Proactively Defending Computing Infrastructures through the Implementation of Live Forensics and Capture in Corporate Network Security

Tameem Chowdhury, Dr. Stilianos Vidalis, Dr. Christopher Tubb

The University of South Wales and The University of Stafford

Abstract. The wide development of the mobile and virtualised technologies in the past decade has further destabilised the already fragile balance between the defenders and the attackers of computing infrastructures. Coupled with the fact that risk is not controlled by the defenders but by the attackers, it makes no sense to try and re-actively defend computing infrastructures. Apropos, in this new socially driven knowledge-based computing era that corporations are asked to operate in, there is a need to pro-actively defend computing infrastructures by attempting to control the source of the threats that they face. In this paper we discuss forensic readiness issues of such a system and we examine how we could ensure and assure evidential integrity and chain of custody of the near real time intelligence that the system would be collecting.

Keywords: Network Security, Forensics, Live Capture, Information Environment.

1 Introduction

Corporations continuously develop and use new business models for maintaining a competitive advantage over their competitors which are forcing them to accept more risks for less. They have to operate in a hostile Information Environment and maintain an information superiority state at a global scale. Alas, the resources that are available to any corporation are finite. There is indeed a need to control decision makers, be it human beings or machines, in order to steer their operations away from the assets that we are tasked with defending. There is a need for active defence systems to become mainstream.

The paper discusses the information environment, the importance of forensically focused system security and how to implement forensic readiness in protecting corporations most commodity; its assets.

2 Information Environment

Information encapsulates a wide range of concepts and phenomena. They relate to both the processes and material states, which are closely interrelated [1]. Information can be:

- "A product, which encompasses information as an object, as resource, as commodity
- What is carried in a channel, including the medium channel itself

– The Contents."[2]

Vidalis[3] adds: "Information assets are physical, hardware, software, data, communications, administrative and personnel resources of a computing system." An asset is a single item of ownership having exchange value. Assets can be tangible or intangible; they are what all businesses rely upon for revenue and growth. The secure protection of a businesses specific assets are crucial to their survival within the business world and therefore procedures need to be in place in order to protect and preserve asset value. Akin to reality, the virtual space is the new realm of information warfare and dissemination of misinformation and this wholly can be defined as the information environment. Clausewitz and Tzu [4][5] theorised about warfare and military mentality and strategy in their respective works, and although the context for use are in different planes, the theory can still be applied to virtual information warfare.

The United States Department of Defense (DoD) has defined the Information Environment (IE) as follows: "The information environment is the aggregate of individuals, organisations and systems (resources) that collect, process, disseminate, or act on information."[6]

Vidalis and Angelopoulou [6] concur "that the IE is indeed the interaction between people with the systems in place which collect, analyse, apply, or disseminate information. Without the mechanisms to provide information in a format that can be interpreted, decision makers are unable to act and provide an analytical response to a particular problem or situation." Alberts et al [7] "takes the aforementioned IE notion further by identifying that the IE can be broken down into three distinct domains: the Physical Domain; the Information Domain; and the Cognitive Domain. The three domains correspond with the conclusions drawn from the DoDs conception of what the IE entails." The physical domain relates to the transmission, infrastructure, technologies, groups and populations of information. The Information domain denotes the location and where it precedes and the cognitive domain exists within the minds of the decision makers. It can be very difficult to define the elements which exist within this domain, because each individual mind has a different perception and is thus unique.[6]

3 System Security

The system security of corporations, now more than ever, requires the design and most importantly the implementation of a forensically [8][9][10][11] prepared network [12][13]. A corporation's entire network needs to be implemented in a manner that accounts for combatting and defending worst case scenario cyber attacks [8]. Cyber crime [8][14][15] is affluent and exponentially growing with the constant and continuous saturation of technological advances and widespread consumer availability; the growth of criminal organisations utilising the internet and world wide web for conducting their illegal activities is unfortunately and inevitably in tandem. Therefore forensic [8][9][10][11] readiness will ensure that when, and not if, an attack is orchestrated, it can be effectively defended and combatted and evidence of any cyber crime

can be collected and preserved [8][9][10][11], ensuring the integrity of the evidence [16], which can be presented to the authorities; thus enabling the appropriate action to be levelled towards the perpetrators. Most importantly, a corporation's assets [3] will be protected, their business disturbacnde minimised and the reputation preserved and intact. The design of a wholly secure network employed by corporation's would require the segregation and inaccessibility of a corporations assets [3] from outside the network's physical infrastructure; the advantages of employing this method will undoubtedly increase security and availibility to the highest level, and most importantly protect assets. However if an employee is not within the corporation's physical domain and network infrastructure, access to corporation resources are limited to the web and mail servers. Therefore a combination of secure authentication and forensic [8][9][10][11] monitoring of the network needs to be implemented. A standard design that can be implemented for a secure network [17][18] is illustrated in figure 1.

