The Legal and Ethical Issues of Deploying Honeypots

Honours Project (INF412-H)

University of South Africa

By

Ronald Mitchell Campbell

3274-194-4

A report submitted in *partial fulfilment* of the requirements for the *degree*

B.Sc. (Hons)

Supervisor

Professor K Padayachee

Abstract

The purpose of this study is to identify the legal and ethical issues involved with the deployment of a computer system defence implementation known as a honeypot. During the course of this research reference shall be made to the term honeypot as an umbrella term covering honeypots themselves, honeynets, honey farms and honeytokens. These systems and devices all claim a common characteristic in that they masquerade as legitimate systems, however their main purpose is to detect, track and analyse patterns of behaviour, both user and software, when the system is illegally accessed.

The aim of this research is to derive a strategic framework for minimizing the legal and ethical risks involved in deploying honeypots specifically within South Africa, but based on best practice from around the globe. The study will derive a taxonomy for honeypots based on their security goals. The taxonomy will serve as basis for evaluating the legal and ethical risks relative to the security goals of honeypots.

The study has been conducted using a wide ranging literature review covering the legal landscape with regards to the areas of entrapment, privacy and liability, and their application in the field of cybercrime based upon the current legal framework in South Africa. This research will determine the different scenarios in which honeypots may and should be deployed and the ethical issues involved in deploying a honeypot specifically addressing the alignment with the various codes of conduct required by computer professionals.

The ethical and legal risks involved in the deployment of a honeypot will be highlighted and ultimately a strategic framework for minimizing the legal and ethical issues involved with the deployment of honeypots will be outlined. This will take the form of a checklist designed to guide the practitioner in deployment of these tools in a legal and ethical manner.

Preface

This research was conducted on a full-time basis between Ronald Campbell in collaboration with the School of Computing at the University of South Africa under the supervision of Professor K Padayachee. The results are the original work of the author and have not been submitted for any degree at any other tertiary institution.

_____

SIGNATURE

_____

DATE

Acknowledgements

I would like to thank my wife, Madelein, and children, Ffyona and Aerynn, for their forbearance during the course of compiling this Research Paper. Also to the guys at, the now defunct, InfoPlan who wound up with sticky fingers…you know who you are.

Contents

List of Figures

List of Tables

No table of figures entries found.

Chapter 1: Introduction

1.1 Introduction

With the proliferation today of networked devices there is a massive increase in network based attacks. Kaspersky Labs (2010) estimate the number of web based network attacks at approximately 580 million. With this proliferation of attacks a way of identifying this type of unwanted behaviour needs to be implemented, however this defence needs to be implemented in a manner that is both legal and ethical.

There are various views on where the term honeypot originated, whatever the origin of the term, in the computer security landscape, the term honeypot as defined by Mokube and Adams (2005) has come to characterise computer system implemented as a decoy network that is used to entice would be attackers into exploiting the system with the various tools within their hacking toolkit.

This research focusses on honeypots as a defence strategy for both monitoring attack behaviour and recording proof of wrongdoing. Currently there are few guidelines to assist practitioners in directing the implementation of a honeypot in a manner that is both legal and ethical. The main focus of this research is to examine the legal framework within South Africa and the ethical constraints within the Information Technology sphere to produce a practitioner's guideline aligned to these topics.

The rationale for this approach is that there is the possibility of legal recourse from the point of view of an attacker or a damaged third party if the honeypot is incorrectly implemented. Honeypots pose legal risks as they may be used as platforms for attacks on external parties. Privacy and entrapment issues span both legal and ethical boundaries.

In addressing the question of what the ethical and legal issues are involved in deploying honeypots the various actors and agents who have a role to play within this environment need to be identified. Throughout this research reference is made to attackers and defenders. Attackers are the individuals wishing to gain unauthorised access into a system and the defenders are the persons responsible for setting up the countermeasures.

The research methodology adopted is a literature study incorporating the Internet, various Industry specific Journals and Symposium papers on the topics of Honeypots, Ethics and Legal Issues involved in the computer security industry. This methodology was adopted to give both a historical perspective of the technology as well as to show the evolving nature of the regulatory framework with regards to the area of computer security.

1.2 Problem Statement

There is little in the way research in the topic of honeypots and their implementation in both a legal and ethical manner. This is especially true in the South African context where no published research was found during the literature study conducted for this research.

Honeypots need to be implemented ethically to ensure that they do not become data gathering tools. Deployment of a honeypot without regards to the legal framework governing the country of deployment, specifically in terms of liability for the leaking of personal information, has the potential to see the security professional moving from the prosecution to the defence side of the courtroom. It is this area that this research will be attempting to address.

1.3 Project objectives

The objective of this project is to examine the legal implications of implementing a honeypot along with the ethical considerations thereof and to derive a practical set of guidelines aligned with these two areas for a honeypot installation. This will be accomplished by the following sub-objectives:

- Reviewing available literature, research papers and conference proceeding on the topic;
- Reviewing the current government legislation applicable within this space;
- Evaluating the pertinent sections of the applicable Acts and Bills to determine whether any illegality exists for the implementation of a honeypot
- Deriving a taxonomy for the field of honeypots and their implementation based upon their security goals.
- Deriving a strategic framework in the format of a checklist for the ethical and legal implementation of a honeypot in the South African context.

The aim of this research is to derive a strategic framework for minimizing the legal and ethical risks involved in deploying honeypots specifically within South Africa, but based on best practice from around the globe. The study will derive a taxonomy for honeypots based on their security goals. The taxonomy will serve as basis for evaluating the legal and ethical risks relative to the security goals of honeypots.

1.4 Project design

This study will be based on a literature review of domain specific sources, Information Technology Industry Standards documentation as well as Government legislation being used as input for the purposes of deriving a checklist to be used as a guide for implementing a honeypot.

1.5 Outline

Following this chapter, the rest of this report is structured as follows. Chapter 2 commences with an introduction to where honeypots originated and then delves into the different types of honeypots currently implemented in both production and research environments. Following this a short introduction to the various deployment modes for honeypots is done and finally the benefits and risks involved with the implementing of honeypots in the research and production spaces is examined.

In Chapter 3 the various legal and ethical issues associated with the implementation of a honeypot, particularly within the South African context is examined. Reference to the Electronic and Telecommunications Act and the Protection of Personal Information Bill is made with a view to proposing the type of information that can be collected and stored regarding an attacker's details.

In Chapter 4 the Research Methodology is outlined including the limitations of the research. Chapter 5 deals with the Taxonomy derived during the course of this research and in Chapter 6 the checklist of process steps uncovered and derived during the course of this research is outlined before presenting the conclusions to this research in Chapter 7

1.6 Relevance of this research

Whilst doing this research it has become apparent that there is a general lack of knowledge or difference of opinion on both how and where a honeypot should be implemented and the type of data that can be stored about an attacker. An example of this is the issue of entrapment. Spitzner (2002) infers that the concept of entrapment does not apply to a honeypot in that definition of entrapment as outlined above almost implies coercion on the part of the honeypot owner. Biggs (2013) on the other hand refers to the practice of baiting internet download sites with multimedia used to track IP addresses of individuals downloading the media as entrapment, this even though the baiting is not necessarily done by an officer of the court.

Given the differing viewpoints and the mounting legislation being promulgated with regards to electronic transactions and personal information it becomes important for an IT Security professional to ensure that when a system is implemented that is intended to track user behaviour, that that professional understands what can and cannot be stored and what should or should not be tracked.

In providing clear guidelines to the implementation of a honeypot which has been correlated to the relevant South African legislation this research is intended to provide a suitable checklist for security professionals to employ when implementing a honeypot type solution. Using the guidelines outlined within this research endeavour it is anticipated to that the implementer is given a view as to whether their approach is covered from both a legal and ethical point of view and contravene no current legislation.

