Countering Cyber Trespass; A proposed Framework

Danquah, P. (PhD)
LUCAS University College, Accra, Ghana
E-mail: danquahpaul@gmail.com

Adedara. O
Department of Computer Science
The Federal Polytechnic, Ado-Ekiti, Nigeria
fafvfk@yahoo.com

*** Longe, O.B & **Ogunjimi, O.A.**
*Heidelberg Laureate Forum Fellow, Heidelberg University, Heidelberg, Germany
**Dept of Computer Science, Caleb University, Lagos, Nigeria
longeolumide@fulbrightmail.org, olaogunjimi@gmail.com

ABSTRACT

This study sets out to develop a framework to guide the development of technical tools or solutions to counter cyber trespass. The approach involves a combination of both inductive and deductive activities by collecting data and using relevant theories respectively. The findings are used to develop the framework as the output of the process. The framework leverages on a combination of scanning detection algorithms, permission, vulnerability database and a trespass detection system to counter any form of cyber trespass on an operating system, an application or a network. A mapping is provided to link these components to the crime displacement theory which focuses on displacing crime from one locale to the other.

Keywords: Cybercrime; cyber trespass; Countering Cyber Trespass

Aims Research Journal Reference Format:
Danquah, P., Adedara, O. & Longe, O.B (2017): Countering Cyber Trespass; A Proposed Framework
Advances in Multidisciplinary & Scientific Research Journal. Vol. 3. No.3, Pp41-50

1. INTRODUCTION

Cyber crime is defined by (Brennar and Clarke, 2004) as a subset of crime: it refers to crimes committed by use of computer technology, either alone or in conjunction with real-world acts. Picker, (2004) also defines cyber crime as just crime over the Internet. However, Katyal, (2001) defines Cyber crime in a much broader sense as an umbrella term that covers all sorts of crimes committed with computers from viruses, Trojan horses, from hacking into private email to undermining defense and intelligence systems, from electronic thefts of bank accounts to disrupting web sites. Katyal, (2001)'s definition is operationalized in this study.

Categories of Cybercrime

Yar (2005) categorizes the types of cyber crime as namely;

- ❖ Cyber-Trespass: This type of cyber crime involves crossing boundaries into other people's property and/or causing damage. Typically all users are authenticated and authorized with access rights and privileges to resources on systems/network, the users would also have boundaries to which they may be confined. A user's access to resources beyond the defined boundaries is referred to as cyber trespass. Examples of cyber trespass are hacking, defacement and viruses.
- ❖ Cyber-Deceptions and Theft: This type of cyber crime involves the use of technology to cause deception and steal. Usually the theft may involve money or property such as credit card fraud, intellectual property violation and piracy.
- ❖ Cyber-Pornography: These are activities that breach laws on obscenity and decency, this law does vary from one jurisdiction to the other however, there some aspects of the law that cut across all jurisdictions. A typical examples is child pornography. Cyber Violence: This involves the use of the internet and related technologies to cause psychological harm or incite physical harm against others, thereby breaching laws pertaining to the protection of the person. Examples of cyber violence are hate speech, cyber bullying and denial of service attack. (Yar, 2005)

1,1. Objective of this study

The primary objective of this paper is to develop a framework to guide the development of technical tools/solutions to counter cyber trespass.(Ngo & Jaishankar,2017) The protection of citizen privacy in the investigation and prosecution of cyber crime is perhaps one of the most controversial and hotly debated topics in recent years, this is due the high tendency of compromising users' privacy in trying to counter cyber trespass. This study however attempts to address this issue proposed solution.

2. METHODS

2.1 Theoretical Framework Underlying Proposed Frameworks

There are three key reasoning alternatives in research, these are deductive reasoning, inductive reasoning and abductive reasoning. The deductive reasoning is working from the more general to the more specific. It starts with premises contained in the theories or models and then draws conclusions. In information systems research, deductive reasoning is most common with the application of theories to specific phenomena and human behaviors resulting in extensions to the existing models or theories. Hence, deductive approach requires a considerable deal of theoretical work before data are collected (Blaike, 2009). Theories applied can be from either a single source or multiple sources where relevant constructs from different models are combined to generate a framework to be tested. In contrast, inductive reasoning starts with the collection of data, and, ends with descriptions of patterns in the data (Blaikie, 2009). Often, inductive reasoning is based on observation of signs. For example, weather forecast. Experiences (knowledge) lead to observations which produce certain patterns that are developed into relevant theories or models. Logical experiences create perceptions that give new perspectives on the phenomenon. These perspectives are then captured into new models, frameworks or theories by extending the existing theories or generating new models or frameworks. The primary objective throughout the study was the testing of theory and development of frameworks through the deductive-inductive iteration.

