ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

NETWORK FORENSICS TOOLS IN A MIXED-NETWORK ENVIRONMENT AND THE ADOPTION OF E-VOTING SYSTEM IN DEVELOPING COUNTRIES

Oluranti Jonathan[1], Funminiyi Olajide[2], Charles Ayo[3]
Department of Computer and Information Sciences, Covenant University Ota, Nigeria.
Email: jonathan.oluranti@covenantuniversity.edu.ng

Received on: 20.10.2016 *Accepted on: 25.11.2016*

Abstract

This paper unveils e-voting malpractices and discusses the application of network forensic tools. The paper also presents an introduction to digital forensics with emphasis on network forensics for acquiring digital evidence in a networked environment of an e-voting system. The research adopts qualitative assessment of the various issues of crime or malpractices in e-voting system as it relates to a network environment or distributed applications. Computer networking forms the bedrock of the operating platforms for most modern business organizations and more recently, distributed applications.

This research brings to light the various possible anomalies or issues that a typical e-voting system in a network environment may witnesses per phase of the election. The phases of a typical election include registration, authentication, voting and vote counting and reporting. The research also presents various network forensic tools that can serve to mitigate or eliminate some of the identified anomalies. This research is suitable for election forensics as it will lead to the evidence required to authenticate the transparency and accuracy or otherwise, of a given election. Thus e-voting falls under the category of network-based applications for which network forensics is applicable. The tools recommended are proven tools for forensic investigation and will also serve for electronic-based elections that is, e-voting.

Keywords: Electronic Voting, Network Forensics, Election, Evidence

1. Introduction

In a democratic society, voting constitutes an important activity through which members of the society elect the people that govern them[1]. Voting systems have existed as the traditional paper ballots for voting including the mechanical devices or electronics ballots for elections[2]. Most of these voting systems have been characterized by incidences of election manipulations with the aim of influencing the result of the elections. There have been

allegations of violence, intimidation, ballot stuffing, under-age and multiple voting with errors in counting, absences or late arrivals of election materials and with a host of other issues [3].In spite of this however, some voters today still have faith in the traditional voting system mainly because they are used to the paper ballots, based on the fact that the paper ballots can be recounted where necessary. The traditional method requires more expenses and involves more social and human resources. This is why researchers have put much effort into finding solutions to the problems identified with the traditional voting system. The research has been further enhanced by the development of computer networks which enable computers, applications and other devices to communicate and share resources, leading to what we know as electronic voting (e-voting) system.

E-voting unlike the traditional method of voting, is very convenient for the voters as it makes it possible for them to cast their votes via a network. In some cases, voters do not even need to be at the polling station to cast their votes. Voters can use their personal computers or devices with an internet connection. The e-voting method therefore, can reduce election expenses and avoid voting errors.

An e-voting application relies largely on computer networks including internet to store and transmit data during and after elections. E-voting systems like other network-based applications have their own challenges ranging from unexpected and unexplained incidents. The phases of the election process include preparation, balloting, tabulation and reporting results which are liable to known attacks like denial of service (DOS), hacking and a host of others. In[4], reported an attack on the electronic data systems upon which the integrity of the voting counting depended. This was done with the intention of creating false results. In fact a number of countries have had to discontinue e-voting system projects on the account of insecurity[5].

Although the internet voting (i-voting) system of Estonia has never faced an attack from a hostile power, a recent study on it found a number of loop holes that if exploited could lead to disruption of the entire voting process[4]. The cause and scope of the anomalies identified in e-Voting systems cannot be determined immediately and this is where the application of forensics techniques comes into play. Forensic tools can be applied to review and investigate the entire election process if possible when it has been determined that something went wrong or may have gone wrong.

