decoding attack	The attack was an http exploit. The intuder inllegally inspected HyperText Transfer Protocol (http) to gather information about application protocol for distributing hypermedia data in the networks
119	18	1	Webroot directory traversal	The attack was an http exploit. The intuder possibly accessed data, codes, files, etc via root directory of the web server in the networks
122	1	0	TCP portscan	The intuder inllegally scanned a computer port with intention to gather information about open ports, close ports and services running in the computer
125	2	1	Invalid FTP command	The intuder used invalid FTP command to possibly transfer files in the networks
125	3	1	FTP command parameters were too long	The attack was buffer overflow exploits with FTP client. The intruder used telnet's client to possibly transfer files that exceeded maximum length in the networks
125	4	1	FTP command parameters were malformed	The intruder used badly formed FTP command to possibly transfer files on FTP client

Table 3.
Log analysis of rules that generate alerts.

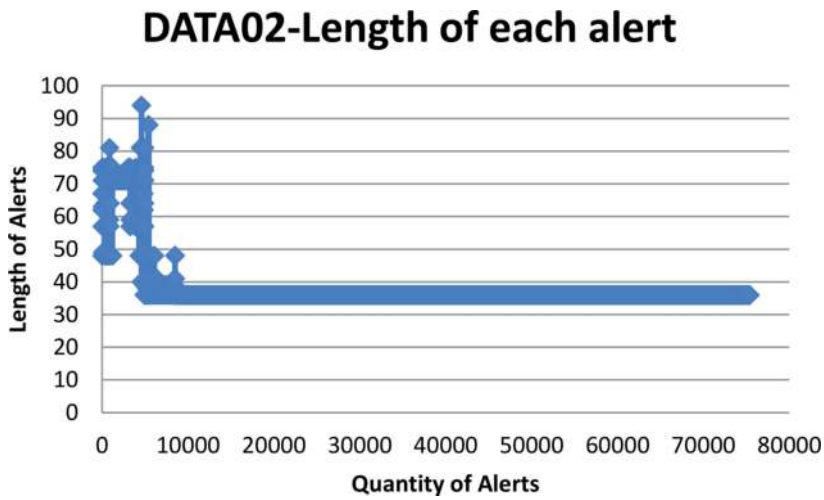

Figure 9.
Log analysis of lengths of alerts (DATA02).

management. In all, it is equally suggested that IDS policy should include methods for handling public awareness and lessons learnt in the case of devastated attacks that require the organization to intimate the general public.

An organization may deploy smart IDSs that run on different operating systems. The performance of smart IDSs becomes necessary whenever they run on different operating systems. For instance, experience shows that Bro usually operates in Linux/Unix, FreeBSD and Solaris' environment while Snort can run with Windows and Unix/Linux operating systems. There are different ways to hardening different operating systems. Therefore, auditors must familiar with different ways to hardening common operating systems in the industry. Some smart IDSs require installations of client software on computers in the networks of Cyber Physical Systems (CPSs). Hence, auditors must also ensure they audit client software on computers in the networks that interface with smart IDSs. Uninteresting activities and activities that are important attacks can vary from organization to organization. Hence, auditors must be professional at all time. They should professionally handle recommendations aiming to limit the number of false positives especially while suggesting extra policy scripts that should be included with existing rules for detecting cyber-attacks.

Some toolkits can express their signatures as regular expressions or as fixed strings. Audit of smart IDSs in Cyber Physical Systems (CPSs) should establish how signatures are designed in each detector. This information is needed in recommending suitable training and professional development to operators of smart IDSs whenever audit reports suggest that operators lack sufficient knowledge to carry out their daily jobs' specifications. Auditors of smart IDSs and log analyzers should evaluate the effectiveness of training facilities that are available for conducting in-house training in the organization. In-house training can be recommended to operators in case the required facilitators are available in the organization. It is ethical for auditors to recommend training outside the organization to operators of smart IDSs whenever there are insufficient facilities to conduct in-house training in the organization [25, 27]. Operational training should include topics such as network or traffic content, false positives. false negatives, policy scripting or writing rules or signature, signature-matching, uninteresting activities, interesting activities, cyber threats and attacks, security, user privileges, front-end and back-end of smart IDSs; installation, configuration, maintenance and execution of smart IDSs and log analyzers to empower operators of smart IDSs in Cyber Physical Systems (CPSs). Auditors should ascertain operators if smart IDSs that aware or unaware of the official websites of various smart IDSs in the organization during audit of smart IDSs and log analyzers. The audit should establish operators of smart IDSs that subscribe or unsubscribe to news update in the official websites of IDSs in the organization. The reason is that official websites of IDSs often contain helpful documentations and new tips about bugs and attacks and strategies to fix them. There should be no bandwidth limitations in the networks for most smart IDSs to be effective. Organizations should strictly adhere to the hardware requirements such as hard disk and processor of host computers; software requirement such as operating systems (Linux, Windows and Solaris) and the required versions of auxiliary tools such as libpcap, Perl and tcpdump that service providers recommend for smart IDSs to ensure high performance. Audit reports should state the location of smart IDSs in the organization; other options for location the toolkits and their respective benefits to enlighten the organization. For instance, smart IDSs can be installed behind an external firewall in the networks. This will enable the firewall to reduce numbers of suspicious packets that smart IDSs in CPSs will analyze. Some organizations may install smart IDSs before the external firewall. This method will enable smart IDSs to detect potential attacks migrating into the networks. The trade-offs is that smart IDSs will produce high number of alerts for log analyzers and operators to analyze. Smart IDSs can also be installed inside internal firewall if the human element in Cyber Physical Systems (CPSs) aims to detect internal hosts that are vulnerable to computer worms and computer virus.

