A Model for the Design of Next Generation e-supply Chain Digital Forensic Readiness Tools

D.J.E. Masvosvere
Department of Computer Science
University of Pretoria
Pretoria, South Africa
dkmasvo911@yahoo.com

H.S. Venter
Department of Computer Science
University of Pretoria
Pretoria, South Africa

Abstract— **The internet has had a major impact on how information is shared within supply chains, and in commerce in general. This has resulted in the establishment of information systems such as e-supply chains amongst others which integrate the internet and other information and communications technology (ICT) with traditional business processes for the swift transmission of information between trading partners. Many organisations have reaped the benefits of adopting the eSC model, but have also faced the challenges with which it comes. One such major challenge is information security. Digital forensic readiness is a relatively new exciting field which can prepare and prevent incidents from occurring within an eSC environment if implemented strategically. With the current state of cybercrime, tool developers are challenged with the task of developing cutting edge digital forensic readiness tools that can keep up with the current technological advancements, such as (eSCs), in the business world. Therefore, the problem addressed in this paper is that there are no DFR tools that are designed to support eSCs specifically. There are some general-purpose monitoring tools that have forensic readiness functionality, but currently there are no tools specifically designed to serve the eSC environment. Therefore, this paper discusses the limitations of current digital forensic readiness tools for the eSC environment and an architectural design for next-generation eSC DFR systems is proposed, along with the system requirements that such systems must satisfy. It is the view of the authors that the conclusions drawn from this paper can spearhead the development of cutting-edge next-generation digital forensic readiness tools, and bring attention to some of the shortcomings of current tools.**

Keywords— Network forensics, e-Supply Chains (eSCs), Digital forensic readiness (DFR), Cyber-Crime, Monitoring tools, Digital forensic data analysis tools, Forensics domains, Digital forensic Investigation (DFI).

I. INTRODUCTION

In the recent past, organisations have become heavily dependent on their computers and networks. Needless to say, the comprehensive use of computers and networks for the exchange of information and services has had a major impact on the escalation of crime through their use [1]. As a result, monitoring such networks has become a mission-critical task.

E-supply chains (eSCs) are becoming an increasingly adopted model for organisations to conduct business. This model encourages organisations to share information and resources in order to achieve improved customer service, speed up business operations and reduce costs. Despite the many benefits that eSCs provide, they also create new avenues for fraudsters. Ayers indicates that current digital forensic tools are not keeping up with the increased complexity and data volumes of modern investigations and insists that the existing architecture of first-generation computer forensics tools is rapidly becoming out-dated [2]. Developments in today's networks, which support both internal and external business processes, call for cutting edge DFR tools that can assist in the collection, storage and retrieval of potential evidence in a forensically-sound manner.

The problem pursued in this paper is that there are no DFR tools that are designed to support eSCs specifically. With all the technological advancements that have occurred over the years in eSCs, there has been very little focus on the implementation of digital forensic readiness within this environment. The EnCase forensic tool and the Forensic Tool Kit (FTK) application, which are the two industry-standard digital forensic analysis tools for digital forensic investigations do not incorporate digital forensic readiness properties in their specifications. Therefore, in this paper, the authors provide an architectural design and blueprint for next-generation eSC-DFR systems along with the system requirements.

The remainder of this paper is structured as follows: section II provides background on eSCs and digital forensic readiness. Section III sheds light on the limitations of current digital forensic readiness tools. Section IV defines the next generation DFR tools; setting out a series of requirements that such tools must meet. In section V the design of the eSC-DFR is introduced, showing the dynamic aspect of the system through the use of a use-case diagram. In section VI the proposed architectural design of the next generation eSC-DFR system is presented and discussed to illustrate how the requirements set out in the previous section may be implemented and to demonstrate the benefits of doing so. Finally, the last section concludes with a discussion about the proposed system and future work.

II. BACKGROUND

In this section, a background on eSCs and Digital forensic readiness is conducted. eSCs form an integral part of this paper because they provide an environment that supports the transmission of information and services between trading

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

partners and customers. DFR provides ways to capture critical data in the eSC environment-data that is crucial for DFIs and information risk assessments in the eSC.

A. E-supply chains

A conventional supply chain comprises of a system of firms, activities, people, information and resources that harmoniously facilitate in the moving of services or products from supplier to customer [3]. An eSC is an advancement of a conventional supply chain, meaning it has additional building blocks, such as web technologies, that contribute to an improved and integrated supply-chain relationship. This relationship is facilitated by web technology solutions that effect information exchange between trading partners and consumers over a distributed network environment. In the next section a more detailed description of the components that make up the eSC environment is given.

B. E-supply chain Architecture

E-supply chains are built on hardware, middleware and software components that work together to facilitate the smooth operation of business processes between trading partners.

Software components such as Supply-chain management (SCM) systems and Customer-relationship management (CRM) systems provide both internal and external services to trading partners and an integrated view of core business processes. These software components, in conjunction with the internet and web services, provide an entry point for an enterprise to access information from other trading partners.

Middleware components, such as application servers and content management systems, are computer software that support enterprise application integration (EAI). Middleware can be defined as programs that provide messaging services, which include enterprise-application integration, data integration, links between database systems and webservers in the eSC.