The theoretical framework underlying the development of the proposed frameworks adopt the inductive and deductive approach. The inductive aspect constitutes the use of research findings related to the behavioural patterns of cyber criminals as per findings of research objectives. The deductive aspect constitutes the use of the principles of the Crime Displacement Theory to explain how cyber crime can be prevented. The findings outlined the behavioural pattern of cyber criminals by providing the steps involved in cyber crime commission and the principles of the crime displacement theory for displacing crime from one locale to the other are merged to determine the essential themes to counter the respective categories of cyber crime. The above formed the basis for the components of the two proposed frameworks. The approach is diagrammatically represented below in Figure 1.

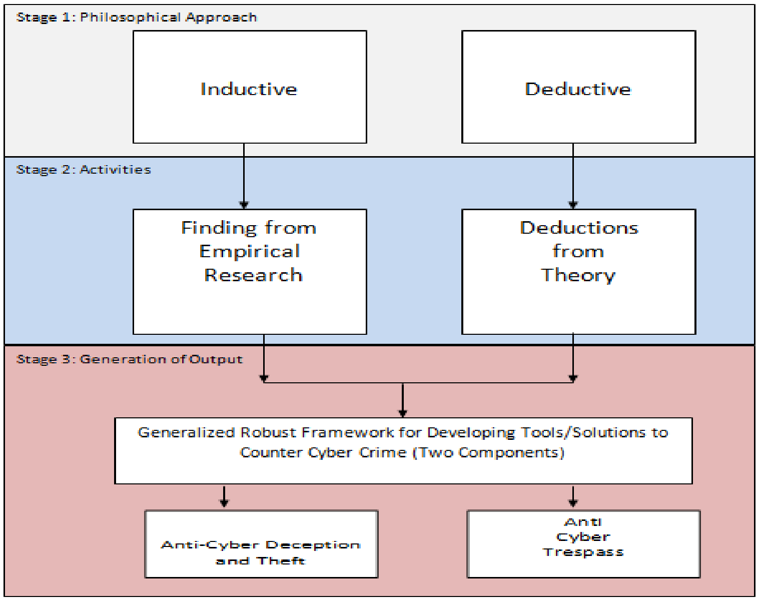

Stage 1: Philosophical Approach
Inductive
Deductive
Stage 2: Activities
Finding from Empirical Research
Deductions from Theory
Stage 3: Generation of Output
Generalized Robust Framework for Developing Tools/Solutions to Counter Cyber Crime (Two Components)
Anti-Cyber Deception and Theft
Anti Cyber Trespass

Figure 1: three stages of the theoretical framework for developing the frameworks to be used

Figure 1 shows the three stages of the theoretical framework for developing the frameworks to be used as a guide for developing tools or solutions to counter cyber crime. The first stage as shown in the diagram involves the philosophical approach, this is a combination of both inductive and deductive approach, the second stage involves the precise activities involved in implementing the philosophical approaches, thus, collecting data and using existing theory as inductive and deductive approaches respectively. The third stage involves the usage of findings from stage two to develop the framework as the output of the process.

2.1 Basis for the Development of the Framework

As indicted in the objective of this study, after a considerable literature review, deductive reasoning applies to the phenomenon of interest to verify specific frameworks to counter cyber crime developed from the Crime Displacement Theory and deduced behavioural patterns. The objective of is to verify the generalizability of the constructs that exist in the literature and deduced behavioural patterns.

3.2 Theories and Concepts

This section assesses relevant theories and concepts to cyber crime as a field of study.

Routine Activity Theory (Crime Theory):

The Routine Activity Theory is a criminological theory that was propounded by Cohen and Felson(1979), the theory pre supposes that for a crime to be committed, the following must be concurrently present;

(a) A suitable target is available: The suitable target here refers to a person, object or place.
(b) There is lack of a suitable guardian to prevent the crime from occurring: The capable or suitable guardian refers to a deterrent like police patrols, security guards, neighborhood watch, door staff, vigilant staff and coworkers, friends, neighbors and CCTV systems.
(c) A motivated offender is present: This presupposes that there can be no victim without the intentional actions of another individual.

This theory definitely applies to cyber crime regardless of the category. It must be emphasized that a crime must occur when there is the opportunity for the crime to be committed. Opportunity is the cause of crime and indeed root cause of crime. For cyber crime to be successfully committed, the opportunity for crime is multiplied by the simple fact that the criminal is no longer "place-bound". The routine activity theory was confirmed by Bossler and Holt(2009) publication On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory.

Crime Displacement:

Cox, Johnson & Richards (2009) The primary focus of crime reduction is opportunity reduction. The logical question is whether or not such efforts simply displace or move the crime to another locale.