Audit reports should specify agencies that require external reports of incidents from the organization that is being audited. Statistics on incident information can suggest prevalence of security breaches of Cyber Physical systems (CPSs) nationwide. Auditors can evaluate compliance of the organization to the various requirements of regulatory bodies by reviewing information about the frequency regulators required for submitting mandatory reports to the government and National Agency for Incident Analysis (NAIA). The formats of the reports may be summary of critical incidents or all cases of security violations on monthly, quarterly, biannual or annual basis. Interview with someone who inspects and forwards the reports to the required external recipients will appropriately establish details of how and when the reports are due for submission. The reports to agencies should be informative in case they require the reports in specific formats. Operators should express the date and time the incident begin and end. The number of each type of incident could be included in the report period for statistical purpose.

Smart IDSs and log analyzers merely detect suspicious events. They cannot make authoritative decisions if a suspicious event is an attack or not attack. These mechanisms also lack the intelligence to decide whether an attack is successful attack or a failed or unsuccessful attack. Therefore, operators and recipients of alerts from smart IDSs and log analyzers must constantly investigate the reports they receive from the above mechanisms. Furthermore, IDS audit reports and reports on log analyzers should be simultaneously made available to the IDS operators in the organizations to address all audit issues pinpointed in the reports.

Above all, the above audit model is an integral part of the information security of an organization. Host machines, hardware-based IDSs and repository for storing reports on smart IDSs should be regularly protected from intruders like burglars. For software-based IDSs, the logical security of databases of the IDSs; web servers and various infrastructural components on the networks such as router, firewall and location of the smart IDSs in relation to the firewall should be thoroughly reviewed to ascertain their levels of compliance with best security standards. Segregation of duties among network engineers, Database Administrators (DBAs), internal control and operators of smart IDSs in Cyber Physical Systems (CPSs) is highly recommended. It is disastrous if the logs are deleted while the toolkit is running. Auditors should recommend enforcement of strong access controls to restrict illegal logging in to the configurations and logs of smart IDSs as panacea to information leakages and attacks on smart IDS through the back-end of applications in Cyber Physical Systems (CPSs) [12].

The root causes of intrusions are dynamic security and privacy issues in Cyber Physical Systems (CPSs). Broad audit should be able to reveal how log analyzers adopt classification rules to segment logs of smart IDSs in Cyber Physical Systems (CPSs) and classify alerts into normal and abnormal events. Without sound understanding of data mining procedures, IDS auditors might face difficult challenges to audit association and episode rules necessary to expose hidden relationship among alerts that are not obviously related. Research has discovered that sequence of the intrusions on cyber physical resources in an organization can occur within different timestamp. Practically, it is difficult to find the mean of categorical datasets that have no numerical attributes. Instances whereby the designers of log analyzers have adopted weighted values to transform alerts in the logs of smart IDSs must be clearly reviewed during audit. The reports will enable end users to establish limitations of algorithms that adopt concepts like k-nearest-neighbor (KNN) classifiers and how to improve on the underpinning concepts for transposing alerts into human readable form in the organization. Auditors should establish types of Security Information and Event Management (SIEM) and other threat solutions in Cyber Physical Systems (CPSs).

The above results submit that auditors must audit log analyzers irrespective of whether they are locally designed or they are proprietary models in the organization. The reports should reveal expert rules that are used to process events' logs and their characteristics. Auditors should strongly recommend proper documentations for log analyzers and other threat solutions in Cyber Physical Systems (CPSs). Essentially, the above audit model should establish the existence or absence of audit team in the organization. Reports obtained from the audit should be submitted to the unit in charge of monitoring smart IDSs in the organization. Thereafter, auditors should notify them and management with written reports stating past audit issues that have been suitably addressed [16, 26]. Otherwise, a terminal date to ensure that all pending audit issues must be addressed and potential impacts of noncompliance must be issued to the above stakeholders as well.