Hardware components create a communication link between each trading partner in the eSC for the transmission and processing of data. Examples of hardware components include PCs, mobile computers, routers, switchboards and servers just to mention a few, all of which are vulnerable to IT-specific threats. From figure 1 below, the different components that make up an eSC environment are illustrated at a high level. The figure illustrates the structure of an eSC and how the internal infrastructure of a trading partner (TP) interacts with the information hub that supports interactions with other trading partners' internal systems via internet-based protocols [12].

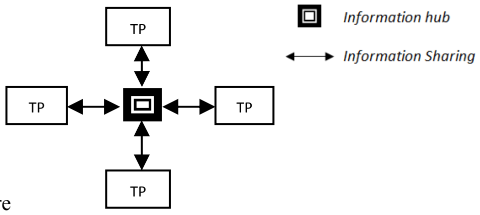

Figure 1. eSC Structure

The eSC network environment is full of potential evidence data that can be used when an incident occurs; that is if data is collected in a forensically sound manner. Therefore, it is the authors' view that a digital forensic readiness system can provide such critical data.

C. Digital Forensic Readiness

Due to the above-mentioned security issues and problems, there is a need for ways to gather digital evidence in a forensically-sound manner. DFR provides different techniques which can be used to address such issues [4]. Rodney McKemmish [4] defines "forensically sound" as a term used in the digital forensics community to qualify and justify the use of a particular forensic method or technology..

Very often digital forensics is called upon in response to an information security incident or computer-related crime. Although this happens in most cases, there are many situations where DFR may benefit an organisation before an incident occurs, providing the ability to gather and preserve potential digital evidence [5]. By definition DFR is the capability of a system to efficiently collect valid digital evidence that can be used in a court of law [6]. It is important for organisations to understand the crucial role that DFR plays as a proactive process in digital forensics and the impact a DFR system could have in a DFI. In an article Rowlingson [6] mentions a number of goals that are essential to DFR. These goals include gathering admissible evidence legally without interfering with business processes, gathering evidence targeting the potential crimes and disputes that may adversely impact an organisation and to minimise interruption to the business from any investigation.

Therefore, the role of a DFR tool in an eSC environment would be to gather such evidence from the eSC network environment and store it in a forensically-sound manner. A digital forensic investigator may therefore require access to potential evidence that will be able to support its position, in the event that an incident occurs. Unfortunately, the current variety of DFR tools do not support forensic readiness processes that maximise the eSC's ability to provide digital forensic evidence. Therefore, in the next section, the authors review some limitations that such tools exhibit.

III. LIMITATIONS OF CURRENT DFR TOOLS

A considerable amount of research has been conducted on the adoption of DFR processes in different network environments. Unfortunately there has not been adequate attention given towards the development of eSC-DFR tools. It is in this paper that the authors identified a number of limitations concerning DFR tools in the eSC category. Limitations include:

- Limited throughput for data capturing devices.
- Poor Usability.
- Compromised Privacy and limited filtering of packets.

- No technical support.
- Centralising the storage of data captured in a distributed network for data retrieval.
- Software errors.

Each of these limitations are elaborated upon in the sections to follow.

A. Limited throughput for data capturing devices

Due to a tremendous increase in network traffic over the years, current DFR tools are struggling to keep pace with network traffic speeds. These tools cannot capture 100 percent of network traffic data at higher speeds [7]. For an investigation to be successful, especially in the DFR arena, as much data as possible needs to be captured.

B. Poor Usability

Most DFR tools do not provide a user-friendly interface for end-users to quickly scan through a visual timeline of an event, deeply interrogate the activity, and understand the context associated with each object [8]. Large amounts of unfiltered data are collected from different network access points and represented in a form that is too sophisticated for an ordinary person to understand; creating a need to improve the GUI, data search and filtering capabilities in DFR tools. Considering that an eSC is a distributed system, there is a need for DFR tools that can capture potential digital evidence at different parts of the supply chain and store it in a central place, where collected data can be retrieved by digital forensic investigators or law enforcement, which would be readily available in the case of an enquiry.

C. Compromised Privacy and limited filtering of packets

Packet sniffing and filtering has its drawbacks [1]. Firstly, only limited filtering on packets received is carried out, resulting in massive post processing. Secondly, no filtering is done based on the packet payload content (which is the critical data that is carried within a packet or other transmission unit). Lastly, as the entire data is dumped into a central database, the privacy of innocent individuals who may be communicating during the time of monitoring may be violated. Therefore, access to captured eSC data is not restricted to relevant potential evidence and relevant parties.

D. No technical support

Commercial Digital forensics tools that offer technical support are generally costly, making it difficult for small to medium-sized enterprises (SMEs) to purchase them [2]. On the other hand, open-source network monitoring tools are very often difficult to use as they do not provide technical support and the ability to gain insight into their inner workings [2]. The validity and trustworthiness of digital evidence is an essential part of digital forensics. This calls the validity of DFR tool to verify that tools meet the requirements of a digital forensics tool.