Crime Displacement may involve the following;

❖ Geographical: Moving Crime from one location to the other
❖ Temporal: Moving Crime from one time to the other
❖ Target: Moving Crime from one target to the other
❖ Tactical: Changing the approach to committing the crime from one to the other
❖ Crime type: Changing the type of crime that is to be committed. (Felson and Clarke 1998)

The use of Crime Displacement as a method of reducing crime may have varying outcomes, these are;

(a) Positive: A crime is displaced to a less serious damage. It represents a success since it produces a net gain.
(b) Negative: A crime is displaced to a more serious crime with greater reward or greater social cost.
(c)Neutral: A crime is displaced to one of the same seriousness, of the same risk, rewards and damage.
(d) Even-Handed: Prevention is concentrated on those who are repeatedly victimized in order to achieve a more equitable distribution of crime.
(e) Attractive: Activities and /or places attract crime from other areas or activities (eg-red light districts attract customers from other areas, as well as other criminal activities)

Space Transition Theory:
Jaishankar (2008) explains; The Space transition theory argues that, people behave differently when they move from one space to another. The postulates of the theory are as follows:

1. Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.
2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime
3. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.
4. Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.
5. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space.
6. Associates of physical space are likely to unite to commit crime in cyberspace.
7. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.
8. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cyber crimes. (Jaishankar, 2008)

This theory was postulated like any other criminological theory which came during the medieval era, it is yet to be tested empirically to determine its authenticity. The Space Transition Theory if proven accurate or otherwise could serve as a premise for Cyber Forensic Investigations and even better to model anti cyber crime solutions. Brenner(2004a) has provided another two important differences between the cyberspace and the real space, that is the absence of physical constraints and lack of hierachical constraints. Danquah and Longe(2011)'s empirical test of the Space Transition Theory was instructive by indicating that researchers particularly could leverage on the causal relationships to build a model or unifying framework to neutralize cybercriminal activities.

2.3 The Cyber Trespass Context

This study emphasizes on cyber trespass which involves crossing boundaries into other people's property and/or causing damage with unauthorized access rights and privileges to resources on systems/network. Users usurp boundaries to which they may be confined in cyber trespass. Sung(2017) explain that greater computer use and perceived stress were related to more cyber delinquency in recent years. Given the different categorizations of cyber crime, it is evident that there is some significant amount of mutual exclusivity in the occurrence of the different categories. For instance, socially engineered cyber deception and theft requires that the perpetrator gains the trust of the victim where as cyber trespass does not require any form of trust between the victim and perpetrator. Cyber trespass is strictly based on unauthorized access whereas cyber deception and theft is not.

2.4 Research Instrument

Interview questions were designed and validated by experts in the cyber crime field of study. The analysis of data collected is done qualitatively via an attempt to compare the findings from the primary data with the meanings derived from the secondary text for the purpose of using it to optimize the conceptualization of cybercrime.

3. RESULTS

3.2 The Case of Universities

Data was collected from four Universities within Ghana, two had had their websites compromised whereas the other two had their Students Information System compromised with grade manipulation. The respondents were from the Information Technology departments. Interview revealed the compromised websites on a couple of occasions and also remote access to sensitive data on the campus network. It was evident that vulnerabilities in the campus networks and also website hosting service had been exploited from the responses provided. All these Universities indicated that they felt extremely violated and embarrassed given the amount of effort that had gone into trying to remedy the situation and preventing future occurrence. The Universities prefer to have their names withheld.

3.2 The Case of Banks:

Interview with 3 Banks (Name Withheld): It was evident from the banks' response to questions that they had bank accounts compromised as well as their network and banking application. The respondents were from the Information Technology and Operations departments of the banks. The responses tend to portray some level of social engineering involved which eventually lead to an evident example of cyber trespass. One specific case involved the installation of key loggers on a customers' computers to determine the customer's key sequence for logging in, subsequently this was extended this to some key staff of the bank and then eventually to systems on the banks network. The culprits on numerous occasions successfully withdrew money and also transferred money between numerous accounts thus causing financial loss to individuals and the bank as a whole.

3.3 The Case of Telecommunication Companies :

An interview of three telecommunication companies in Ghana to determine the type of cyber crime they may have possibly experienced. With much reluctance from the telecommunication service providers some data was obtained. The respondents were predominantly from the Revenue Assurance, Information Technology, Call Centers and Technical departments. Much as access to live and historic data would have been most ideal, this was not permitted by the telecommunications companies hence one had to resort to only interviews.

3.4 Salient Findings

There was some consistency in their responses, they all experience SIMBOX fraud on their networks. The pattern of occurrence is the same as explained below.