This paper presents a brief description of an e-voting system especially as it relates to developing countries. The paper also presents e-voting system as an internet or network-based applicationin comparison to other internet-based application that provide various services like e-commerce, banking phone directory, among others. E-voting system activities as related to fraud or malpractices are also presented. In other sections, we introduce network forensics, its

tools and their application to e-voting system. We also present sample cases of e-voting application violation like hacking for which network forensics tools are useful. Finally, we suggest network forensics tools that are useful in typical e-voting application operating environment which is usually a mixed network environment consisting of both wireless and wired LAN or WAN.

2. Background Information

A number of issues usually come up during an election. For instance, a card reader might fail to read cards for voter accreditation as was the case in Nigeria during the 2015 general elections. In fact, the electoral body had to quickly fall back to the manual means of accreditation which is prone to errors. Not only that, the voting equipment itself might fail to work or freeze up at the point of voting.

Although, election officials might try to resolve some of the issues immediately, there may still be issues that may not be resolved immediately and that may eventually affect the result or general conduct of the entire exercise. Such incident can result to candidates contesting the outcome of the election and requesting for a recount if not a rerun of the election.

In resolving some of these issues, it becomes necessary to carry out what is called 'election forensic' where the issues are analyzed for the discovery of the root causes and possible remedy of the technical issues during the election[6].

Election Forensics may include computer forensics where the unexpected behavior of the computer is determined. Computer forensics can also determine whether the total votes were affected or attempt to recover missing or damaged voting records.

Our focus here is on computer-based forensics since e-voting is a computer machine comprising of both hardware and software for conducting an election in a network environment.

3. Electronic Voting (E-Voting) System

Electronic voting (E-voting) refers to a system of voting that makes of use of electronic devices.E-voting system is designed to perform exactly the steps in the traditional methodbut in this case the use of computer systems has been incorporated[7].

However, E-voting has been classified as supervised and unsupervised mode[8]. The supervised mode is where a voter visits the polling station (a kiosk)to cast his or vote. The election officials monitor the entire exercise here and identify and accredit every voter before they cast their votes. To vote, voters move to a computer or machine where they press or push buttons to cast their votes.

The second type of E-voting system is the unsupervised mode which is based on remote technology[8]. In this mode, election officials are not present at the point of voting but voters are solely responsible. Voters do not go to any polling station to cast their votes but instead use their devices such as mobile phones, personal computers and others. Voter devices will usually connect to the main servers or stations via the internet or GSM networks. However, voting must be done within the stipulated time for the election. This is one of the major advantages of remote electronic voting as voters can even vote abroad.

The general name for this category of e-voting is Internet voting or i-Voting.Figure 1 below describes the basic steps of voting in any type of election or voting system either traditional, supervised or unsupervised, polling site-based e-voting or remote e-voting.

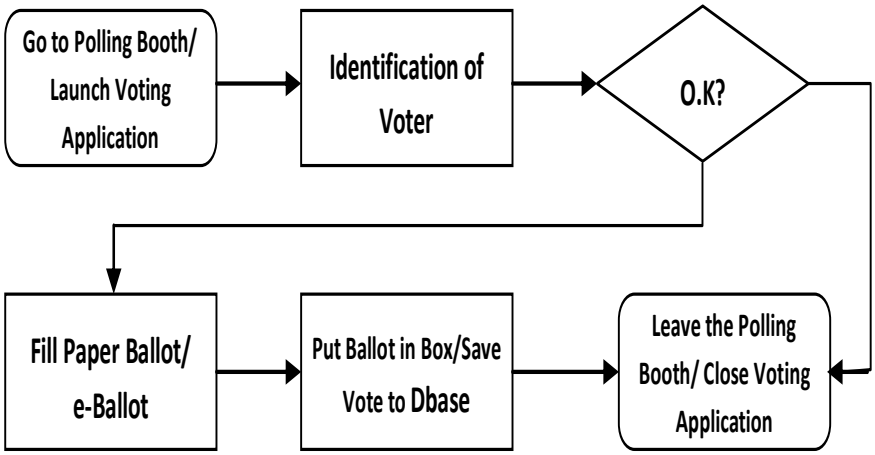

Figure 1: Generic Voting Procedure for Traditional and Electronic Voting (Abdallah &Samani, 2013).