1.7 Scope and Limitations

The checklist that has been produced must be viewed as this researcher's interpretation of the current legislation and, as such, implementation thereof should be ratified by a legal counsel prior to the deployment of a honeypot as the researcher does not have a background in law.

1.8 Summary

Given the paucity of research in the South African arena of the legal and ethical implications involved in the deployment of a honeypot this research is intended to provide security professionals with a framework upon which decisions can be made with regards to the implementation of this type of security tool.

This chapter has given a brief introduction to the scope of the research contained herein. The next chapter focusses on the background and distinguishing characteristics of honeypots, their deployment modes and deployment scenarios.

Chapter 2: Literature Review

2.1 Background of Honeypots

Spitzner (2002) details a timeline from the point of Stoll's publication in 1990 through to his own publication in 2002. Essentially the early toolsets were coded and implemented by individuals for a specific purpose. As access to the Internet grew more widespread the need for tools that could be easily configured grew. To this end Fred Cohen released his Deception Toolkit. This Toolkit was used to publish fake services that could be attacked by individuals intent on breaking into a system and was the first example of a honeypot type implementation that could be widely used.

Pelletier and Kabay (2003) define a honeypot in a much broader context as a system whose express purpose is to be exploited in a manner contrary to the terms of service of that system. Furthermore, Azadegan and McKenna (2005) state that the purpose of the honeypot is to determine tools and techniques utilised by hackers and to utilise this data to analyse these incursions and prepare rules for Intrusion Detection Systems to ensure that similar techniques cannot be used to gain access to these more strategic information systems.

Cowan et al (2000) describe the Deception Toolkit as 'most effective at disguising a genuine service provider by surrounding it with faux service providers'. At this point the general idea was to model specific services to provide as a target rather than to model entire environments. Joshi and Sardana (2011) expand the field further with their description of the dynamic honeypot concept where the system learns from the type of attack in order to keep it relevant. This is done so that when attackers learn that there is a weakness in the honeypot design, the system can reconfigure itself in order to prevent denial of service attacks from bringing down the honeypot. Abbassi et al (2013) describe this type of learning by example as exemplar learning

Since the first implementation of the Deception Toolkit, the field of honeypots has advanced and created a number of different implementation types and are profiled according to the amount of interaction that attackers can have with the system. These different levels of interaction, classified as low, medium and high, and various types of honeypot implementation will be discussed in section 2.2.

Arguably the best definition of a Honeypot is provided Mokube and Adams (2005) who characterise a honeypot as a decoy network that is used to entice would be attackers into exploiting the system with the various tools within their hacking toolkit. Every interaction with the system is monitored and recorded and the output can be used to implement rules on Intrusion Detection Systems.

It differs from a traditional passive, fortress based approach to security characterised by Baker (1996), which implements security measures such as firewalls and Intrusion Detection and Prevention Systems to keep attackers from gaining access to system resources to create a 'centralized reference validation mechanism with knowledge of and control over the system entity'.

Edmead (2002) lists the following advantages of using honeypots within organisational security toolsets:

- Honeypots deter attacks just by virtue of their implementation;
- Honeypots cause attackers to focus on the exploitation of non-core systems allowing for more time to bolster the security posture within the production systems;
- They allow for research to be conducted on the latest attack vectors; and
- They can detect insider attacks

2.2 Types of Honeypots

2.2.1 Shadow Honeypots

Anagnonstakis et al (2010) define a shadow honeypot is a mixture of both honeypot and anomaly detection which is any behaviour on the network which

is not considered as ‘normal’ or is characterised as suspicious according to a set of pre-defined rules. Eskin et al (2002) define these rules as a set of signatures against which traffic is compared. If a known signature is found in the network traffic, then the system is alerted of anomalous behaviour. In this type of implementation network traffic that is thought to be suspect is diverted to a shadow network. This network contains a safe, monitored instance of the application that the suspected attack is being directed against.

This instance of the application shares an internal state with the real or live application and as such is a replication of the live system, meaning that the two systems are kept synchronised with regards to functionality. The idea behind this is to capture malign behaviour but also to transparently route the user back to the real system in the event of traffic being determined as suspect or hostile in error, (Briffaut, Lalande and Toinard, 2009).

2.2.2 Honeynets

Spitzner (2002) defines a honeynet as ‘nothing more than one type of honeypot. Specifically, it is a high interaction honeypot designed primarily for research, to gather information on the enemy,. A honeynet is different from traditional honeypots, it is what we would categorize as a research honeypot’. The enemy that Spitzner refers to is defined as anyone trying to break into the target system.

Hoepers et al. (2003), in a distinction from Spitzner, define a honeynet as ‘a research tool consisting of a network specifically designed for the purpose of being compromised, with control mechanisms that prevent this network from being used as a base for launching attacks against other networks’. The difference between these two definitions is the extent and boundaries of the network involved in the honeynet. This network consists of multiple machines which mirror the traffic flow of a live network

Sarabadani (2012) describes the type of information that can be collected via a honeynet as determining the '…full extent of the attacker's behaviour, characteristic [sic], damage, keystrokes, and even the tools they use from new rootkits to communication on the international IRC sessions'.

This illustrates the emphasis in a honeynet in extracting the maximum amount of information regarding the attacker's toolsets and methods.. Spitzner (2003) classifies this derived value as 'response' in his prevention, detection and response hierarchy of value, as the information is used to protect production systems.

2.2.3 Honeyfarms

Jiang, Xu and Wang (2006) describe a Honeyfarm as a dedicated set of honeynets (i.e. high interaction honeypots sitting on a network segment implemented in such a fashion as to appear to be a functional computing unit comprising different types of machines with various purposes and weaknesses.

The idea behind implementing multiple machines is that as opposed to a one dimensional view of an attacker gained from a honeynet, the defender is able to gain a broader view both of attack behaviour and identification of anomalous interactions between different systems. Whilst there is little semantic difference between the Honeynet and the Honeyfarm, Jiang et al (2006) focus on the scale of the implementation in providing this distinct type of honeypot

2.2.4 Honeytokens

Whilst the objective of this research report is to discuss honeypots, the area with the most current focus on ethics and legal issues is the area of honeytokens. Spitzner (2003) defines a honeytoken as a piece of information which is placed in a computer system to be accessed by someone who does

not own the information. The information is uniquely identifiable as having come from a particular source.

The relevance of honeytokens at the moment is due to the increasing use of these devices by police services and copyright infringement agencies internationally to trace and identify perpetrators of copyright fraud, particularly with regards to the illegal downloading of music, television series and feature length films, (Biggs, 2013). Identifiable markers can be both visibly and invisibly placed on the media in question to determine the origin of the copyright material and can be checked back against a known source in the event of a legal dispute. This method of catching individuals flaunting copyright is discussed in more detail in Chapter 3 under the Entrapment section 4.2.

2.3 Honeypot Interaction Levels

One characteristic of honeypots is their interaction level. This is the degree to which an attacker has access to system services. The interaction level ranges from low, where there is little to no access of the system services allowed through to high interaction systems where the attacker has full access to the system's functions.

2.3.1 Low Interaction Honeypots

Lall and Vivek (2012) describe a low interaction honeypot as one where interaction with system services are kept to a minimum. Typically the attacker is kept within the bounds of the system ensuring that the honeypot cannot be used as a base to launch attacks to external systems. This has the added advantage of limiting the liability of the person or organisation deploying the honeypot where no damage can be made to external systems.

Whilst this limitation in liability may be advantageous from both a business and possible costs point of view, the disadvantage to a low interaction honeypot is that its true nature can be identified relatively quickly. Mukkamala

et al (2007) describe a method of 'service exercising' in order to detect honeypots based on the length of time ports within the system take to respond to a simple ICMP packet (a 'ping' command).

The major disadvantage of the identification of a honeypot is that once an attacker has determined that the system is indeed not all it appears to be, that it is marked and discarded as a source of potential resources, thus ensuring that the primary reason of existence for the honeypot (i.e. to gather data on attackers), no longer signifies.