6. Conclusion

This chapter shows that pragmatic studies on audit of smart IDSs in the context of Cyber Physical Systems (CPSs) are erroneously taken lightly over the years. This gap has generated negative impacts in the security of computational components, cyber and physical resources of Cyber Physical Systems (CPSs) over the years. Manufacturers of smart IDSs can design rules or policies that are deactivated by default because they are not immediately needed to protect Cyber Physical Systems (CPSs). Such rules or policies can be completely useless if smart IDSs are not periodically audited. Operators can waste huge resources to redesign inactive rules or policies due to lack of information about possible threats and cyber attacks in Cyber Physical Systems (CPSs) and ignorance of the existence of similar rules or policies in the detection engines of smart IDSs. Consequently, the chapter demonstrates that log analyzers can serve diverse objectives in a corporate setting. It has also been stated that series of intrusions can elude smart IDSs whenever the periodic audit of smart IDSs in Cyber Physical Systems (CPSs) is not based on empirical findings. The idea is that smart IDSs and all log analyzers in a corporate setting must be specially audited and their readiness for packets processing must be routinely verified to ascertain their compliance with best security practices.

There are several concerns that may arise if the computers hosting smart IDSs are weakly protected or if they are not protected at all. The toolkit can be compromised by intruders, thereby under-reporting or over-reporting security breaches in Cyber Physical Systems in the organization. Intrusions that overpower hosts of smart IDSs can suddenly shutdown the toolkits without the awareness of operators. The smart IDSs can begin to generate series of false alerts. These devices can suddenly stop to trigger alerts if intruders cleverly re-configure them without the awareness of dedicated employees. Experienced intruders may modify rules or policies of smart IDSs and compromise the passwords for logging to the root directories of smart IDSs in Cyber Physical Systems (CPSs). They may delete logs, modify alerts and other related components of these toolkits. Some intruders may disable smart IDSs in Cyber Physical Systems (CPSs) before they will attacks the networks. The integrity of the log analyzers that analyze logs of compromised smart IDSs in these circumstances will also be subjective. Therefore, smart IDSs and log analyzers in Cyber Physical Systems (CPSs) must be periodically audited to establish lapses or hidden faults in the validity and the strength of the protection that the internal controls offered to the detectors and to help the company to settle on the cost of ownership of their smart IDSs.

This chapter has proposed an audit model that should contain significant and explicit information necessary to guide human elements in Cyber Physical Systems

(CPSs). The chapter also substantiates the importance of smart log analyzers in the security of Cyber Physical Systems (CPSs). These groups of log analyzers are configured to remotely send brief statements that present the main points about alerts/attacks and in the form of short text messages to the operators of smart IDSs in Cyber Physical Systems (CPSs). The message may include "source IP, destination IP, short descriptions and time of occurrence of the attacks". The above model has also suggested that audit reports should contain executive summary on audit of smart IDSs and log analyzers in Cyber Physical Systems (CPSs); objectives or purpose and scope of the audit. The reports must also include all proprietary and locally developed log analyzers that relate to smart IDSs in the review. The reports will be informative if they convey information about the available resources, challenges and date of the audit. Columns that outline the serial number (S/N); control tests that auditors have carried out, findings, risk assessment of each problem, suggestions that can mitigate the problems; human elements in Cyber Physical Systems (CPSs) that should fix the problems and remarks or explicit comments (that will state whether the problem has been fixed or is still a pending issue) should be incorporated in the audit reports. Useful explanations regarding the entire phases of the audit, signatories to the reports and annotations should be included in the reports to clarify and substantiate the validity of the reports to stakeholders in Cyber Physical Systems (CPSs).

Furthermore, auditors must periodically verify that logs of smart IDSs and log analyzers in Cyber Physical Systems (CPSs) are regularly archived and operators strictly adhere to the modality for maintaining them. This chapter has further provided a new pathway on how to investigate the sufficiency of IDSs intelligence and log analyzers and the degree at which they conform to IDS policy and best security practices in a real-life environment and in the context of Cyber Physical Systems (CPSs). Since empirical studies have shown that IDS policy is a well-established fact in IDS manuals, similarly, future studies should provide best standards and frameworks for concurrent auditing of smart IDSs and log analyzers in Cyber Physical Systems (CPSs) using non-statistical metrics. Finally, strong cooperation between organizations, GSM operators and research community can help to lessen issues and challenges in Cyber Physical Systems (CPSs) that have been identified in this chapter.