There is more interest for i-voting these days as people are now getting used to Internet-based services. They are wondering why it is not possible to successfully vote via the Internet the same way we buy and sell goods and services over the Internet e-Commerce solutions without any concerns. Based on this, voting on the Internet could be viewed as a transaction with some unique aspects. A typical financial transaction (e-Commerce) is an end to end process with valid proof connecting a buyer and a seller. This means that for online voting, we must be able to link a voter to a vote. This may however negates some of the principles of voting like secrecy, anonymity and coercion-free. However, developers of online voting applications should put this into consideration as they try to achieve absolute audit-trail ability.

3.1 E-Voting System Threats and Vulnerabilities

Threats to e-voting systems exist in different forms and can affect the voting system in several ways. The resultant effect of these threats is that they lead to voting systems that are not trustworthy. A number of these vulnerabilities can be exposed by forensics tools which are discussed below:

3.1.1. Denial of Service

This type of attack has devastating consequences. The attack usually makes it impossible to access a system or a resource thereby making it appear that the resource or service is not available. There are two ways this type of attack is carried out by hackers[9]. This may be experienced in e-voting systems being a network-based application.

3.1.1.1 Ping of Death

The intention of this method of attack is to fill up the memory allocated for storing packets until there is no more space which will then lead to the crashing of the remote system receiving such packets. For example, this trend of cybercrime may be used to perpetrate attack into any e-Voting application such like in developing countries where hacking activities are high. The attack relies on a defect in some TCP/IP stack implementations. However, the attack affects systems differently. For some it will lead to their crashing while some others may remain unaffected but unavailable[10].

3.1.1.2 Packet Flooding

In this category of attack, the attacking host sends numerous packets to another host without responding with an acknowledgment to the receiving host. This is traceable to man-in-the-middle attacks prone to e-voting election preparation when systems are deployed ahead of campaigns. In this case of packet flooding, the receiving host keeps waiting for more and more acknowledgements until its buffer queue gets filled up and it can no longer accept legitimate connections. This type of attack takes advantage of the three-phase handshake between the systems.

3.1.2 Viruses

A virus is a computer program that is capable of reproducing itself to cause damages to computer files and programs. A virus usually attached itself to programs or code that a user is likely to execute. This is one of the tricks of cybercrime attacks that can influence e-voting application but with the “election forensic”,this can be minimized or uncovered.

Viruses can compromise the availability of an e-voting system at election time and this can result in the postponement of the election [10].

3.1.3 Worms

A worm is a type of virus that copies itself within its victim and then spreads to other systems to become active. This type of virus is highly destructive and has affected many organsation such like Facebook and was classified as “sophisticated attacks”.

This virus can overwrite portions of the files with random data. The damages caused by worms are usually not repairable necessitating the re-installation or restoring from a backup. This type of attack can affect smooth operations of an e-voting system if care is not taken. Worms can also overwrite files and change election if programmed to do that. This affects the integrity of the entire process[11].

3.1.4 Trojan Horses

These are malicious pieces of computer code that get downloaded to victim's computers when they connect to internet. Some Trojans are harmless while others can be very destructive to the extent of modifying important files on the computer, steal users' passwords or even transform into a virus. With Trojans, all forms of fraudulent schemes are possible for example, in the recently concluded general election in Nigeria, it was mentioned that possibly, but not confirmed information about hackers' manipulation attacks on servers at the INEC office. This may be traceable to Trojan Virus in which an application was dubiously or unknowingly opened by a user. Trojans gain access to passwords and other personal information and disseminate same to the attacker. Thus Trojans put the confidentiality and integrity of an e-voting system under threat[12].