The Subscriber Identity Module (SIM)Box is a device that maps a call from Voice over Inter Protocol(VoIP) to a SIM card (in the SIMBOX) of the designated mobile operator. Therefore international calls terminating as home call to subscriber country are usually cheap compared to the cost of terminating the international call. This is to just bypass international tariffs. The perpetrators use a device called a SIMBOX which makes calls by means of VoIP then are mapped onto simcards in the SIMBOX. These simcards are mostly network SIMs of the designated home base mobile network and thus all calls made through these the local call tariffs. These simboxes can be located either at the source of the call or the recipient side, all with the sole and prime objective of re-routing calls via this device to attract lower call tariffs at the expense of the telecommunication network providers. This is a major point of revenue loss to most telecommunication networks and dealing with it has been very discreet matter. Aside that they also have a major impact on the networks, causing call drops, missing CLI (calling line identity), bad quality of service etc.

It turned out that most telecommunication companies have outsourced this service to outside companies, this implied the respondents who are primarily from various departments including Revenue Assurance, Information Technology, Call Centers and Technical may have provided their opinion based on their respective experiences in dealing with the phenomena. Numerous possible parameters and metrics were mentioned as possible criteria for detecting SIMbox fraud, the exact thresholds for the respective service providers' parameters are subject to service provider's discretion. These thresholds have been represented with "x" in the listed parameters. The noteworthy ones are listed below;

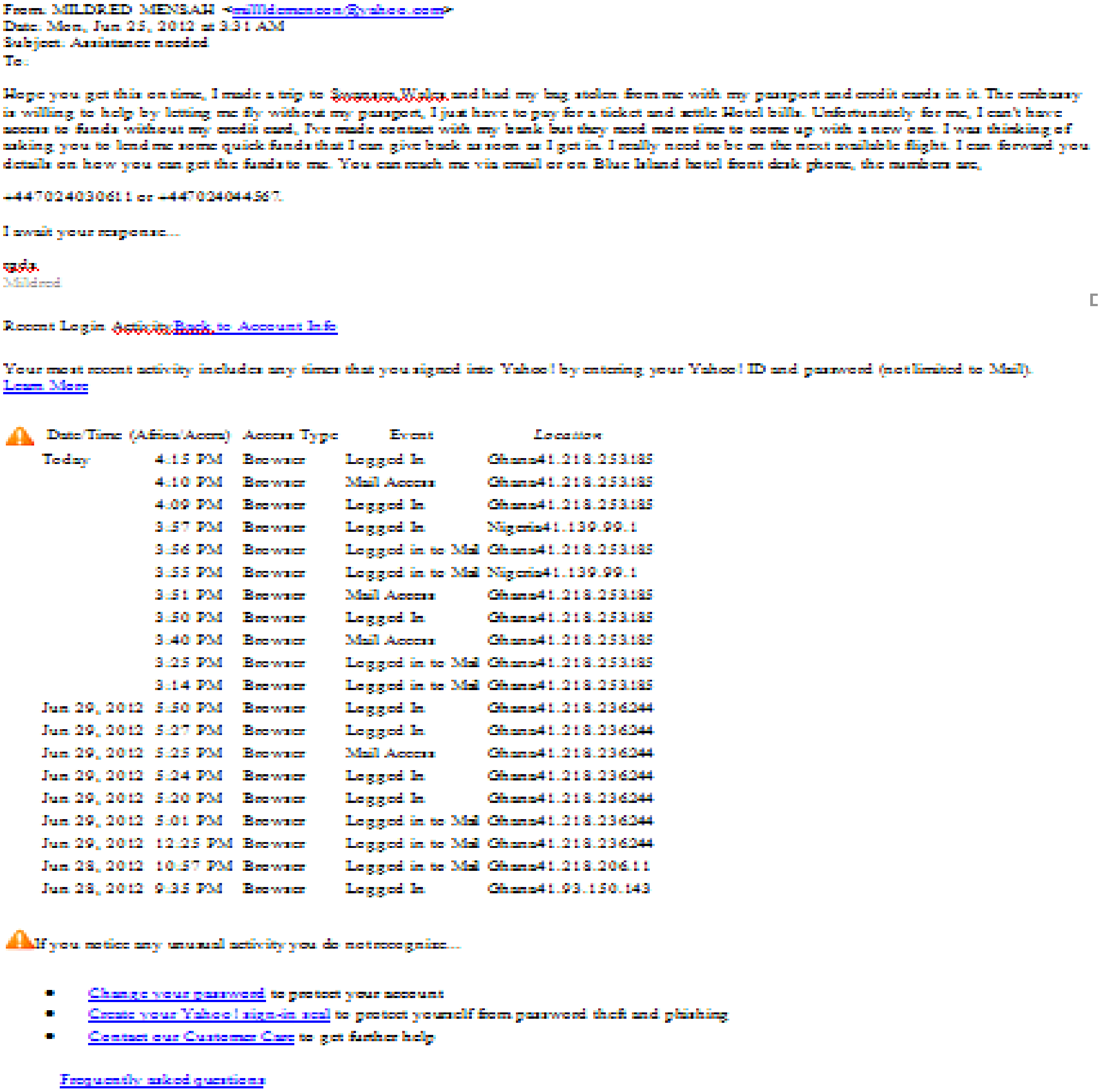
No.	**Metric / Parameter**
1	Total number of calls in a day/ High volumes of calls
2	Number of calls dropped in a day
3	Number of calls more than x minutes in duration
4	Less than x% international calls
6	Less than x distinct locations
7	Calls originating from specific telephone numbers and location (HLR)
8	Less than x% incoming calls
9	More than x% mobile-to-mobile calls.
10	Advanced Predictive Intelligence for Termination Bypass Detection and Prevention