E. Software errors

Software errors continue to pose a challenge for tool developers. Analysts and other digital forensic tool users are often faced with the problem of unexplained crashes that lead to disruption and often to loss of data [2]. These seem to be caused by a combination of factors, such as design errors in tools and a lack of high-integrity software development practices within the tool. Therefore, software crashes continue to be a significant concern for analysts and improvements to the robustness of forensic tools are crucial for this reason alone.

The authors, in the next section identify some crucial requirements that next-generation eSC DFR tools must incorporate for optimum results.

IV. Requirements for Next generation DFR tools in E-supply chains

The ability of an organisation to gather potential digital evidence from its network environment before an incident occurs is the focus of digital forensic readiness. Therefore the functional requirements of a DFR eSC tool, basically define the services that such a tool must provide; which are

- Monitor and capture all network traffic from the eSC.
- Ensure confidentiality of captured data.
- Exceptional Usability and Availability.
- Provide accessibility to the system.
- Ensure access control to system.

Therefore, the proposed requirements are elaborated in the sub-sections that follow.

A. Monitor and Capture Data from E-supply Chain

The main function of a DFR tool is to provide forensically-sound records of events before an incident occurs [9]. Therefore an eSC-DFR tool should give the user a holistic view of the events transpiring in the eSC. The use of probes and other data capturing techniques ensure that all the events that take place within an eSC are recorded in a forensically-sound manner and incidents are identified. An eSC DFR tool must therefore, have a monitoring component, which is able to monitor and capture (logging) all the events that take place across the IT infrastructure of an eSC communication network. Once the system captures data, it should ensure the safe-keeping of this data in order to ensure that the integrity is not compromised.

B. Confidentiality, integrity and privacy of collected Data

One of the biggest concerns of many organisations is the privacy of their users' sensitive data. An eSC-DFR system must ensure that users' privacy is not compromised. The authors stress that logging facilities and log information which refers to captured data from different parts of the eSC, must be protected against tampering and unauthorised access. An eSC is a highly-targeted environment; therefore it is safe to assume that an eSC-DFR system will also be a target for hackers and criminals [10]. For that reason it is highly critical that such a system be able to provide as much security as possible by employing security measures such as confidentiality, integrity, access control and privacy.

C. Improved Usability and Availability

The usability of an eSC-DFR tool is of utmost importance. Most monitoring tools are not easy to navigate, making it difficult for users to identify incidents when they occur or to just monitor traffic [2]. It is very crucial that an eSC-DFR system be user-friendly, displaying data to trading partners and law enforcement in a manner that is easy to deduce and trace events recorded. The graphic user interface (GUI) of such a tool must provide users with enough flexibility to either view, download, search categorically and filter captured data. A digital forensic investigator must be able to sign up, login and navigate through captured data effortlessly. Hence, the availability aspect of such a tool is crucial in its design. A DFR tool must be able to perform all its designated functions, that include providing forensically sound captured data to users upon demand. It is therefore crucial that usability and availability tests be conducted to ensure that the system meets its intended functions.

D. Having an accessible system

Since an eSC is a web-based system, an eSC-DFR system must also be web-based, providing services to law enforcement agents and digital forensic investigators from this platform. eSC network developers must integrate the eSC-DFR system with the eSC system, giving the tool access to the systems that are in the e-supply chain network (trading partner systems) for data capturing purposes. The system must direct all captured data to a central eSC-DFR system repository server where it is securely stored. Any system errors or alarms raised by a trading partner's internal system must also be captured by the eSC-DFR system and stored in the repository server, where records can be retrieved once a user logs in to the eSC-DFR system.

E. Access control of Data retrieval

Considering that eSC DFR tools have to be web-based, strict authentication and access control measures must be implemented. Different entities must be allocated different roles within a DFR tool. Therefore, it is proposed that an eSC-DFR system limit the access rights of different users as a privacy and confidentiality measure, in order to ensure that users only access relevant potential digital evidence from the eSC-DFR system. This requires that the system be able to store meta-data about different users, which include the system administrator, trading partners, digital forensic investigators and law enforcement agents.

In the next section the authors present a high level use-case diagram to show an outside view of the proposed eSC-DFR system and show how such a system interacts with its users and other software.

V. ESC-DFR SYSTEM USE-CASE DIAGRAM

A use case diagram is widely used to capture the dynamic aspect of a system, displaying steps a user needs to follow to reach the goal as well as how the various components interact with a user. In this section the authors make use of a use-case diagram to show the high-level view of an eSC-DFR system and the interactions between actors of the system with the system itself. The authors identified three main actors i.e. eSC trading partner systems, system administrator and law enforcement agents/Forensic Investigators, depicted in the use-case diagram in Figure 2. Each actor is discussed in the sections that follow and an illustration of the roles that each user executes are also depicted in the figure.

For the system to work effectively, there are conditions that must be met. Namely, each user must have an account with the system as a system administrator, law enforcement agent or digital forensic investigator. Furthermore, the eSC network must incorporate the eSC-DFRsystem.