2.3.2 Medium Interaction Honeypots

Medium interaction honeypots implement a reduced set of services as in the case of a low interaction system(Lall and Vivek, 2012). The difference between the two is that the services have some intelligence built into them so that it is not immediately apparent that the system is indeed a honeypot.

Lall and Vivek (2012) characterise the medium interaction model as being able to respond in an acceptable manner when a service is queried. The main difference between the low and medium interaction systems and a high interaction system lies in the fact that for a high interaction system a full operating system is deployed, with full functionality on all services as opposed to the system emulation performed by the low and medium interaction systems, (Gibbens and Rajendran, 2012).

John et al. (2011) implemented a range of what they termed 'heat seeking Web-server based honeypots' whereby the honeypots were designed as full web servers but were specifically configured with versions of Web Server software that contained known attack vectors. They then studied attacks and when the situation warranted further study a high interaction honeypot was set up where the attacker could then actually interact with the real services.

2.3.3 High Interaction Honeypots

As mentioned previously a high interaction honeypot implements a full operating system with the entire range of system functionality available to the attacker once the system has been penetrated. This means that this type of system can be used to launch attacks on other systems and thereby start attracting liability issues which are discussed further in Chapter 3.

Spitzner (2003) refers to a high interaction honeypot example which he terms a honeynet. As the full operating system is made available for the hacker to utilise in a high interaction honeypot it becomes important to provide an entire network of machines which they can attack otherwise the system will quickly be seen for what it is – a dead end.

2.4 Deployment Modes

Scottberg et al. (2002) define honeypots as being deployed in one of three modes namely for deception, intimidation or reconnaissance purposes. Each of these deployment modes with its associated objectives will be described in detail below. It should be noted that attacks to an IT system can originate from either inside or outside an organisation and similarly a honeypot can be positioned with a focus on internal, external, or both, threats.

In general accessing a system requires an elevation of privileges of some sort. Kassner (2011) alludes to the prevailing thought that due to this elevation of privilege most (up to 80%) of incursions are performed by insiders or staff. However this statistic was based on FBI investigations of some 20 years ago. Given the resources that external agents now possess the implementation of a honeypot needs to cater for both these internal and external attacks.

As Kassner (2011) explains whilst there may be more external threats today, as a rule internal attacks tend to cost an organisation more money. However in a world which now has state sponsored cyber-espionage and links between government and Original Equipment Manufacturers this balance in terms of attack cost is bound to shift to external attacks in the short to medium term.

2.4.1 Deception

Deception in the context of honeypots refers to the manipulating of a hacker to believe that the responses being received come from a live system. Martin (2001) refers to deception within the IT context as a system which is used as a decoy and contains security weaknesses in order to attract hackers.

Deception techniques are used to ensure that the hacker implements the widest array of hacking tools at his disposal to ensure the honeypot implementers are deriving as much information as possible to be utilised in the protection of production systems. A honeypot according to Scottberg et al. (2002) is involved in deception activities if its responses are used to deceive an attacker into thinking that come from a fully functional production system.

This information gathered could be toolset based in that the software the attacker is using to attempt to compromise the system is identified. Alternatively the system could record the attack patterns themselves including time, port probes and actions initiated and use this information to create or modify the Intrusion Detection System rulebase.

Finally the system could attempt to gather any personal information pertaining to the attacker. This would include data such as source IP addresses, platforms, and mail sent or chats initiated whilst within the system boundaries. This type of information, if it is going to be used in a criminal case, should be prepared in such a manner that it will stand up to scrutiny in court. As such

legal counsel and specialist forensic auditor advice should be consulted when this is the case.

2.4.2 Intimidation

Intimidating a would-be hacker with a computer system is done by making the hacker aware that measures to ensure security are in place in the system. Lakhani (2003) uses an example in his thesis to highlight why an intimidation tactic would be used. In discussing types of hackers, he differentiates between novices (those with very little knowledge about what they are doing), script-kiddies (who may have some view as to what they are doing, but utilise hacking tools developed by someone else) and finally blackhats – the hackers with in-depth knowledge of hacking techniques and operating system vulnerabilities.

Obviously it is not cost effective or even resource effective to capture activity from the first two groups as the chances of determining new attack vectors from these individuals is low. A warning mentioning that the site is monitored may scare the bulk of these would-be attackers off. In this way the Intimidation tactic, lowers the amount of data that needs to be processed and makes the honeypot more cost effective.

To intimidate an attacker, a honeypot would need to advertise itself on one or more ingress points as an active security monitoring device. Here the intention is to make the attacker aware that his actions are being monitored and that his access to the system has been recorded, (Scottberg et al. 2002).

The result of this type of message will generally result in the termination of the incursion by the attacker. Spitzner (2002) recommends the implementation of a banner on commonly accessed points of entry into the system along the lines of telling the person accessing the system that the system is monitored, is a private system and furthermore that by accessing the system the user

agrees to have any interactions with the system recorded and handed over to third parties in the case of any disputes arising.

2.4.3 Reconnaissance

Within the Security field the term Reconnaissance is used in both the attacker's and the researcher's contexts. The attacker scans the target systems for vulnerabilities before making any incursions. Schrage (2004) states that one of the more important features of a honeypot is the ability of the system to capture and document new exploits for gaining access to a system.

In reconnaissance mode, on the defender, or researcher's side the honeypot is used to determine what tools and techniques are being utilised by the attacker. It determines the attack surface of a system and the extent to which it is vulnerable. This information is stored and then used to determine rules implemented in production based system including the implementation of heuristics based rules in Intrusion Detection and Prevention Systems. This can be done manually, or as in the Giakouminakis et al. (2010) patent US 20120174228 A1 for Google detailing 'methods and systems for integrating reconnaissance with security assessments for computing networks' it can be done automatically.

In this mode a honeypot is an ideal vehicle for detecting both internal and external attack vectors. The difference between a Reconnaissance and a Deception deployment mode is that whilst both modes attempt to extract usable data from an incursion, a Deception deployment will actively try and keep the attacker on the system as long as possible by feeding back information which is designed to be engaging. This could be along the lines of revealing further networks within the organisation, which would, in this type of scenario, be additional honeypots or honeyfarms.

2.5 Deployment Categories

Spitzner (2002) classifies honeypots within two general categories namely being used in production and research environments. Production honeypots are used in general when there is an existing threat on a system and the implementer is looking to identify a specific individual in terms of actions taken upon the system.

We shall now examine these systems with their associated benefits and risks in more detail.

2.5.1 Production Honeypots

Production honeypots are used to protect systems that are being utilised by an organisation in other words, real world systems housing corporate or research data. Spitzner (2002) defines the three security goals based on Schneier's (2000) earlier definition in determining the value that the honeypot can add to the system. These three categories are Prevention, Detection and Response are discussed further in Security Goals, Section 2.6.

Production honeypots are used in cases where there is an active threat to a system. Spitzner (2002) speaks to the use of a honeypot to catch internal threats to an environment. An internal threat is one where the attacker is part of, or has links inside, the targeted organisation.

2.5.2 Research Honeypots

Research honeypots on the other hand are implemented with a specific goal in mind and exist, in general, to track and record behaviour rather than to catch and punish intruders. This information is then utilised to update toolsets that protect production systems.

Research honeypots on the other hand are set up to determine new methods of attack and translate this information to new defensive strategies on

production systems to combat hackers. Spitzner (2002) further defines the advantages of a honeypot as the following:

- Data Value
  All data collected within the honeypot is by definition valuable as there should be no reasonable reason for external persons to access this system
- Resources Utilized
  A honeypot uses less resources as the attacker is not trying to flood the system to attempt to get into it, he is attempting to expose specific parts of it to scrutiny. As such there is much less chance of the 'resource exhaustion' that an exploit such as a Denial of Service attack would bring.
- Simplicity
  Intrusion Detection and Prevention Systems and other active security frameworks need to be constantly updated. The Honeypot does not as it is left in its original state until it has served its purpose.