One peculiar solution that was used by three of the telecommunication companies was a method very synonymous to the "Advanced Predictive Intelligence for Termination Bypass Detection and Prevention". All three companies using this method had however subscribed to foreign service providers whose sole business was to track down simbox fraud. They used the approach of generating one or more test calls from remote agents abroad to a local agents. The local agent is a subscriber number, the emphasis is on identifying the presence of bypass fraud by analyzing caller identification information of the test call received on the local number. Once a local number is detected, that number is blocked on the basis of being a fraudulent SIM box number. The telecom companies indicated that they felt extremely violated and embarrassed given the amount of money lost, effort that had gone into trying to remedy the situation and preventing future occurrence. A fundamental flaw in the setup of Ghanaian Telecommunications inter companies communication was the absence of an Interconnect Clearing House via which all calls could be routed.

3.5 The Case of Individuals

The case of individuals featured four individuals who volunteered to assist with the research by sharing their experiences. Three of these had their emails hacked whereas one had the debit card hacked. The mail accounts were hacked and numerous mails sent to contacts to solicit for funds. Some fortunately detected this early hence culprits were unable to block their accounts and access. The trailing mail shows an example of mails sent and subsequently results from the tracking facility that was used to detect the location form where the account was hacked.

Mildred is Ghanaian based in Ghana and a regular internet user from her home PC, the yahoo mail access tracker showed her account was compromised from Nigeria. A sample of the tracking is shown below;



From: MILDRED MENSAH <millidemensah@yahoo.com>
Date: Mon, Jun 25, 2012 at 3:31 AM
Subject: Assistance needed
To:

Hope you get this on time, I made a trip to Swansea,Wales and had my bag stolen from me with my passport and credit cards in it. The embassy is willing to help by letting me fly without my passport, I just have to pay for a ticket and settle Hotel bills. Unfortunately for me, I can't have access to funds without my credit card, I've made contact with my bank but they need more time to come up with a new one. I was thinking of asking you to lend me some quick funds that I can give back as soon as I get in. I really need to be on the next available flight. I can forward you details on how you can get the funds to me. You can reach me via email or on Blue Island hotel front desk phone, the numbers are,

+447024030611 or +447024044567.

I await your response...

regds.
Mildred

Recent Login ActivityBack to Account Info

Your most recent activity includes any times that you signed into Yahoo! by entering your Yahoo! ID and password (not limited to Mail).
Learn More

⚠ Date/Time (Africa/Accra)		Access Type	Event	Location
Today	4:15 PM	Browser	Logged In	Ghana41.218.253.185
	4:10 PM	Browser	Mail Access	Ghana41.218.253.185
	4:09 PM	Browser	Logged In	Ghana41.218.253.185
	3:57 PM	Browser	Logged In	Nigeria41.139.99.1
	3:56 PM	Browser	Logged in to Mail	Ghana41.218.253.185
	3:55 PM	Browser	Logged in to Mail	Nigeria41.139.99.1
	3:51 PM	Browser	Mail Access	Ghana41.218.253.185
	3:50 PM	Browser	Logged In	Ghana41.218.253.185
	3:40 PM	Browser	Mail Access	Ghana41.218.253.185
	3:25 PM	Browser	Logged in to Mail	Ghana41.218.253.185
	3:14 PM	Browser	Logged in to Mail	Ghana41.218.253.185
Jun 29, 2012	5:50 PM	Browser	Logged In	Ghana41.218.236244
Jun 29, 2012	5:27 PM	Browser	Logged In	Ghana41.218.236244
Jun 29, 2012	5:25 PM	Browser	Mail Access	Ghana41.218.236244
Jun 29, 2012	5:24 PM	Browser	Logged In	Ghana41.218.236244
Jun 29, 2012	5:20 PM	Browser	Logged In	Ghana41.218.236244
Jun 29, 2012	5:01 PM	Browser	Logged in to Mail	Ghana41.218.236244
Jun 29, 2012	12:25 PM	Browser	Logged in to Mail	Ghana41.218.236244
Jun 28, 2012	10:57 PM	Browser	Logged in to Mail	Ghana41.218.206.11
Jun 28, 2012	9:35 PM	Browser	Logged In	Ghana41.93.150.143

⚠ If you notice any unusual activity you do not recognize...