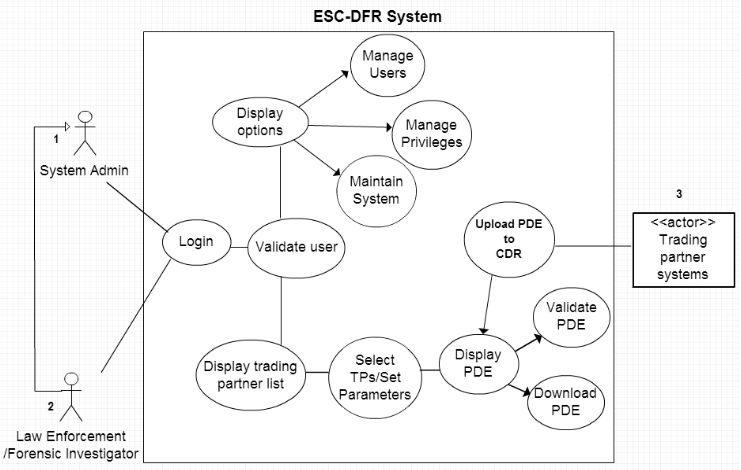

Figure. 2. ESC-DFR System use-case diagram

In the sections that follow, each actor is defined, illustrating the role that each user of the system executes.

A. System Administrator

The system administrator (actor number 1 in Figure 2) represents the person responsible for maintaining the eSC-DFR system. This user must have full access rights to the administrative aspects of the system, ensuring that the system is configured correctly. It is the role of a system administrator to manage user accounts, manage user privileges and maintain the system. It the role of the system administrator to implement any updates to the system that add new features and resolve bugs. It is important to note, that all other users in the system are dependent on the system administrator as illustrated in the use-case diagram in Figure 2.

B. Law-enforcement agent/Digital forensic investigator

Actor number 2 represents a law enforcement agent or digital forensic investigator, responsible for downloading, analysing and validating collected potential digital evidence (PDE) from the eSC-DFR system. This actor is granted access to the system to view, download and validate the potential digital evidence captured from the eSC. The regulation of access to captured data is critical within an eSC business environment as organisations might want to maintain a level of privacy concerning their business operations. Therefore, strict authentication measures ensure that a user is validated and granted access to relevant data only.

C. Trading Partners Systems

An eSC is a distributed business network environment; made up of multiple web-based trading partner systems that interact with each other through an information hub, sharing information and services [11]. Therefore, a DFR tool that operates in this environment has to be integrated with the information hub and trading partners' web-based systems (actor 3) to capture data coming in and out of these systems and upload it to the eSC-DFR system. Captured data might be in the form or information requests and responses sent between trading partners through the information hub, eSC system modifications on trading partner systems or other system data such as alarm system data. The eSC-DFR system may use an internet browser for users to access the system, considering that it is a web-based application. Furthermore multiple web servers may be involved in performing different functions such as secure storage, run applications and so forth.

In the next section the design of a next generation eSC DFR system is presented, showing the system's components and how the system operates.

VI. The Design Of Proposed E-supply Chain DFR System

In this section the authors propose a model for the design of an eSC-DFR system. The model is illustrated with two significant views; a high-level structure in figure 5 and a more detailed logical view of the design in figure 6. In figure 4 an activity diagram illustrates the services provided by the system to its users (digital forensic investigators).

Section *A* provides a hypothetical scenario to illustrate how the eSC-DFR system could benefit both trading partners and digital forensic investigators.

A. Hypothetical Scenario

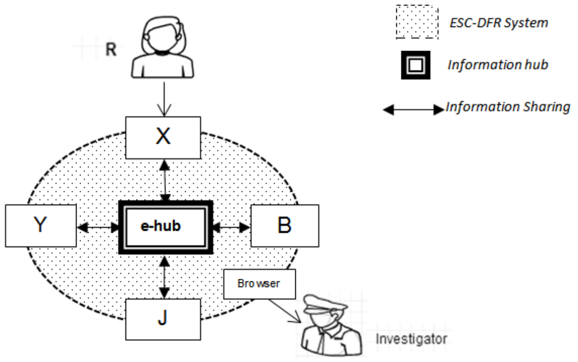

Figure. 3. A small eSC network

In the provided scenario, e-hub is a service provider (information hub) that connects suppliers, retailers and consumers in real time. It allows retailers to sell supplier products that they do not keep in stock on their webstores; connecting Product Catalog Data, using Selling and Fulfilment Tools and lastly making use of Transaction Processing. X is a web store that is connected to the e-hub network, selling Y and J's products. Both Y and J are suppliers running massive warehouses. A malicious employee R who works for X decides to install a malicious code on X's web server that infiltrates the e-hub network, attacking other trading partners Y, J and B's web-based systems. After J, Y and B realise that their systems are being attacked they decide to call upon a digital forensic investigator to assist them with the investigation. With the e-hub network intergrated with the eSC-DFR system (that extracts PDE and log information on each trading partner's web system) that is connected to the e-hub network. The forensic investigator should be able to retrieve readily-available digital evidence pertaining to the incident. The evidence captured could lead directly to trading partner X's webstore, showing the installation of a malicious code and the changes made by the malicious code on trading partner X's web-based system, the time of events and maybe who was logged in at the time of incident. Through the user-friendly eSC-DFR system, the investigator must be able to narrow down from all the captured data to the specific events related to the incident.