Disadvantage of honeypots are defined by Spitzner (2002) as follows:

- Fingerprinting
  Whilst a honeypot can be used to identify attacks (Thakar et al. 2005) there is a corresponding risk that honeypots can be identified by how they respond to specific types of attacks – this response is known as a signature or a fingerprint.. This let the attacker know that the system is not a valid production system.
- Narrow field of view
  A honeypot can only provide value if an attack is launched against it. If it has been fingerprinted as a honeypot then would be attackers will bypass it and search for other targets on the network.
- Risk
  Finally, high interaction honeypots can be used as a springboard for attacks on other systems both inside and outside the boundaries of the honeypot's network. This may expose the person or company implementing the honeypot to legal risk if information is stolen from these systems based on weaknesses in the honeypot implementation.

2.6 Security Goals

The security goals of a honeypot relate to the type of job that it expected to do. Seifert et al. (2006) classify these as Block, Defuse, Slow Down and None. Block as it intimates, restricts access to a system, defuse allows access to a system, but does not allow the attack to proceed against a target. Slow Down, as with Defuse allows access to the system, but at a much reduced rate of engagement with the system allowing defenders time to study and track actions. None allows the attacker to perform any action without any system intervention.

Schneier's (2000) original definition of the security goals of a system are Prevention, Detection and Response. The goals are more aligned with this research studying the legal and ethical implications in deploying honeypots and have therefore been used as a basis for defining the security goals.

Prevention as defined by Kalogridis (2012) has to do with stopping attacks from occurring within a system. Detection is ensuring that any unauthorised activity within a system is reported and that the appropriate people are alerted. Spitzner (2002) states that at some point, prevention will fail – perhaps due to human error or a new unknown attack vector – and at this point the operator of the system must be warned that an incursion has happened.

Honeypots add value in two of these three categories, that of Detection and Response. Honeypots, by definition, are designed to entice attackers to enter the system therefore they have little value in the Prevention category. In terms of Detection any activity within the honeypot is by definition a detected activity as the system is not supposed to have any activity but that provided by an illegal access.

The final category, that of Response also has the honeypot adding value to an organisation in that as the system is relatively 'clean', meaning that audit trails

and logs are focussed on the hacker's actions. As such the tracking of illegal access and subsequent information logs do not require that a huge amount of non-pertinent data be handed over to the authorities.

2.7 Summary

In this Chapter the background to honeypots has been examined from their initial appearance in the early 1990's through to virtualised, adaptive systems that are being implemented today. Types of honeypots were then defined along with their characteristics and implementation examples. Finally the advantages and disadvantages of these systems with respect to their implementation within production and research environments were discussed.

In the next chapter, we shall examine the regulatory framework within both an American and South African context to determine the concerns that should be raised before implementing a honeypot. Finally the ethical considerations involved in this type of endeavour are detailed along with the corresponding concerns.

.

Chapter 3: Research Methodology

3.1 Introduction

Oates (2006) in her book Researching Information Systems and Computing describes a literature study as having two phases. The first phase is the examination of various journals, books and internet articles to determine a topic and define a problem statement. The second phase of research proceeds throughout the rest of the research time, up until the report is delivered and is intended to provide support for the arguments made during the problem statement.

In this study, data was organised using a directory structure and a Microsoft® Excel™ spreadsheet. Data sources were categorised in the following manner:

- Year of Publication;
- Country of Origin;
- Source Type; and
- Subject.

This information was used to produce the category breakdown listed below. Values produced on the y-axes are actual totals and should not be interpreted as being percentages.

3.2 Research Material by Year

The following diagram (Figure 1) depicts a view of the year of publishing for the books, articles and web pages contained within the References section of this document. As depicted, the bulk of the research around honeypots was conducted in the 2002 – 2004 timeframe. Possible reasons for the interest around the 2002 – 2004 timeframe may have to do with the publication of the Spitzner's (2003) book and the general lack of internet security standards at the time.

Another possible scenario is that those latecomers to the Internet who had waited for Y2K to come and go before adopting technology were beginning to see issues with their systems being on-line. A final possible cause of this spike could be due to the generation of children who had grown up with a PC as a more commonplace household item were now starting to buy their own equipment and start exploring the World Wide Web which now had many more connections made to it by companies than before.

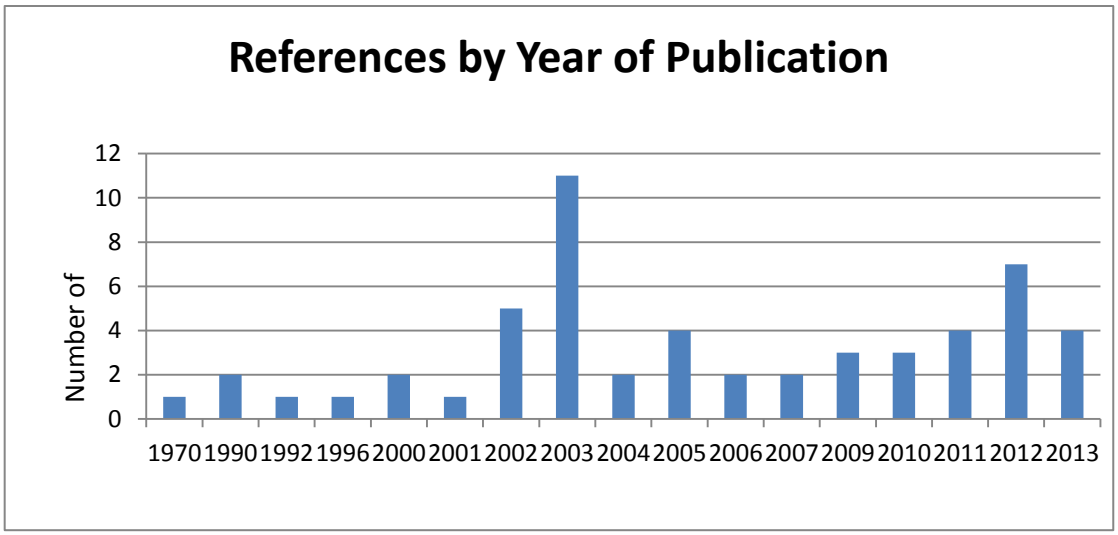

Figure 1: References by Year

3.3 Research Material by Country of Origin

The following diagram (Figure 2) depicts the origin of the research used in this research report. As shown in this figure, the majority of research has emanated from the United States of America. Whilst this may seem to indicate that Americans are either more concerned with security, or are victims of more hacking than anyone else, no valid conclusion could be drawn in this regard. Searches were done using Google Scholar (an American Search Engine), for English language results. The bias seen in this graph may be as a result of these parameters.