The two router combination provides extra security, as the router positioned outside the network (segment 1) carries out initial packet filtering. The internal network is protected by another router positioned on the interior of the network and another firewall (between sement 1 and 2). The De-Militarised Zone (DMZ) provides further security to the internal network, where there is more than one firewall in use to create a secure network. The DMZ contains the web and mail servers, so that access remotely via the Secure SHell (SSH) server is limited to the DMZ and no access to the internal network, thus protecting a corporations valuable assets. The internal network is further protected by a bastion host and firewall to restrict access to the file servers, as well as monitor traffic and usage [17][18]. This is ideally where forensic monitoring of the network should be administered.

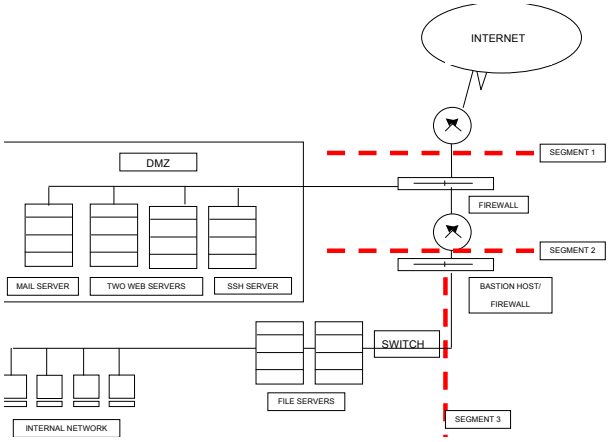

Fig. 1. Secure Network Design

4 Forensic Readiness

Forensic [8][14][15] monitoring of the network [17][18][12][13], focusing on connections from outside the network should be conducted by utilising a methodology that will enable any evidence to be accepted in a court of law. Server security, administration and setup can account for internal discrepancies, but capturing and preserving data regarding outside infringements, needs to be carefully and precisely conducted, so that it can directly be used by law enforcement agencies in immediate investigations. The implementation of live forensic procedure

will accelerate the investigative process, as well enable the collection and preservation of much more data than would be available in simply conducting computer forensic investigations, once a system is infiltrated and after cyber-crimes [8][14][15] has be commited. Furthermore the ramifications of an attack may not only compromise the security of a corporations assets, but may even damage the corporations network beyond immediate repair. Implementing the ACPO guidelines [16] within the monitoring of the network as well as the following procedure, will ensure that evidence collected cannot be dismissed by litigation and scrutiny. Utilising the following software tools can enable the collection of live forensic data, which in the event of an attempted cyber attack, can be preserved and presented against the perpetrators in a court of law.

Collecting evidence [8][9][10][11] using live capture requires the utilisation and combination of a number of software resources; network enumeration tools and methods [18]; software to monitor the memory and process usage and a network packet analyser to view all the associated network traffic [12][13] with its specific virtual behaviour. These procedures need to be conducted in a forensically sound manner [8] to ensure the admissibility and reliability of the evidence gathered [16][9][10][11]. Evidence must be handled and preserved in a forensically sound manner, whilst maintaining the appropriate chain of custody for the evidence. All software tools that will be utilised during live capture procedures need to be prior tested, documented and above all licensed [19]. If the administrator or investigator is using tools that have not been tested or the correct license has not been obtained, the validity and integrity of the evidence and investigatory procedures will be open for scrutiny by opposing council.[20]

The following steps ensure that the collection of data during forensic monitoring can be admissible in a computer forensic investigation and if there is evidence of an attempted attack, the collected data can be preserved and presented as evidence.[20]

Live Capture Procedure:

- A log of all actions should be contemporaneously maintained [16]
- Ensure tools are legal and licensed. Conduct prior testing and document the results
- Host client needs to possess high processing speeds and access to redundant Internet connectivity
- Installation of the required software for live capture
- Conduct network enumeration through software tools
- Create a duplicate of all data. The original data collated needs to be unaltered[20].

The procedure ensures that as much evidence as possible is gathered when conducting the live capture, so that there is an exact record of all actions taken, firstly to gather the information and data in question and secondly how this procedure was carried out, enabling dual verification if necessary [8][9][10][11]. Furthermore, valuable evidence may be recovered and the validity of any evidence can be strengthened, whilst ensuring that evidence-handling techniques have been observed and implemented.