Figure 4 illustrates the behaviour of the system when a forensic investigator logs into the eSC-DFR system.

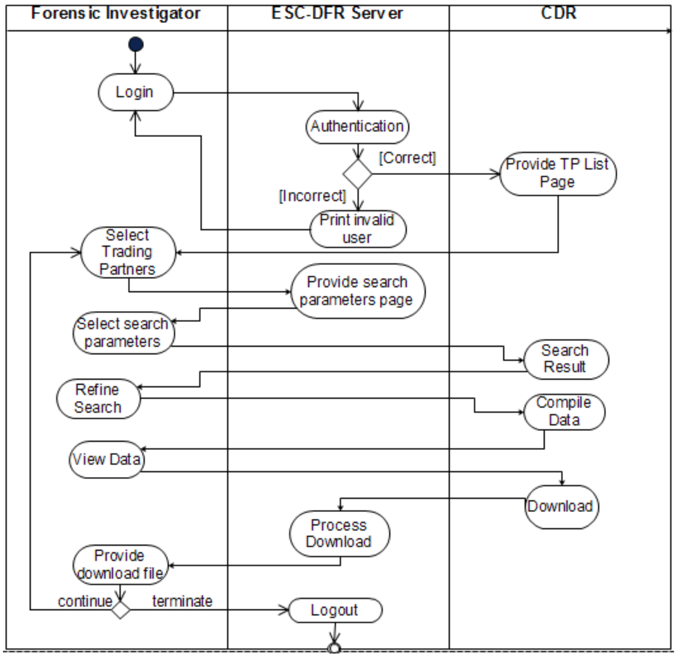

Figure. 4. Digital forensic investigator and law enforcement interacting with ESC-DFR system.

The eSC-DFR system will request that the user enters username and password. If invalid, the system will output an error message and return to the login page. If username and password are valid , the system will retrieve the list of trading partners (TPs) from the central data repository (CDR) and present it to the user through a GUI. From the list, the digital forensic investigator can select the trading partners being investigated. The system will return a search parameter page for the user to search for specific data that is relevant to the selected TPs. The user can then narrow down the search to specific data types, specific time period and send request to database. The CDR compiles the selected trading partners logged data and allowing the user to view the PDE, download the data, logout or return to the trading partner list page. Thereafter the forensic investigator with the PDE can commence the investigative processes.

In the next section, the authors present and discuss the high level eSC-DFR system architecture.

B. High Level ESC-DFR System architecture

There are two essential elements to the discussion of the eSC-DFR system, namely the eSC network and the eSC-DFR component. These elements combined provide a platform for DFR to be achieved across the eSC. The eSC network is an important aspect in the architectural design of the eSC-DFR system because it is the environment where PDE is extracted, with infrastructural components that are critical to the implementation of DFR in the eSC. Some of the components are discussed in the following sections.

The eSC-DFR component provides DFR services to DFI's and law enforcement. Such services include eSC PDE capturing, PDE storage, eSC incident prevention and eSC PDE retrieval. The DFR components that are intergrated with the eSC network infrastructure enable data capturing in the eSC network. Hence, communication between the eSC-DFR component and the eSC network through web protocols and IT infrastructure is a key part of the eSC DFR system architecture as illustrated in Figure 5. This allows PDE to be captured in the eSC network and securely stored in the CDR.

Figure 5 illustrates the integration between the eSC network and the eSC-DFR component, showing the transporting of captured data to the CDR (1) and the requesting/retrieval of PDE at the eSC-DFR component (2).

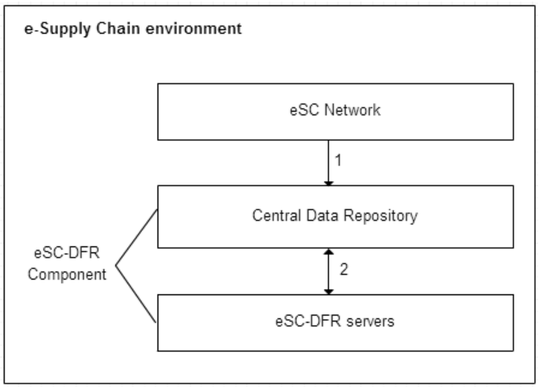

Figure. 5. High level architecture of eSC-DFR system

In the next section a more detailed model of the eSC-DFR system is presented and some critical components of the system are discussed.

VII. Model of the Esc-DFR System Architecture

Figure 6 illustrates a more detailed model of the eSC-DFR system and its key elements. It must be noted that with further research, more components might be added to the proposed model.

As mentioned previously there are two key components in the proposed architecture. One is the eSC network and second is the eSC-DFR component. Both components utilise secure protocols such as the SSL protocol to transmit data over the web; from the eSC network to the eSC-DFR component. There are elements that are critical to both the eSC-DFR component and the eSC network. Such elements include the eSC host servers and deployed logging probes; which are located in the eSC network shown in Figure 6.

In the eSC-DFR component there are 4 key components, the CDR, database management system, eSC-DFR server and a content management system which interacts with the database management system located in the CDR shown in Figure 6 below.