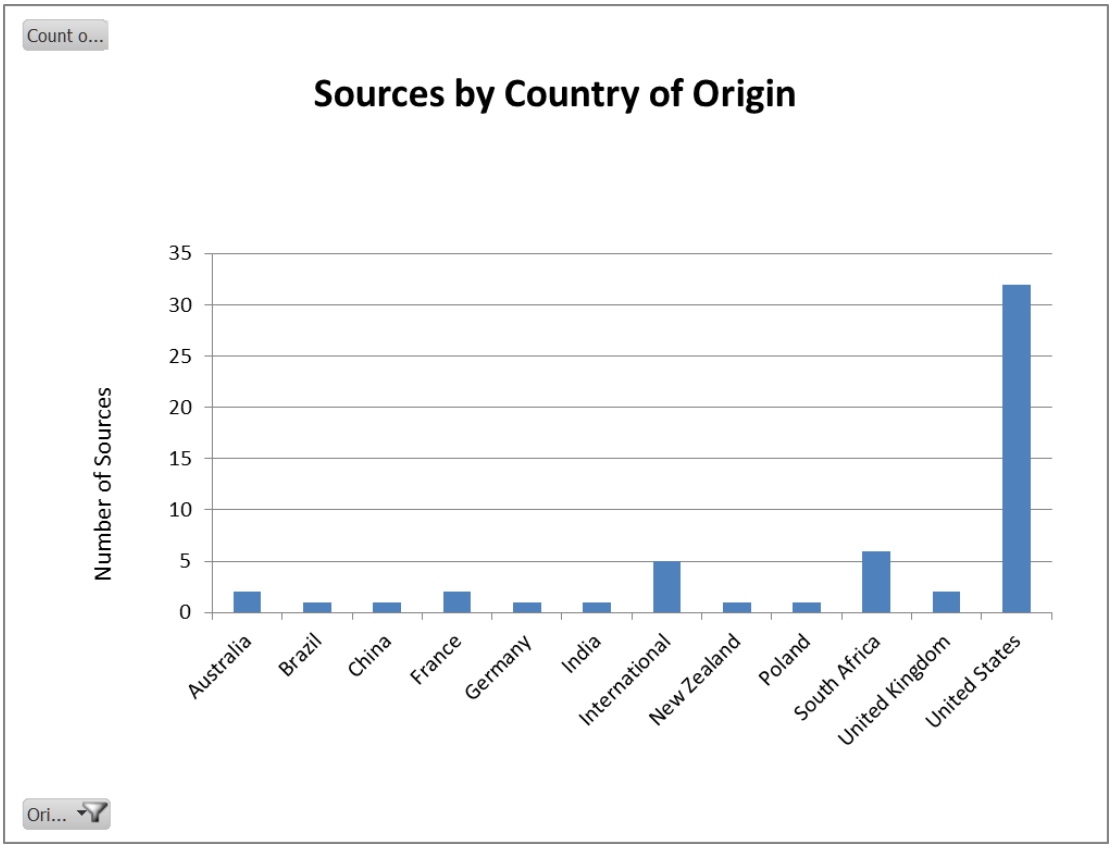

Figure 2: References by Country of Origin

3.4 Research Material by Publication Type

During the course of this research many sources of information were examined and discarded due to duplication of information or non-relevance to the topic at hand. The majority of research was done utilising web pages and journal articles. References in each article were scoured for addition information sources. The majority of journal articles such as those contained within the IEEE Xplore system and the Association of Computing Machinery Digital Library were accessed via the Unisa Oasis system, with local copy PDFs being stored on a personal computer and printed out.

In terms of articles on Ethics, the COBIT 5 standards were reviewed as there has been a substantial increase in the awareness of ethics in the computing field since the previous revision. The IT Information Library standards were also reviewed for salient information in this regard.

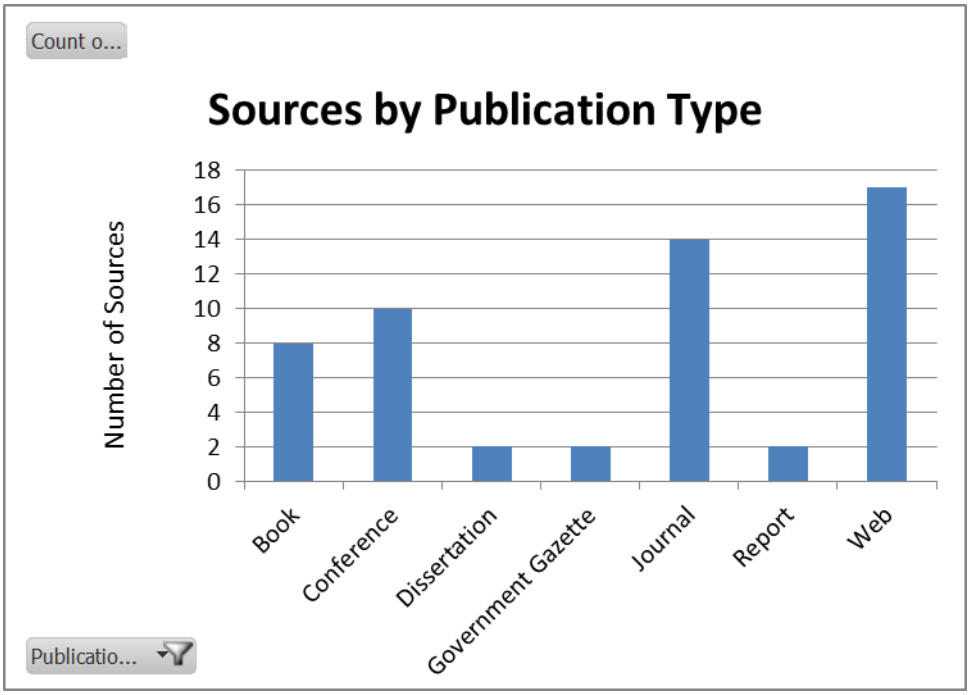

Figure 3: References by Publication Type

3.5 Research Material by Subject

In this section every information source used in the research was categorised within broad subjects addressing the main audience of the publication. Obviously the bulk of the research was based around the honeypot and various derivatives thereof including honeynets, shadow honeypots and honeytokens. Whilst alternative Ethics papers were reviewed, many were discarded due to duplication

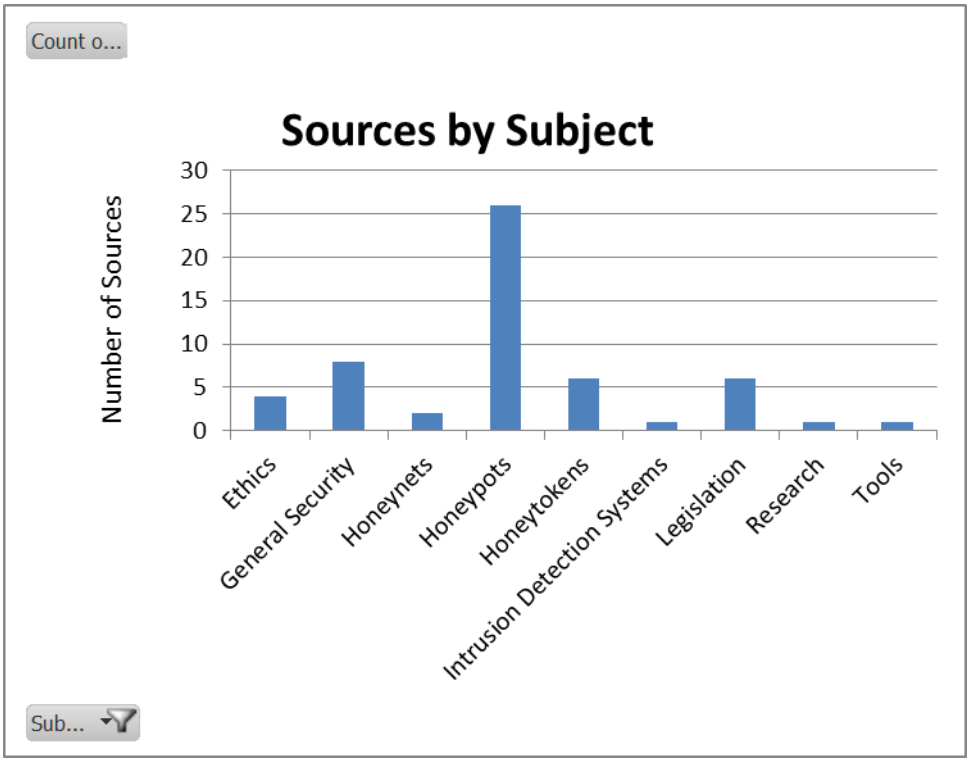

Figure 4: References by Subject

3.6 Limitations

As mentioned previously research was limited to English language publications and the majority of searches were done using Google Scholar or the internal search engines contained within the IEEE Xplore and ACM Digital Library systems. Therefore this research may be missing critical views exposed in publications released in non-English journals.