Author details

Joshua Ojo Nehinbe
ICT Security Consultant, Nigeria, West Africa

*Address all correspondence to: nehinbe@yahoo.com

References

[1] A. W. Colombo, T. Bangemann, S. Karnouskos, J. Delsing, P. Stluka, R. Harrison, F. Jammes, and J. Lastra: Towards the Next Generation of Industrial Cyber-Physical Systems in: Industrial Cloud-Based Cyber-Physical Systems: The IMC-AESOP Approach. Pp. 1-22; Springer Link, ISBN 9783319056234 (2014)

[2] J. Epstein: Security Lessons Learned from Société Générale. IEEE Security & Privacy, Vol. 6, Issue 3 (2008)

[3] W.H. Baker, A. Hutton, C.D.Hylender, C. Novak, C. Porter, B. Sartin, P.Tippett: Data Breach Investigations Report, Verizon Business (2009)

[4] L. George: Cyber-Physical Attacks: A growing invisible threat. Oxford, UK; Elsevier Science. ISBN 9780128012901 (2015)

[5] Gubb P, Takang A. Software Maintenance. New Jersy, USA: World scientific Publishing; 2003

[6] IANA: Internet Control Message Protocol (ICMP) Parameters https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

[7] D. Adams and A. Maier: Confidentiality Review & Audit of GoldBug-Encrypting E-Mail-Client & Secure Instant Messenger (2016)

[8] J.O. Nehinbe: Automated Technique for Debugging Intrusion Detection Systems, 1st International Conference on Intelligent Systems, Modelling and Simulations (ISMS2010), proceedings of IEEE Computer Society's Conference Publishing Services (CPS), London (2010)

[9] J.O. Nehinbe: Methods for reducing workload during investigations of Intrusion Logs; PhD Thesis, University of Essex, Colchester, London (2011)

[10] J .Fitzgerald, P.G. Larsen, M. Verhoef (Eds.): Collaborative Design for Embedded Systems: Co-modelling and Co-simulation. Springer Verlag, ISBN 9783642541186 (2014)

[11] K. Julish, C. Suter, T.Woitalla and O. Zimmermann: Compliance by Design – Bridging the Chasm between Auditors and IT Architects. *Computers & Security*, Elsevier. Vol 30, Issue 6-7 (2011)

[12] D. Wu; D.W. Rosen; L. Wang and D. Schaefer: Cloud-based design and manufacturing: A new paradigm in digital manufacturing and design innovation; Computer-Aided Design, Vol 59, pp 1-14 (2014)

[13] P.R. Bitterli, J. Brun, T. Bucher, B. Christ, B. Hamberger, M. Huissoud, D. Küng, A. Toggwhyler and Wyniger: Guide to the Audit of IT Applications. ISACA (2009)

[14] R.E.: Cascarino, Auditor's Guide to Information Systems Auditing. John Wiley & Sons publication (2007)

[15] R. Ciprian-Radu; H. Olimpiu; T. Ioana-Alexandra and O. Gheorghe: Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture; Agriculture and Agricultural Science Procedia, vol. 6, pp. 73 – 79 (2015)

[16] R.U. Rehman: Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID, Library of Congress, New York (2003)

[17] Snort Users Manual 2.9.11:The Snort Project; Cisco and/or its affiliates (2017)

[18] S. Senft and F. Gallegos: Information Technology Control and Audit; Auerbach Publications (2009)

[19] T.S. Kumar and P. Radivojac: Introduction to Data Mining:- Lecture Notes (2017)

[20] ISACA: Information Systems Auditing: Tools and Techniques Creating Audit Programs (2016)

[21] The Global Information Assurance Certification (2003), Snort Intrusion Detection System Audit: An Auditor's pers-pective; GSNA practical version 2.1 (2007)

[22] D.E, Robert: IT Auditing: An Adaptive Process. Mission Viejo: Pleier Corporation (2005)

[23] The National Science Foundation-US: Cyber-Physical Systems (CPS) (2020)

[24] T. Phatak; P. Isal, O. Kadale; A. Nalage and S. Bhongle: Smart Intrusion Detection System, International research journal on engineering and technology, Vol. 4, Issue 04 (2017)

[25] R. Alder, A.R. Baker, E.F. Carter, J. Esler, J.C. Foster, M. Jonkman, C. Keefer, R. Marty and E.S. Seagren: Snort: IDS and IPS Toolkit, Syngress publishing, Burlington, Canada (2007)

[26] R. K. Rainer, C.G. Cegielski, I. Splettstoesser-Hogeterp, C. Sanchez-Rodriguez: Introduction to Information Systems: Supporting and Transforming Business, 3rd Canadian Edition, ISBN: 9781118476994 (2013)

[27] W.H.Murray: Data security management: Principles and Applications of Key Management; Auerbach publication (1999)

[28] W. Buchanan: *The Handbook of Data and Networks Security* (1st Edition), Springer-Verlag New York, Inc. Secaucus, NJ, USA (2007)

[29] W. Stallings: Network Security Essentials: Applications and Standards, 4th edition, Prentice Hall (2011).