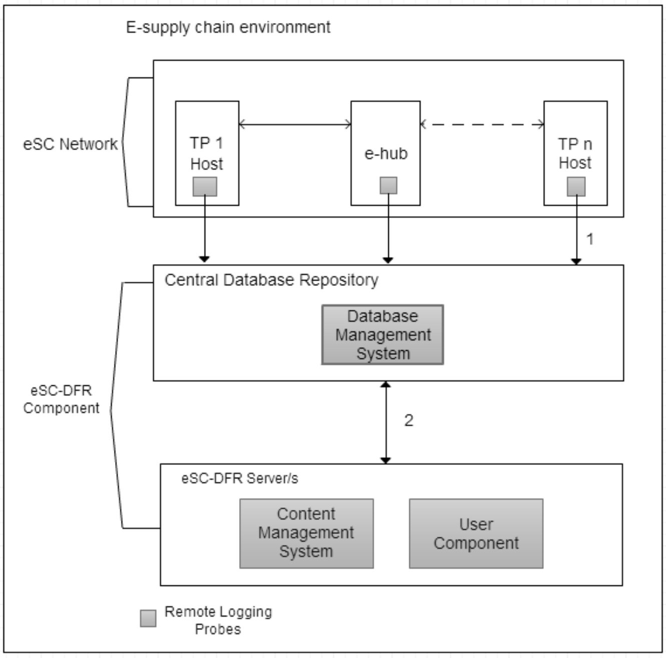
E-supply chain environment
eSC Network
TP 1 Host
e-hub
TP n Host
1
Central Database Repository
Database Management System
eSC-DFR Component
2
eSC-DFR Server/s
Content Management System
User Component
Remote Logging Probes

Figure. 6. Architecture of the ESC-DFR System

As mentioned in section *B,* PDE is captured in the eSC network by the deployed probes and sent through to the CDR; where it is processed by the database management system (DBS) and stored. In an event that an incident occurs, digital forensic investigators and law enforcement agents can retrieve captured PDE from their work stations through the user component that connects them to the content management system. In the sub-sections that follow, the authors take a deeper look into the role that each element illustrated in Figure 6 performs in the eSC-DFR system.

A. Remote logging probes

Remote probes generally offer a number of different functions for different scenarios. In this scenario, the main function of such probes is to extract critical information about the eSC network from the host machines, compute digital signatures and initiate the transmission of captured data from the eSC network across the web to the eSC-DFR component. PDE might include firewall data, system log files, erased files, temp files and sniffed packets depending on the configuration of the probes. Considering that the eSC network and the eSC-DFR system are integrated, the logging module has to be incorporated in the code of the eSC System application. Once the eSC system is installed onto a trading partners host machine, the probe must start capturing system activity and initiate communication with the eSC-DFR component.

For such communication to take place, it is important to establish a connection between the eSC network and the CDR server. This might require that all the necessary ports in the eSC-DFR component firewall be opened. To ensure the security of transmitted data, the remote probes must send the captured data through secure channels such as the SSL protocol. This is to ensure that data sent back and forth from different parts of the eSC-DFR system is not visible to intruders.

The logging probes collectively must be able to record the entire procedure leading to an incident. They must be able to identify, where requests and responses in the eSC network are coming from, the time when requests are sent and received, protocols being used and type of data being transmitted between entities in the eSC. For improved performance a number of remote probes can be deployed. This number is based on the number of eSC hosts being monitored and the eSC network traffic throughput.

B. E-supply chain DFR server

The eSC-DFR server resides in the middleware tier discussed in section II. This component provides middleware services that include system security, system maintenance, content management, system configuration and user management. The server ensures that all the DFR processes are systematically executed in the eSC, also providing authenticated user access to the system's functions. It is important to mention that the eSC-DFR system might incorporate a server cluster. This means that the functions that an eSC-DFR server executes might be spread over a cluster of servers, running simultaneously and working together to provide increased scalability. The main functions of a content management system (CMS) are to send requests to the CDR and retrieve data from the CDR, organise them in the eSC-DFR server and provide controlled access to data[11]. The eSC-DFR server can be presented using the layered approach, with a presentation layer, services layer, business logic layer and data layer that all perform different roles.

C. Database server (4)

The central database repository (CDR) is where captured data from different parts of the eSC network is stored, including eSC-DFR system files, metadata and user profiles. The CDR can be defined as a central place where data is stored and maintained or a place where data is obtained for distribution across a network. When information is transmitted across the eSC or actions are executed on trading partner systems, deployed eSC-DFR system infrastructure will capture as much data pertaining to the those events and send that data to the CDR. Where the captured data is processed by a database management system (DBMS). A DBMS can be defined as a program or collection of programs that manage incoming data, organise the data, and provide ways for that data to be retrieved by users or other programs. It is the view of the authors that an eSC-DFR system might require large volumes of storage, depending on the size of the e-suppy chain and considering the amount of data collected from different parts of the ESC network. Hence, issues of big data might arise but are not discussed in this paper. The database management module handles the structuring of PDE and retrieval of stored data. With the help of the (CMS) in the eSC-DFR server, users can access the eSC-DFR system content with relative ease.