3.7 Research Design

The research was done by conducting a review of available books, journal articles and conference proceedings. Where necessary web pages were consulted in clarifying points although an attempt was made to include formal publications only to ensure that input into this research was, at least, peer reviewed.

3.8 Summary

This chapter has examined how the research contained within this research topic was conducted and presented the sources of that data categorised along a number of axes. The researcher recognises that this research has shortcomings based on the language exclusions and, perhaps search engine specificy, ranking systems or cultural bias.

Given that the output of this research is to be a checklist for the IT professional to use when deploying a honeypot in South Africa, it is believed that with the investigation into the South African legislative frameworks and the alignment of honeypot implementation practice to that done in the United States of America this checklist will stand an implementer in good stead should it be utilised.

Chapter 4: The Legal and Ethical Concerns with Honeypots

4.1 Introduction

Wherever there is surveillance the possibility exists of abuse of the systems, to this end both parties within a system interaction need to have some general guidelines to operate under. This chapter will examine the legal issues associated with the implementation of a honeypot, in particular considering at Spitzner's (2010) defined areas of Entrapment, Privacy and Liability.

Following this introduction to the legal complexities we shall examine the South African legislative framework which covers electronic transactions and the protection of personal information. Finally we will examine the ethics of implementing a honeypot revisiting the entrapment argument and discussing the case of building a better hacker and hacking tool sets.

4.2 Entrapment

'Entrapment is the conception and planning of an offense by an officer, and his procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion, or fraud of the officers.' [The accepted standard legal definition of entrapment as stated by Justice Roberts in 1932 in Sorrells vs. United States]

Entrapment as it relates to the area of honeypots refers of the baiting of a computer system to make it appear as though the security controls on it will allow access in an unauthorised manner, (Mokube and Adams, 2005). The South African definition of entrapment dovetails with the American legal definition outlined in Pelletier and Kabay (2003) where the person implementing the trap is a representative of the police force or other officer of the court.

In this regard Biggs (2013) refers to the practice, by certain film studios, of 'baiting' popular torrent sites – where illegal copies of media are made available through Peer-to-Peer networks. A film will be released onto a known piracy site and then it is monitored for activity. The way that torrent sites work is by breaking up the initial file so that only a piece of the file is downloaded from a computer and no single person is therefore responsible for transmitting the full film across the internet.

The studios performing this practice generally make use of third parties to actually monitor connections made to transmit the data and supply IP addresses and timestamps to Internet Service Providers in order to get access to personal information for the purpose of serving legal papers on the person responsible for the account logged into that IP address at that particular time. Obviously a whole range of problems exist with this approach.

From Biggs' (2013) 'ephemeral' IP address argument – meaning that IP addresses are constantly being reissued to people coming on line as the initial part disconnect, to the accused being a victim of war-driving or WiFi hijacking depending on the technology being used on the accused's premises. What this means is that the court cannot be certain that the source IP address used in downloading the data may or may not be being utilised by the purported 'owner' according to Internet Service Provider records.

Spitzner (2002) infers that the concept of entrapment does not apply to a honeypot in that definition of entrapment as outlined above almost implies coercion on the part of the honeypot owner. Given that the honeypot is by nature a passive system, this means that there can be no entrapment defence by someone being prosecuted as the system has no way of soliciting attacks from would be hackers. In order for a defendant to make a case for entrapment the system would need to, in some way – either via email or similar advertising – lure the attacker to the site.

The other issue with entrapment is that it can only be done by an officer of the court and as such, unless the authorities have specifically baited a site and lured hackers there, it cannot be used in a defence.

4.3. Privacy

Privacy as an issue with honeypots is again divided between attacker and defender. The attacker has network traffic intercepted, monitored and stored without his knowledge (if the defender has not set up the honeypot properly). Scottberg et al. (2002) maintain that intruders are not covered by privacy strictures since they have 'no legitimate accounts or privileges' on the system being accessed. In the South African context this definition may unintentionally come into conflict with the current Electronic Communication and Transactions Act (2002) legislation which states that 'An interception direction is a written direction by the designated judge on request of an applicant authorising the interception of communication' (Thornton et al., 2006, 319).

No mention is made in the Regulation of the Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 with regards to the interception of traffic in the case of a honeynet and there may be a case to be made for dismissal by the attacker if the defender has not identified the system as being monitored.

By the same token, the defender has a right to privacy, although it could be argued that implementing a deliberately flawed system in terms of security in the hopes that someone will attack it, nullifies this right to some extent. Scottberg et al. (2002) draw parallels to the setting up of a honeypot as 'encouragement activity' on the part of the defender with similar behaviour in law enforcement sting operations. Its applicability is then questioned due to the fact that the attacker needs to set out with the intent of breaking into a system, has to scan through many systems to determine which are vulnerable and then attempt to directly access the system.

Private implementations of honeypots do not suffer the same strictures as those of crime prevention or other government office installations. Both Pelletier and Kabay, (2003) and Mokube and Adams (2005) cite the Fourth Amendment issues which deals with what information the (American in this case) government can search for and seize with or without a warrant. In the private arena, the American Wiretap Act, which is somewhat analogous to the Lawful Interceptions Act in South Africa provides for a number of scenarios when information can be gathered including the Computer Trespass, Consent of a Party and Provider (System Protection) Exceptions.

4.4 Liability

Liability, according to the van der Walt (1970) has at its core the notion of fault. In the security context the practitioner may become liable if due care is not taken to protect a security system or the information stored therein, particularly if this information relates to people and makes them personally identifiable.

The defender may be liable for actions launched from the compromised system should the services in the honeypot be closely modelled on an actual system, particularly in the case of a high interaction honeypot (Spitzner, 2003). This allows the attacker to interact with all processes that would normally run on a system. In this type of high interaction system it is unclear who would be responsible for damage suffered by a third party as a result of actions taken by an attacker on launched from the defender's system.

However South African Law within the Protection of Personal Information Act (2009) states that part of the duty of someone administering the security on a system is to ensure that all relevant patches and safeguards are maintained on the system. This puts the honeypot implementer at odds with the letter of the law, in that a honeypot must be made enticing in a way that attracts attackers and this normally means that known exploits are left within the system.

Scottberg et al. (2002) draw attention to the fact that the implementer of the honeypot should perform adequate due diligence before setting up the system. This would include determining the profile of interaction – is it low or high, the available services on the system should it be compromised and the potential egress points of the system to the internet at large.

4.5 The Electronic Communications and Transactions Act (2002)

The Electronic Communications and Transaction Act of 2002 is a set of guidelines for governing electronic data interchanges. Chapter XIII of the Act deals with cybercrime and covers Sections 85 through 89. For the purposes of this research Paragraph 4 of section 86 in the Act states that:

'*A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto is guilty of an offence*'.

Thus there are clear legal guidelines as to what constitutes an illegal attempt to access a system. This means that security professionals have recourse to the law when an attacker can be positively identified as the person who breached their systems.

4.6 The Protection of Personal Information Bill (2009)

The most important item for the security professional looking to implement a honeypot, with regards to attempting to catch an intruder, within the Protection of Personal Information Bill is presented in the Chapter 2 Application Provisions section where the exclusions are detailed. Section 4 states:
'*This Act does not apply to the processing of personal information—*
(a) in the course of a purely personal or household activity;
(b) that has been de-identified to the extent that it cannot be re-identified again;

(c) by or on behalf of the State and—
(i) which involves national security, defence or public safety; or
(ii) the purpose of which is the prevention, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures,
to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information;' Protection of Personal Information Bill (2009)

Section 4, Item c(ii), indicates that the act does not apply when a crime is being committed and the researcher is attempting to investigate or prove what is happening. When combined with Section 86 of the ECT Act this would seem to make an open and shut case for the honeypot implementer being within his rights both legally and morally when installing a honeypot.