- Change your password to protect your account
- Create your Yahoo! sign-in seal to protect yourself from password theft and phishing
- Contact our Customer Care to get further help

Frequently asked questions

Figure 2: A Sample of the Tracking

The last whose debit card was hacked had a transaction he was carrying out on the internet interrupted and subsequently his debit card was used to make numerous purchases online. An assessment of the forms of cyber crime presents a myriad of effects amongst which are;

Loss of Revenue: One of the main effects of cyber crime on a company or an individual is a loss of revenue. This loss can be caused by an outside party who obtains sensitive financial information, using it to withdraw funds from an organization or victim’s account. It can also occur when a business's e-commerce site becomes compromised--while inoperable, valuable income is lost when consumers are unable to use the site.

Wasted Time: Another major effect or consequence of cyber crime is the time that is wasted when IT personnel must devote great portions of their day handling such incidences. Rather than working on productive measures for an organization, many IT staff members spend a large percentage of their time handling security breaches and other problems associated with cyber crime.

Damaged Reputations: In cases where customer records are compromised by a security breach associated with cyber crime, a company's reputation can take a major hit. Customers whose credit cards or other financial data become intercepted by hackers or other infiltrators lose confidence in an organization and often begin taking their business elsewhere.

Reduced Productivity: Due to the measures that many companies must implement to counteract cyber crime, there is often a negative effect on employees' productivity. This is because, due to security measures, employees must enter more passwords and perform other time-consuming acts in order to do their jobs. Every second wasted performing these tasks is a second not spent working in a productive manner.

Reduced Self Esteem: This is particularly the case with victims of cyber pornography and occasionally cyber violence, exposure of nude images, publication of hate or derogatory speech and crippling of online services or business activity tends to deflate the victims’ self esteem especially when none of these were executed without their consent.

4. RESULTS FROM PERPETRATORS

4.1 Results From Ethnographic Study;

4.1.1 Cases of Non-convicted Criminals (Observation and Interviews)

This was done upon obtaining a police clearance from the Ghana Police, a copy is provided in the appendix. Responses from the interviews and observations made showed that several varying approaches were used by the culprits to socially engineer their way into defrauding victims. These ranged from love scams, business men and contractors with fake pictures of ministers awarding contracts as newspaper items with evidence of documents, theft of credit card numbers etc. The focus of this study was however on those who typically engage in cyber trespass related crimes. Specifically, five cases were observed to determine the mode of operation, it was observed that remote servers with sensitive data were the most targeted with e-mail hacking also quite prevalent followed by credit and debit card hacking. Upon a close monitoring of operations, Trespassers have the following behavioural pattern:

Cyber Trespass:

1. Exploration
2. Gaining Access
3. Commit Offense
4. Clear Tracks (Optional)

The effect of this crime on the victim is also usually loss of money, waste of time, reduced productivity and loss of esteem. Perpetrators of cyber trespass on the other hand seemed to have a different approach, given the limited primary data gathered on cyber trespass, the deduced approach was derived from predominantly from secondary data. It entailed the following;

1. Exploration: This involves an exploration and scouting for potential targets, this may be either be a consciously effort or not, in some cases the perpetrators identify potential targets by accident.

- exploration and scouting for potential targets
- scanning/assessing target
- enumeration of vulnerabilities
- deciding on approach for launch

2. Gaining Access: Once they identify the target, they then work at gaining access to the target system from any possible loophole available. This sometimes may range from the Operating System level to Application level or Network level.
3. Commit Offense: Once access is gained, the offence is committed.
4. Clear Tracks (Optional): The spatio-temporal nature of the internet makes it possible for some perpetrators to disappear and not make their cyber footprints visible.

A striking consistency in responses from the interviewees at the telecommunication companies was the fact that, their respective call centers received countless reports of erroneous blocks on the basis of SIMbox fraud; this is understandably so since the use of just one parameter automatically changes subscriber numbers to SIMbox fraud blocked status. This implies, for instance in the context of the metric “Less than x% incoming calls”, if a subscriber line is used for just outgoing calls with a private or unknown caller identification, then it stands the risk of being labeled a SIMbox fraudulent number. Likewise, a mistakenly dialed number in the context of the metric “Advanced Predictive Intelligence for Termination Bypass Detection and Prevention” would wrongly label the dialing number as a SIMbox fraudulent number. On the basis of prevalent counter measures, the above listed metrics in under “The Case of Telecommunication Companies” and the concerns of erroneous blocking of subscriber lines, an optimum model is essential to comprehensively neutralize the SIMbox fraud.