3.1.5 Physical Attacks

An e-voting system is not confronted by only intangible threats. Tangible threats by way of physical attack on the e-voting system infrastructure also exist. For instance, the equipment may be physically vandalized or can even be stolen some few days or moments to the Election Day. Saboteurs may also cut off network connections to e-voting machines resulting in the lost of votes. Attackers may even go to the extent of replacing hardware and the smart cards data with false data. All these are threats to e-voting and may affect the entire process negatively or may result in loss of interest in the e-voting systems.

Table 1 below shows a summary of e-voting vulnerabilities and counter measures as you move from phase to the other i.e. registration to voter verification to voting and counting of votes

Table 1: Summary of Risks and Counter Measures of E-voting Phases.

	Registration Phase	**Authentication Phase**	**Voting Phase**	**Counting and Reporting Phase**
Risks	Lower risks: Attacks could target availability, confidentiality, or authentication of the system.	Lower risks: Attacks could target availability and authentication of the system.	Very high risks: Attacks could target availability, confidentiality, or authentication of the system.	High risks; DDOS attacks are possible to keep all voting locations from reporting, but the main threat is against integrity.
	DDOS attacks can	If separate servers are	DDoS attacks can	Intruders could potentially

	overload servers preventing voters from registering	used for verifying voters, then the verification servers can be separately targeted for a DDoS.	overload servers, preventing voting, especially if elections are held on a single day.	break into election servers and change previously cast votes.
	Intruders could read personal info, submit false info, or even change info on voters	Attackers could also take the place of legitimate voters through phishing attacks, tricking users into revealing their credentials.	Attackers could potentially impersonate legitimate voters, or monitor network traffic to see how individuals voted.	
Counter Measures	To prevent DDoS, properly design networks and contract for more network bandwidth at critical times, such as just before registration deadlines. Cryptography, secure software, and strong access control beyond passwords – including biometrics data such as fingerprints – can help keep intruders out of the system. Nontechnical controls also help, such as mailing physical registration cards for people to confirm details.	Basic and effective methods for electronic authentication are relatively cheap and easy to deploy. The best solutions will use strong access control beyond passwords, such as biometrics or a smart card and personal PIN	To beat DDoS, properly design networks and contract for more network bandwidth during voting day. Cryptography, secure software, and strong access control beyond passwords – including biometrics are a must to ensure votes are not stolen. For extra security, voters could use a preconfigured bootable USB or CD in their PC, guaranteed free of malicious software. Nontechnical controls also help, such as voting over an extended time period.	Cryptography, secure software, and networks; and strong access control beyond passwords must protect election servers and the accounts of the users and especially systems administrators Other solutions, such as 'tripwires' to see if any data has changed, are also recommended.

Some of the developing countries are considering e-voting for a number of reasons which is discussed in this section. For instance, quite a number of resources are required for e-voting system. Among the required resources are functional computer network infrastructure and computer systems. Other important resources required to support and ensure that e-voting is successful should include knowledge of computer systems and Internet technology, with adequate and qualified manpower resources among others. Many developing countries do not yet have these resources in place and therefore, cannot properly tap into e-voting systems. For instance in Nigeria,the level of communication and Internet infrastructure has improved over the years but there is still literacy issue as well as lack

of qualified human resources. In some developing countries, the rural dwellers that still live below the poverty level neither know about computers nor know about how to operate them. Therefore, introducing e-voting systems in such environment will only amount to disenfranchising the people from exercising their civic rights of voting. The initial investment on e-voting is enormous and can impact negatively on the national budgets of these developing countries.

Estonia is one example of a developing nation that has successfully deployed and used e-voting. In Estonia, Internet access is considered a right for all citizens[4]. No wonder since 2000 the nation ventured into internet voting (I-Voting) and has been consistent along that line. Estonia is reputed to be the first to make of Internet voting in an election that covered the entire nation. A total of 9,317 electorates voted online representing about 1.85% voted in 2005. The number was 30,275 in 2007 during national parliamentary elections. I-voting is made easy in Estonia because all electorates use their national IDs that is chip-enabled to authenticate and vote.For online voting, the case is slightly different as voters have to acquire card readers and the necessary software. In summary, inadequate infrastructure and low literacy level coupled with limited national budgets may be reasons, why most developing countries are yet to adopt e-voting for their national elections.