However consider the following scenario. A high interaction honeypot is used as a platform to steal credit card and personal information. One of the 8 guiding principles of the PoPI Bill is Principle 7 – Security Safeguards is Section 18 which states that:
'*(1) A responsible party must secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—*
(a) loss of, damage to or unauthorised destruction of personal information; and
(b) unlawful access to or processing of personal information.
(2) In order to give effect to subsection (1), the responsible party must take reasonable
measures to—
(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
(b) establish and maintain appropriate safeguards against the risks identified;
(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations'.

It is not difficult to see a defence lawyer making an argument that the honeypot implementer has some liability in the theft as Paragraph 2 Item d states that systems must be 'continually updated in response to new risks' which in part defeats the idea of leaving a purposefully hack-able system (the honeypot) open on the Internet for a hacker to attempt to gain access.

Ultimately the law will be tested in court and its deficiencies, or lack thereof, will be put to the test. However honeypot implementers should note this information when deciding whether to implement low or high interaction systems.

4.7 Ethical considerations

Raval (2012) describes ethics as they relate to Information Technology as a branch of general ethics which 'links the enabler Principles, Policies and Frameworks with the enabler Culture, Ethics and Behaviour. This is because the former 'should reflect the culture and ethical values of the enterprise and they should encourage the desired behaviour.' '. In this view Raval (2012) is specifically addressing Ethics as outlined in the CobiT 5 framework.

Immediately issues arise with this description in that attackers are not going to conform to an ethical value system that they have not opted into. Security professionals on the other hand may find their hands metaphorically tied by the stricture of the corporate ethical code.

Whilst most of the codes of conduct can be distilled to a central set of common tenets there are regional variations thereof that hamper the definition of frameworks that can cover the industry as a whole. The Association of Computing Machinery in their Code of Ethics and Professional Conduct (1992) states as two of its fundamental moral imperatives that one should avoid harming others and that one should be honest and trustworthy.

Although these are admirable goals they do not co-exist easily with the implementation of honeypots where the idea is to track and catch attackers by enticing them into soft looking targets (Warren and Hutchinson, 2003) which is essentially an unethical practice.

Honeypots remain a controversial topic and although they are generally seen as being a legal solution, not everyone sees then as ethical. Pelletier and Kabay (2003, 05 15), make the following statement, 'As for entrapment, although this is not a legal problem, this does not mean that the way a honeypot entices attackers is not unethical.' Their central tenet is that in the same way that it is illegal to entice someone into stealing something it could be considered illegal to instantiate a system with known weaknesses on a network or the internet in the hopes that it be attacked. Given that the former is illegal in law and by virtue of this fact would be assumed to be unethical, could the same not be said of implementing a honeypot?

The world is connected, zero day exploits are made available via dark webs almost instantaneously allowing less seasoned or experienced hackers access to the knowledge required to compromise a system. Every time a system is breached hackers, as a community, become that much more aware of attack vectors. The ethical dilemma here for the honeypot implementer is whether he is, by virtue of the fact of making a system available to hack, adding fuel to this fire and essentially allowing the exploits that were used within his honeypot to be exploited elsewhere within other corporations and

government entities around the web who may not have the same level of insight into hacking attack vectors.

In Scottberg et al (2002), the ‘best defence is a good offence’ argument is used in saying that by monitoring an attack pattern and implementing anti-measures against that particular attack vector in future organisations can better protect themselves. On its own this argument has merit however unless there is sharing of attack information between organisations this view is merely espousing the view that ‘as long as my system is better protected than the next guys, attackers will go there’, which is not a particularly ethical approach.

4.8 Summary

In this Chapter we began by introducing the legal and ethical issues associated with honeypots, particularly within the American context, where the bulk of the research found has originated.

Following this an examination of the relevant sections of the Electronic Communications and Transactions Act was conducted to determine if there were any particular legal inhibitors to implementing a honeypot in South Africa. This was followed by a review of the Protection of Personal Information Bill to determine any alignment with the data, which makes a person individually identifiable, that can or cannot be stored by the honeypot.

This Chapter shows that there is not much in the way of specific legislation, as by necessity laws of the country need to be broad but it highlights the sections of the ECT Act and the PoPI Bill which are relevant to the security professional or researcher..

The next Chapter will introduce the taxonomy, providing the framework for terms that make up the honeypot landscape.

Chapter 5: The Taxonomy

5.1 Introduction

A taxonomy is a means of classifying or codifying the terms related to a particular subject or field. In terms of this research sources for an existing taxonomy that relates to all of the technology, legal and ethical areas were not found.. Martin (2001), Spitzner (2002) and Lakhani (2003) have similar frameworks for the description of a honeypot and its various methods of deployment. Seifert et al. (2006) expanded on these earlier works with an alternative approach to the security goals of the system

Much of the research within this area has been built on these early works and classification has changed in an evolutionary rather than revolutionary fashion. These terms have been defined within this document, the bulk of the definition takes place in Chapter 2 and, therefore, only a short description will accompany each term here.

5.2 Existing Taxonomies

Seifert et al (2006) take a more system oriented view of the taxonomy with regards to its implementation and focus on factors such as Communication Interface, Distribution Appearance and Role in a multi-tier architecture. The also address ‘common’ elements of honeypots with regards to their Interaction Levels and Security Goals.

Zhang et al (2003) utilised Schneier’s (2000) base for determining the security goals of a honeypot, these being: Prevention and Detection and have split the Response goal into Reaction and Research Reaction. This taxonomy comes into conflict with other taxonomies where the Research security goal can be confused with the deployment category being defined as Production or Research systems.

In terms of interaction levels, Zhang et al. (2003) quantify only a high interaction level honeypot. Seifert et al (2006) offer both a low and high interaction system. Grudziecki et al, (2012) speak to low, high and hybrid interaction honeypots; where the hybrid system is a combination of low and high interaction systems. Lall and Vivek (2012) simplify this approach with their definition of low, medium and high interaction systems.

The security goals of the honeypot are dependent on the posture. External facing systems are generally deployed for reconnaissance purposes in order to get the maximum amount of data on how attacks are conducted from monitoring the hacker's actions during his session on the system.

Internally focussed honeypots are deployed, for the most part, to catch employees attempting to access systems for a variety of reasons. Here the focus is not so much on the information gleaned about attacks, rather it is about what systems the employees are attempting to gain access. This type of deployment mode would be categorised as deception.

If an Acceptable Usage Policy exists, there is no need for an internally focussed honeypot implementation to advertise itself for intimidation reasons as the employee has to accept and abide by the policy or face disciplinary action.

As detailed in Chapter 4, unless the honeypot has been deployed by an officer of the court, entrapment is not an issue. However practitioners need to ensure that they adhere to the Privacy Information laws within their country. As stated previously, in South Africa if the system is used to attack an external system and in that attack personal information is exposed, the security professional runs the risk of exposing himself to possible liability actions

5.3 Derivation of Taxonomy

This research has used Lall and Vivek's (2012) classification of low, medium and high interaction systems as a basis for interaction categorisation. Scottberg's et al. (2002) Deployment Mode covering Reconnaissance, Deception and Intimidation was incorporated along with Schneier's (2000) Security Goals. This gives a fairly high level taxonomy which can be understood by individuals within the IT arena and those responsible for legal and ethical compliance.

Figure 5 below illustrates these terms and incorporates the legal and ethical portions addressed by the research. Legal issues cover Entrapment, Liability and Privacy and are covered in detail in Chapter 4. Ethical issues, also covered in Chapter 4, introduced during the course of this research address the privacy and personal and personally identifiable information areas.