VIII. Architectural Aspects

Considering that the key functions of a eSC-DFR system are to capture PDE and to securely store the captured PDE for retrieval, it is safe to assume that the most critical elements of such a system are data capturing, secure storage and system reliability. Therefore, in this section the authors elaborate further on the design of the remote probes as indicated in Figure 6 and key factors to consider for system reliability and secure storage.

A. Design of Remote Probes

A remote probe in general can be seen as an object used for data extraction. Data includes system log files, Intrusion detection system log files, system configure files, temp files and network packets [11]. Within an eSC environment, this capturing module would be installed within each trading partner's host machine where it can capture data concerning the eSC system and send captured data to the CDR, where all captured data is stored [11]. In Figure 7 the authors display the adapted architecture of the remote probes.

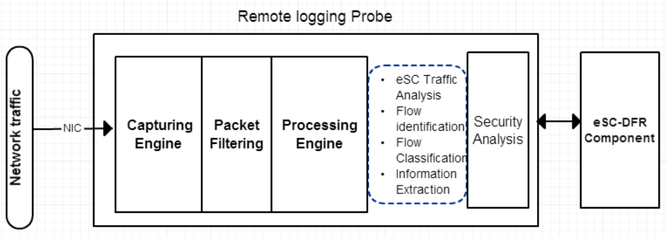

Figure. 7. Remote probes

In an eSC environment information is shared and transmitted at fast rate; many transactions are conducted by different trading partners. It is for that reason that a probe capturing PDE in this environment needs to be able to handle the rate at which data is transmitted.

As stated in section III, current limitations in DFR tools include limited throughput. Hence, as a measure to ensure that the eSC-DFR system is able to cope with the high-speed traffic, the authors propose the use of a kernel-level multi-processor traffic probe that captures and analyses network traffic in high speed networks [11]. This solution is based on execution threads that are designed to take advantage of multiprocessor architectures. The network interface cards (NIC) within the eSC host machins direct the network traffic to the probes where it is captured by the capturing engine. In the eSC-DFR system the probes as illustrated in Figure 7 are responsible for capturing eSC network traffic, filtering through captured traffic (based on their protocol or IP address), capturing system data related to the eSC network on host machines and processing/analysing captured traffic before it is sent to the CDR for storage.

B. Evidence storage and system reliability

It is no secret, that digital forensic workloads are characterised by large volumes of data and the need for high data throughput is in fact real. Therefore, it is in the authors' opinion that improvements to data capturing rates and data transfer rates will definitely improve the performance of an eSC-DFR system. A suggested solution would be to use clustered or parallel file systems where a user reading data from the eSC-DFR system is actually receiving data from multiple physical servers at once. This would mean that a user's read rate can exceed the maximum network I/O bandwidth of a single server. This supports the idea that was stated by Ayers that the performance of clustered file systems is greatly increased when servers and clients use teamed network adapters to increase bandwidth [2]. The eSC-DFR system will incorporate a module for managing the capturing of potential evidence and maintaining a detailed record of all tasks executed users by the system.

Making sure that the system is reliable is also of utmost importance, especially considering that this system must provide services to businesses of all sizes. Hence, the proposed system has to be carefully designed and implemented to ensure that the system is highly robust. The use of modern software engineering techniques has to be considered to ensure that the system is as secure, robust and versatile; able to handle any unforeseen software errors while minimising the risk of data loss.

While there is room for more thorough optimisation of the eSC-DFR system, it is in the authors' opinion that the core elements that are included in the proposed design validate this approach.

IX. Discussions

The primary objective of this research was to design a high level architecture of an eSC-DFR system that can provide useful data to digital forensic investigators and law enforcement agents to aid in digital forensic investigations and other processes that might require such data. From the limitations identified in current DRF tools. The proposed architecture is designed to cater to the security needs of an eSC environment specifically, ensuring that the eSC is forensically ready. It comprises of a secure eSC-DFR system web server, remote logging probes that are strategically deployed in the eSC network, a central repository database for storage of PDE and a user component that provides users with controlled access to the system. The authors identified the need for next generation DFR tools that:

- Can handle high throughput that passes through eSC information networks.
- Are robust and can meet DFR toll requirements.
- Can present captured PDE in a comprehensible manner.
- Are able to maintain a level of privacy for trading partners.
- Provide users with uncompromised forensically sound data.
- Collect data on supplier's supplier relationships.

Considering that an eSC environment may comprise of many entities, the proposed architecture was designed to handle large amounts of potential evidence data. It is in the authors' opinion that software developers must ensure that the capturing and storage components of such a system can capture data at high speeds and accommodate large volumes of data. Also considering that an eSC is a distributed network environment connecting retailers to suppliers and suppliers to more suppliers. The architecture of the eSC-DFR system is designed to cater to those kinds of relationships. The deployment of remote probes as data capturing modules onto host systems in the eSC network ensure that potential digital evidence is captured across the eSC.

As mentioned earlier in the paper, a major requirement of a DFR tool is that it must ensure that the integrity of captured PDE is not compromised, thereby meeting digital forensics standards. Therefore, the use of secure communication protocols and remote probes is incorporated in the proposed architecture. The use of encryption and digital signatures amongst other methods are suggested to maintain the integrity of captured data. Also a specialised probe design was incorporated to ensure that the capturing of high speed traffic is accomplished [11].