Network enumeration tools enable an investigator to gather intelligence, a process commonly referred to as foot printing[18]. Exhibits that can be collated during intelligence gathering, through the implementation of network enumeration tools can include:

- The processes that execute when the webpage or website is loaded
- The process names and start-up times
- The status of the processes
- Which user executed which process
- The amount of system resources used by specific processes over time
- System and user processes and services executing at any given time
- The method by which each process is normally started and what authorisation and privileges have been assigned to those processes
- Hardware devices used by specific process
- Files currently opened by specific processes
- Media Access Control (MAC) address of the source transmission, which can identify the manufacturer and its unique part identification
- The protocols utilised in the data transmission
- The ports utilised by the source transmission for incoming and outgoing traffic and
- The operating system and their current version implemented by the source transmission. [20]

There are numerous tools available that can conduct network enumeration [18] across the application of different platforms, which enables administrators or investigators to verify and validate the tools that they choose to utilise in an investigative monitoring phase.[20]

Windows Platform	UNIX Platform
NetScan Tools	TCP Dump, TCP Trace
NetDetector Alpine	Wireshark
NetIntercept	Snort
NetWitness	NMAP
Process Monitor	EtherApe
Portmon	
WinDump	

Fig. 2. Network Enumeration Tools [20]

The classification of these tools to a particular operating system platform is not definitive; WinDump is the Windows equivalent of the TCP Dump tool available through UNIX platforms and the NMAP and EtherApe tools are only available on UNIX based operating systems. The other tools can be applied under either operating system environments, but can be most effectively utilised under the specified platforms.

	Processes Executed	***Process Name***	***Process Start Time***	***Process Status***	***User Process***
Net Scan Tools	No	No	No	No	Yes
Net Detector Alpine	No	No	No	No	Yes
Net Intercept	No	No	No	No	Yes
Net Witness	No	No	No	No	Yes
Process Monitor	Yes	Yes	Yes	Yes	No
Portmon	No	No	No	No	No
Win Dump	No	No	No	No	No

Fig. 3. Process Analysis for Windows Platform [20]

The open source tools described as well as the tools that provide a trial version have

been tested, in order to assess their capabilities. A number of the tools applicable under the Windows platform, that do not provide a trial version, have not been tested, so their specified capabilities cannot be validated. They have been classified according to the tool desciptions provided by their respected vendors and websites[20]. The network enumeration tools that can be utilised to monitor the processes and their specific usage under a Windows environment are compared in figure 3. The following figure illustrates which tools are applicable when gathering system information on a particular target utilising a Windows platform.

	System Resource Utilised by User	*System and Processes Utilised*	*Hardware Devices Used by Process*	*Files opened by Process*
Net Scan Tools	Yes	Yes	No	Yes
Net Detector Alpine	Yes	Yes	No	Yes
Net Intercept	Yes	Yes	No	Yes
Net Witness	Yes	Yes	No	Yes
Process Monitor	Yes	Yes	Yes	Yes
Portmon	No	No	No	No
Win Dump	No	No	No	No

Fig. 4. System Analysis for Windows Platform [20]

Figure 5 illustrates which tools are applicable when gathering network data on a particular target whilst utilising a Windows Platform. The network enumeration tools that can be utilised to conduct process usage and analysis under a UNIX environment are compared in figure 6.

Figure 7 illustrates which tools are applicable when gathering system information on a particular target whilst utilising a UNIX platform.

	MAC Addr	*Protocols Used in Data Tranmission*	*Ports for incoming /outgoing traffic*	*Operating System and Current Version*	*IP Addr*
Net Scan Tools	Yes	Yes	Yes	Yes	Yes
Net Detector Alpine	No	Yes	Yes	Yes	Yes
Net Intercept	Yes	Yes	Yes	Yes	Yes
Net Witness	Yes	Yes	Yes	Yes	Yes
Process Monitor	No	No	No	No	No
Portmon	No	Yes	Yes	No	No
Win Dump	Yes	Yes	Yes	No	Yes

Fig. 5. Network Analysis for Windows Platform [20]

	User Executing Process	*Process Status*	*Process Start Time*	*Process Name*	*Processes Executed*
EtherApe	No	No	No	No	No
NMAP	No	Yes	Yes	Yes	Yes
Snort	No	No	No	No	No
Wireshark	No	No	No	No	No
TCPDump	No	No	No	No	No

Fig. 6. Process Analysis for UNIX Platform [20]

	System Resource Utilised By User	*System and User Processes Utilised*	*Hardware Devices Used By Process*	*Files Opened By Process*
TCPDump	No	No	No	No
Wireshark	Yes	Yes	Yes	No
Snort	Yes	Yes	Yes	No
NMAP	Yes	Yes	Yes	No
EtherApe	No	No	No	No

Fig. 7. System Analysis for UNIX Platform [20]

Finally figure 8 illustrates the tools that can be implemented in gathering network data on the intended target utilising a UNIX platform.