4. Overview Of Network Forensics

Generally, computer crimes as well as Internet-related crimes otherwise known as cyber crimes are on the increase as a result of the phenomenal growth of the Internet and computer networks. The present tools available are able to detect and take counter measures whenever cyber attacks occur. For instance an IDS is able to detect attacks. Firewalls on the other hand, are able to filter what goes in and out of a network via a host. These tools and a host of others stop at just the stage of monitoring and protecting but do not link the crime or attack to the criminal or attacker. If the attacker or criminal is not found or punished,there is the likelihood of a repeat of that same attack by the same attacker, using a different approach or technique. Offender profiling is important to be applied in the case to avoid or minimize the likelihood of a repeat offence, hence a database forensic may be considered. If a crime is linked to the criminal and the criminal duly punished, it will serve as deterrent to other attackers planning similar attack, thereby reducing such crimes. This is where network forensics tools come to play. In order to attain an enhanced network security and cyber crime investigations, it becomes necessary to employ network forensics tools. Network forensics tools are capable of passively monitoring and capturing all network traffic. The aim of doing this is to use the necessary forensics tools to analyze the traffic with a view to tracking security violations as well as protecting the network against future attacks.In [13],highlighted the specific functions performed by a typical network

forensics analysis tool. A network forensics tool should be able to perform these three major tasks namely; capture network traffic; analyze the traffic according to the user's needs; and allow system users discover relevant facts from the analyzed traffic based on e-voting systems. Network forensics has been defined in a number of ways. The most generally accepted one is that network forensics is the science of detecting and recovering evidential information in a network environment that will be acceptable in a court of law. This is applicable to any malpractices of e-voting systems. In [14], defined network forensicsas the act of using proven scientific methods to acquire, gather, discover, study, correlate, analyze and document digital evidence from a number of different sources. In [15], included in his definition, analysis of network events with the aim of identifying the source of the attack. In network forensics, data captured via firewalls or intrusion detection systems or network devices like routers are analysed through network forensics. The main goal of network forensics is to link an attack to its source leading to the prosecution of the offenders. The activities of network forensics include monitoring the traffic of the network to detect anomalies and to confirm if the anomalies indicate an attack. The nature of the attack is determined once the anomaly is found to be an attack. Network forensics is an active research domain as the number of security incidents targeted at organizations and individuals is on the increase. There has also been noticeable increase in the degree of sophistication of the cyber attacks in recent time.The attackers usually take actions like changing system logs, installing a rootkit to avoid detection during and after the attack. This can make traceback and prosecution more difficult. Also, the Internet service providers have also been directed to keep constant record of traffic that passes over their network.

4.1 Classification of Network Forensics Tools

Network forensic has been classified in a number of way. There is classification based on how packets are capturednamely: Catch-it-as-you-can tools and stop-look-and-listen tools[16].

4.1.1 Catch-it-as-you-can Tools

These tools capture all the packets passing through a particular traffic and write them to storage. The packets are then analyzed in a batch mode afterward.Large amounts of storage are needed for this approach. Privacy issues may arise as a result of capturing all data including personal data. The law also forbids internet service providers from interfering or disclosing personal data of people without permission.

4.1.2 Stop-look-and-listen Tools

A fast processor is required in this approach in order to match the rate of incoming data. In this approach, each packet is analyzed in a rudimentary way in memory and only certain information is saved for future analysis. The two

approaches require great amount of storage so the old data is often deleted to create the required storage space for the new data. Some tools used for this purpose include "tcpdump" and "windump"which we shall discuss under this section.