It has been strongly emphasised by the authors that ease of use that a DFR system provides and its ability to present captured data in a comprehensible manner is of utmost importance (Usability). Therefore in this paper the authors emphasise the importance of paying close attention to the design of a usable graphic user interface; making the eSC-DFR system easy to navigate and the time taken to retrieve captured evidence and trace events is greatly reduced. Hence, developers must ensure that much attention is placed on the usability aspect of the system.

The strict authentication of users through the security component in the eSC-DFR system architecture ensures that a level of privacy for sensitive data is maintained. It is of great importance to stress the point that the eSC-DFR system is a system designed to serve law enforcement and digital forensic investigators to solve cases and monitor the eSC. Therefore, rights of access must be strictly monitored to ensure that only validated users are granted access to the system. Therefore, measures taken to control access and at the same time maintain a level of flexibility for users must be considered in the development of such a system.

It is evident, that the use of IT comes with numerous challenges that can cost organisations large sums of money. Although the effectiveness of a DFR system can only be fully comprehended through an assessment of the system, the authors believe that the proposed eSC-DFR system can help organisations avoid incidents in the eSC. Also such a system can assist law enforcement agents and digital forensic investigators by providing readily available digital evidence that can be used in the investigative processes.

X. Conclusion

Existing general purpose DFR tools are rapidly becoming inadequate for modern commercial network systems (eSCs). The out-dated architecture of such tools limits their ability to scale and adopt the current and future eSC forensic readiness processes. In the recent past, researchers have cited the need for more capable DFR tools that can support digital forensic investigations in the event an incident occurs. As much as these are steps in the right direction, implementing security policies and processes alone does not ensure that the eSC environment is fully forensically ready.

This paper proposes a model which can be used as a blueprint for the design of next generation eSC-DFR systems that can fully cater to the DFR requirements of such an environment. The eSC-DFR system is a useful tool for collecting data and monitoring the eSC environment. The design of the proposed system is built around improving the user experience and providing adequate forensically sound data to trading partners and law enforcement agents about all trading partner interactions. The use of kernel-level multiprocessor network probes ensures that no data is lost during the packet capturing process. The authors also acknowledge that an eSC handles large amounts of data that are transmitted upstream and downstream the supply chain, hence the eSC-DFR system provides clustered storage to increase the performance, capacity and reliability of the system.

In this paper the authors were able to discuss the limitations to current DFR tools and requirements for next-generation eSC-DFR tools where proposed. An early high-level design for a practical next-generation eSC-DFR system was presented. The design and implementation of such as system is on-going. The system incorporates strategies for optimising and managing potential evidence data collected from different parts of an eSC. For future work an implementation of the eSC-DFR system is necessary, also providing a look into the performance of the proposed system. This would assist in verifying whether the proposed system accomplishes what it is intended to accomplish.

References

[1] B. Pande, D. Gupta, D. Sanghi, and S. K. Jain, "The Network Monitoring Tool-PickPacket," in Information Technology and Applications, 2005. ICITA 2005. Third International Conference on, 2005, pp. 191-196.

[2] D. Ayers, "A second generation computer forensic analysis system," digital investigation, vol. 6, pp. S34-S42, 2009.

[3] S. D. Pathak, D. M. Dilts, and G. Biswas, "Next generation modeling III-agents: a multi-paradigm simulator for simulating complex adaptive supply chain networks," in Proceedings of the 35th conference on Winter simulation: driving innovation, 2003, pp. 808-816.

[4] D. Barske, A. Stander, and J. Jordaan, "A Digital Forensic Readiness framework for South African SME's," in Information Security for South Africa (ISSA), 2010, 2010, pp. 1-6.

[5] R. Rowlingson, "A ten step process for forensic readiness," International Journal of Digital Evidence, vol. 2, pp. 1-28, 2004.

[6] B. Endicott-Popovsky, D. A. Frincke, and C. A. Taylor, "A theoretical framework for organisational network forensic readiness," Journal of Computers, vol. 2, pp. 1-11, 2007.

[7] L. Pulevska-Ivanovska and N. Kaleshovska, "Implementation of e-Supply Chain Management."

[8] R. G. Clegg, M. S. Withall, A. W. Moore, I. W. Phillips, D. J. Parish, M. Rio, et al., "Challenges in the capture and dissemination of measurements from high-speed networks," arXiv preprint arXiv:1303.6908, 2013.

[9] G. Disterer, "Iso/iec 27000, 27001 and 27002 for information security management," 2013.

[10] G. Smith, K. Watson, W. Baker, and J. Pokorski Ii, "A critical balance: collaboration and security in the IT-enabled supply chain," International journal of production research, vol. 45, pp. 2595-2613, 2007.

[11] L. Zabala, A. Ferro, A. Pineda, and A. Muñoz, "Modelling a Network Traffic Probe Over a Multiprocessor Architecture," Edited by Jesús Hamilton Ortiz, p. 303, 2012.

[12] D. Masvosvere, H. Venter, “A Conceptual Model for Digital Forensic Readiness in e-Supply Chains”.