	IP Addr	***Op Sys and Ver.***	***Ports In; Out going Traffic***	***Protocols in Data Trans-mission***	***MAC Addr***
EtherApe	Yes	No	Yes	Yes	No
NMAP	Yes	Yes	Yes	No	Yes
Snort	Yes	Yes	Yes	Yes	Yes
Wireshark	Yes	No	Yes	Yes	Yes
TCPDump	Yes	No	Yes	Yes	No

Fig. 8. Network Analysis for UNIX Platform [20]

In line with computer forensic procedures, the tools described require administrators or investigators to practise and learn their functionality for efficient and accurate evidence collection. The network protocol analysers provide a wealth of data through utilisation during online activity, though they are complex to familiarise with and require the investigator to have appropriate knowledge regarding network fundamentals and their technology [20].

5 Conclusions

To be added later today.....

References

1. L. Floridi. Semantic conceptions of information. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Spring 2011 edition, 2011.
2. M J Menou. The impact of information ii: Concepts of information and its value. *Information Processing & Management*, 31(4):479–490, 1995. (Cited in Vidalis, S. and Angelopoulou, O. 2013. *Deception and Manoeuvre Warfare Utilising Cloud Resources*. Under review).
3. S Vidalis. E-crime. University of Wales, Newport, February 2009.
4. Carl Von Clausewitz. *On War*. Princeton: Princeton University Press., 1976.
5. Sun Tzu. *The Art of War by Sun Tzu Special Edition (Translated and annotated by Lionel Giles)*. El Paso Norte Press, 1910.
6. S Vidalis and Angelopoulou. Deception and manoeuvre warfare utilising cloud resources. *Under Review*, 2013.
7. D Alberts, R.E Garstka, Hayes, and Signori D.A. *Understanding Information Age Warfare*. Washington DC: CCRP Publications, 2001. (Cited in Vidalis, S. and Angelopoulou, O. 2013. *Deception and Manoeuvre Warfare Utilising Cloud Resources*. Under review).
8. E Casey. *Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet*. 2nd ed. London: Academic Press, 2004.
9. R. Anzaldua, J. Godwin, and L Volonino. *Computer Forensics: Principles and Practises*. New Jersey: Pearson Prentice Hall, 2007.
10. F Adelstein. Live forensics: diagnosing your system without killing it first. *Communications of the ACM*, 49(2):63–66, 2006.
11. H Berghel. The discipline of internet forensics. *Communications of the ACM*, 46(8):15, 2003.
12. M. Greggs and D Kim. *Inside Network Security Assessment: Guarding Your IT Infrastructure*. Indiana: Sams Publishing, 2006.
13. W Stallings. *Operating Systems*. United States of America; Prentice Hall, Inc, 2001.
14. B Carrier. *A Hypothesis-Based Approach to Digital Forensic Investigations*. PhD thesis, Purdue University, Indiana, 2006.
15. B. Carrier. *File System Analysis*. New Jersey: Pearson Education, Inc, 2005.
16. Association Of Chief Police Officers. The principles of computer-based electronic evidence. good practice guide for computer-based electronic evidence. *Association Of Chief Police Officers.*, 2008.
17. F Derfler. *How Networks Work*. Indianapolis, Macmillan Computer Publishing/Que Corporation, 1998.
18. S. McClure, J. Scambray, and G. Kurtz. *Hacking Exposed Network Security Secrets & Solutions*. 3rd ed. Berkeley: Osborne/ McGraw-Hill, 2001.

19. J Mitchell. Computer forensics (finding and preserving the hidden evidence). Technical report, Hertfordshire: LHS Business Control., 2004.
20. T. Chowdhury and S. Vidalis. Collecting evidence from large-scale heterogeneous virtual computing infrastructures using website capture. In *4th IEEE International Conference on Intelligent Networking and Collaborative Systems and EIDWT 2012 3rd International Conference on Emerging Intelligent Data and Web Technologies*, 2012.