There is also classification of network forensics tools based on the location of the tool. Two categories exist namely: host-based tools and network-wide tools[17]:

a) Host-based Forensics Tools

This category consists of network forensics tools that reside on a single host in a network and is responsible for monitoring, capturing and analyzing packets that arrive at that host. Such tools that provide lots of information in form of logs for user to analyze are in this category. Examples include Tcpdump, Pcap and Snort.

b) Network-wide Forensics Tools

These tools consist of a number of monitors that are installed at various points in the network for distributed network monitoring. The collection of data that is required to carry out network forensic is usually done from the host in the same domain. Niksun Net Detector is an example of network monitoring tools that combine data from the different monitors with a view to providing a comprehensive view of the network activity.

Table2 below gives a summary of the various tool used for capturing data/packets, analyzing and reporting in network forensics investigations.

Table 2: List of Network Forensics Tools Useful for E-voting System Forensics.

Name	Description	Use/Remark
E-Detective	A real-time Internet interception monitoring and forensics system that captures, decodes and reconstructs various types of Internet traffic	It is commonly used for organization Internet behavioral monitoring auditing, record keeping, forensics analysis, and investigation as well as, legal and lawful interception for lawful enforcement agencies.
NetDetector	NetDetector is a full-featured appliance for network security surveillance, signature anomaly detection, analytics and forensics.	It complements existing network security tools, such as firewalls, intrusion detection/prevetion systems and switches/routers, to help provide comprehensive defense of hosted intellectual property, mission-critical network services and infrastructure.

Netstat	Netstat includes information such as listening/active ports and their protocols. Established connections will also list the IP address (potentially an attacker's) that the machine is connected to.	Netstat is an extremely powerful tool that can be used to view the network connection info on a machine.
NetIntercept	It recognizes over 100 types of network protocols and file types, including web traffic, multimedia, email, and IM.	NetIntercept captures whole packets and reassembles up to 999,999 TCP connections at once, reconstructing files that were sent over your network and creating a database of its findings.
NetVCR	It is an integrated, single-point solution that decisively replaces multiple network performance monitoring and troubleshooting systems. NeetVCR's scalable architecture easily adapts to data centers, core networks, remote branches or central offices for LAN and WAN requirements.	NetVCR delivers comprehensive real-time network, service and application performance management.
Snort	Snort is a freeware network security tool which was initially developed for the UNIX platform and has now been ported to the Windows platform	The tool can capture traffic flowing into and out of a computer network or it can put the network adaptor in promiscuous mode and listen to all network traffic. It is a simple, command line tool used to show network traffic, detect network intrusion, perform protocol analysis, and ensure network troubleshooting.
Tcpdump	Tcpdump is a common packet sniffer for Unix-like operating systems (Linux, BSD, etc)	Tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression. It can also save the packet data to a file for later analysis.
Tcpflow	A program, that captures data transmitted as part of TCP connections (flows), and stores data in a way that is convenient for protocol analysis and	Each TCP flow is stored in its own file. Thus, the typical TCP flow will be stored in two files, one for each direction. Tcpflow can also process stored

	debugging.	'tcpdump' packet flows
WHOIS	WHOIS is a query and response protocol that is widely used for querying databases that store the resgistered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information.	The protocol stores and delivers database content in human-readable format.
Wireshark	A free and open source packet analyzer. Originally named Ethereal.	It is used for network troubleshooting analysis, software and communications protocol development and education
Pcap	Pcap was initially developed for network interfaces of a system running UNIX OS	Pcap is a packet capture tool used to collect traffic going through a network interface.
WinPcap	This includes a network statistics engine and provides support for packet filtering.	WinPcap is a packet sniffing tool used to capture the packets flowing in and out of a network interface of a system running the Windows OS.
AirPcap	This may capture the control frames (ACK, RTS, CTS) management frames (Beacon, Probe Requests and Responses, Authentication) and data frames.	AirPcap is an extension of WinPcap tool used to collect packets going through a 802.11 Wireless LAN interface of Windows system.