Huge datasets that are constantly evolving in telecommunication industry brings about complexity of fraud detection method to be deployed and also fraudsters are adaptive, hence once it is known that one detection method is in place, they will change their tactics and try others. Many fraud detection systems are based on Call Detail Records or billing data. Existing methods of detecting fraud are based primarily on setting predetermined thresholds and then monitoring service records to detect when a threshold has been exceeded. Parameters for such thresholds include total number of calls in a day, number of calls less than one minute in duration, number of calls more than 1 hour in duration, calls to specific telephone numbers, calls to specific countries, calls originating from specific telephone numbers, etc. Many parameters can be used to tailor a particular thresholding system for certain customers or services. These thresholds must be manually programmed, which is labour intensive and time consuming. Moreover, these thresholds are generally subjective and not directly based upon empirical data. In addition, manually programmed thresholds are static and thus do not adjust to changing patterns of fraud. They are therefore easy for criminals to detect and circumvent.

5. DISCUSSION

Critical requirements to address the behavioural pattern of cyber trespassers are the need for a database of known system vulnerabilities, known scanning algorithms and the appropriate permissions to granted users of systems. These constitute components of framework to detect and counter cyber trespass .

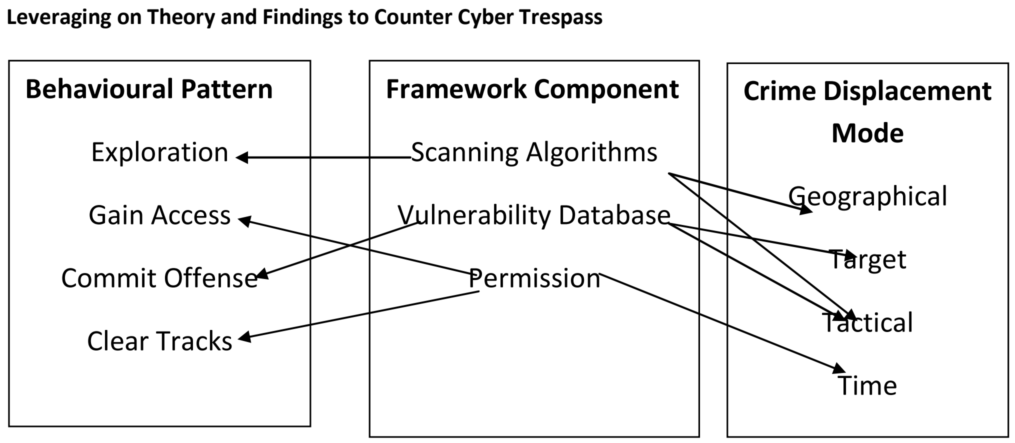


Figure 3: Relationship between Theory, Behavioaural Patterns and Anti-Cyber Trespass Framework

The figure 3 shows the deduced behavioural patterns for cyber trespass and also shows the components of the proposed framework, on one hand the essential components of the crime displacement theory is also shown with arrows showing the relationship between the three and their respective components. The crime displacement theory indicates that for crime to be neutralized, it must be displaced from one local to the other. Technically, the components of the framework namely permission displaces crime temporally, the scanning algorithms displace crime geographically and tactically whereas the vulnerability database displaces crime tactically and from a target perspective. The outlined components of the also in turn neutralize the various steps in the behavioural pattern, as shown, the permission component prevents perpetrators from clearing their tracks and also gaining access, the vulnerability database component prevents the offense commission once the appropriate safeguards are implemented. The framework therefore sets out to place these relationships in perspective to counter the specific category of cyber crime as shown in figure 4.

5. CONCLUSION

The framework unifies various approaches to implementing cyber security, much as it is inductive, its development was based on deduced consistent behaviour. It is important to emphasize that the framework does not apply to the types of cyber deception and theft that exclude social engineering such as intellectual property violation and cyber piracy. The framework leverages on a combination of scanning detection algorithms, permission**,** vulnerability database and a trespass detection system to counter any form of trespass on an operating system, an application or a network.