5. Conclusion

The internet and computer networks remain the future of information and communications technology. Almost everything we do is now being done on the Internet or it may require that we connect to other hosts somewhere. This phenomenal increase in Internet and network-based activities has attracted cyber criminals who consistently improve their strategies and modes of attack to keep network and security professionals constantly on their toes, finding ways to protect or mitigate these attacks. In this paper therefore, electronic voting system is discussed and evaluated based on the applicability of network forensic as applied to e-voting application. It is certain that e-voting application relies much more on networks as well as the Internet (i-voting). With this in mind, we have outlined the threats and risks that the e-voting application faces as more developing countries buy into this idea. Introduction of network forensics was considered together with its tools as one of the major way of reducing the attacks that network-based applications

suffer. Network forensics is capable of tracing the behavior of network abuse and also for discovering potential risks through the analysis of collected network data. We are therefore, of the opinion that the more network- related crimes are traceable to their perpetrators with evidences which may leads to their prosecution, then the likelihood of reduction in the number of attacks that could be experienced.

References

1. Malkawi M., Khasawneh M. and Al-Jarrah O., (2009), "Modeling and Simulation of a Robust E-voting System", Communications of the IBIMA, Volume 8, 2009. ISSN: 1943-7765.
2. Okediran O. O., Omidiora E. O., Olabiyisi S. O., Ganiyu R. A. and Alo O. O., (2011), " A Framework for a Multifaceted Electronic Voting System". International Journal of Applied Science, Philadelphia, USA, vol. 1 No .4 pp 135-142.
3. Okediran O. O., Omidiora E. O., Olabiyisi S. O., and Ganiyu R. A. (2011), " A Survey of Remote Internet Voting Vulnerabilities", WCSIT, ISSN: 2221-0741, Vol 1, No. 7 pp 297-301.
4. Peter H. (2014), "Online Voting: Rewards and Risks", Atlantic Council of United States.
5. Drew S. et al (2014), "Security Analysis of the Estonian Internet Voting System", University of Michigan. http://jhaldem.com/pub/papers/ivoting.ccs14.pdf
6. Matt B., Sean P., Candice H., Mark G. and David J. (2010), "E-Voting and Forensics: Prying Open the Black Box"
7. Abdallah A. and Samani T. (2013) "The Technical Feasibility and Security of E-voting", International Arab Journal of Information Technology, Vol 10, No.4.
8. Matej T. (2014), "Electronic Voting: To Have or Not To Have", European Scientific Journal Vol3. ISSN:1857-7881 pp 224-230.
9. Gibson S. (2011) "Distributed Denial of Service Attack", available at http://www.grc.com/dos/drdos.htm last accessed 2011.
10. Ragupathy R and Rajendra S. (2014), "Detecting Denial of Service Attacks by Analyzing Network Traffic in Wireless Networks' International Journal of Grid Distribution Computation, Vol 7, No.3 ISSN:2005-4262
11. Tavish V. (2015), "2001-2013: Survey and Analysis of Major Cyber Attacks. Arxiv.org/pdf/1507.06673.pdf
12. Steven M.B. (2013), "Viruses and Trojan Horses". https://www.cs.columbia.edu/~smb/clases/fib/i-virus.pdf

13. Varun C, arindam B., Vipn K. (2009), "Anomaly Detection: A Survey". cucis.ece.northwestern.edu/projects/dms/publications/Anomaly detection.pdf
14. Bhavesh P., Sanjay M.S., and Sameer S.C. (2010), "Comparative Analysis of Network Forensic Systems". research.ijcaonline.org/ipmc/number1/ipmc018.pdf
15. Atu K.K., Emmanuel S. P., and Joshi R.C. (2010), "Network Forensic Analysis by Correlation of Attacks with Network Attributes. International Conference, ICT 2010, Kochi, India pp124-128
16. Amor L. (2013), "A Survey of Network Forensic Tools", International Journal of Computer and Information Technology, ISSN:2279-0764, Vol2, No 1.
17. Karthikeyan K.R. and Indra A. (2010), "Intrusion Detection Tools and Techniques", International Journal of Computer Theory and Engineering Vol 2, No 6