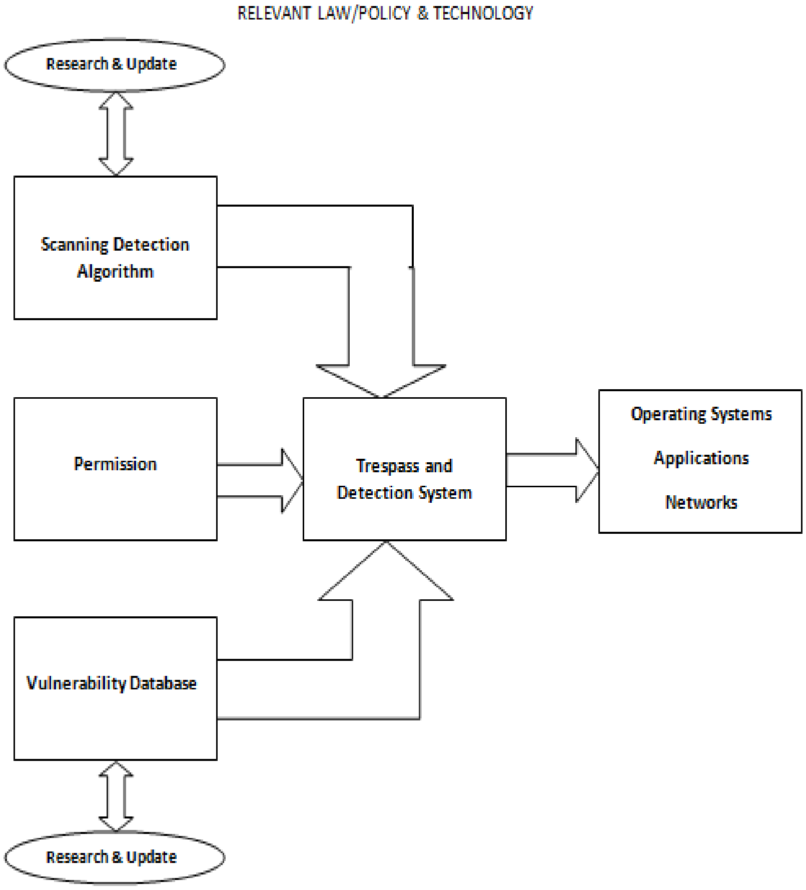


Figure 4: Framework to counteract cyber trespass

Below are antecedents to components of the framework;

Table 1: Table Describing Antecedents of Framework

Breach Approach	Antecedents
Scanning Algorithms	• Identify Target • Scanning • Footprinting • Enumerating • Identify Vulnerabilities
Permissions	• System Hacking • Escalating Privileges
Vulnerability Database	• Purpose Driven Activities
Trespass Detection & Prevention System	• Delete any visible logs • Exit from System • Delete any possible evidence of access log

Definition of Antecedent

- **Scanning Algorithms** refers to a set of procedures for identifying hosts, ports, and services in a network. Scanning is one of the components of intelligence gathering for an attacker to create a profile of the target organization.
- **Permissions** refers access, identification, authentication, authorization and privacy in resource usage on systems and a network.
- **Vulnerability Database** is collection of known vulnerabilities of various operating systems, networks and applications.
- **Trespass Detection & Prevention System**: This is the engine that leverages on the three previous components to obtain knowledge of a breach or potential breach in security of user's system.

REFERENCES

1. Blaike, N. (2009). Designing social research. *Cambridge: Polity Press.*
2. Bossler Adam M. & Holt Thomas J.,(2009) Online Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory, *International Journal of Cyber Criminology (IJCC)* 3 (1): 400–420
3. Brenner, S.W. 2004b, Toward a criminal law for cyberspace, Distributed Security.Boston University *Journal of Science & Technology Law* 10 (2).
4. Cohen L. E., & Felson. M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44: 588-608
5. Cox, Johnson & Richards (2009), Routine Activity Theory and Internet Crime, *Crimes of the Internet*, Pearson, p.302-316
6. Danquah P. & Longe O.B.(2011). An Empirical Test Of The Space Transition Theory of Cyber Criminality: The Case of Ghanand Beyond. Afr J. of Comp & ICTs. Vol 4, No. 2. pp 37-48
7. Felson C. & Clarke R. (1998), Opportunity Makes the Thief: Practical Theory for Crime Prevention, *Police Research Series, Research Development and Statistics,* UK, Paper 98
8. Jaishankar K., (2008), Space Transition Theory of Cyber Crimes, Crimes of the Internet, Pearson, ISBN-13:978-0-13-231886-0 .283-299
9. Katyal, N.K., (2001). Criminal Law in Cyberspace, *University of Pennsylvania Law Review*, 149
10. Ngo F. & Jaishankar K.(2017),Commemorating a Decade in Existence of the International Journal of Cyber Criminology:A Research Agenda to Advance the Scholarship on Cyber Crime. International Journal of Cyber Criminology,ISSN: 0973-5089,
11. Sung M. B.(2017),The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study, Children and Youth Services Review, Volume 78, July 2017, Pages 74-80, Elsevier
12. Yar, M (2005). The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology* 2(4): 407-27