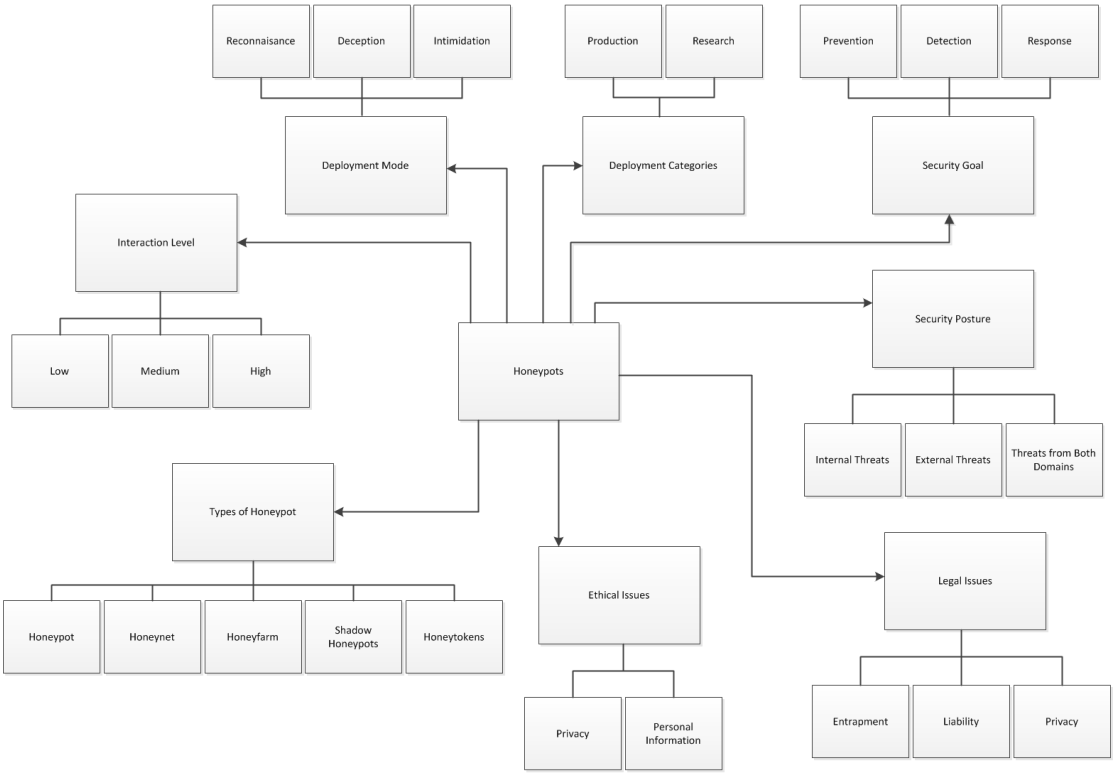

Figure 5: Honeypot Taxonomy

5.4 Summary

In this chapter the categories commonly used within the honeypot community have been gathered into a taxonomy. The introduction of legal and ethical categories into the taxonomy was done as these areas were not encountered during the research and the derived taxonomy. The taxonomy is based upon work done by Seifert (2006), Zhang (2003), Schneier (2000) and Scottberg (2002) underpinned by Spitzner's (2002) seminal book: Honeypots: Tracking Hackers.

The next chapter details the checklist that has been formulated based upon this literature review.

Chapter 6: Checklist

6.1 Introduction

This chapter provides a set of practical that a security professional, particularly one without experience in the field, should address when implementing a honeypot. This set of steps, based on the above research will guide a practitioner in the implementation of a honeypot in a manner that takes cognisance of South African law and highlights possible ethical issues.

Whether in a production or research environment the implementer should consider the following questions:

- Do you have an existing threat that you are concerned about or need to address?
- Can this threat be addressed by the implementation of an IPS or IDS?
- Is your threat internal or external in origin?
- If Internal – do you have a formalized IT Policy that is made available to users?
- If External – have you included a disclaimer on your external interfaces stating that activity on the system may be recorded?
- Have you contacted the Authorities with regards to this threat?
- Have you specified which data is being captured and how it relates to the Protection of Personal Information Bill?

As an output of the research a series of practical steps emerged that could be understood by both the security professional and the legal or ethical advisor involved with the deployment. The steps form a high level process that can be easily followed when a honeypot is implemented. The following flow chart (Figure 6) diagrammatically illustrates this process.

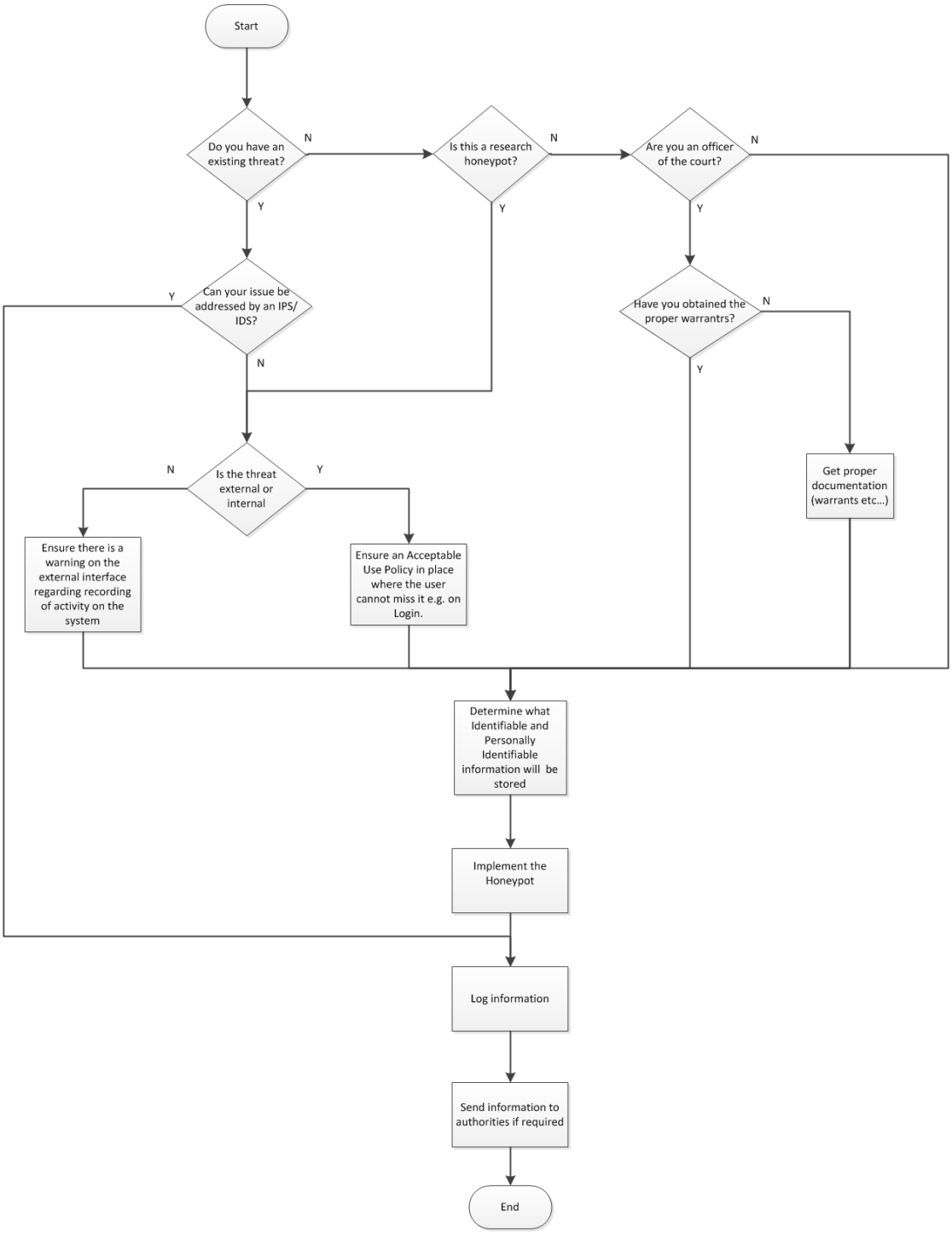

Figure 6: Flowchart for Implementing a Honeypot

The questions outlined above are now expanded in the sections below.:

6.2 The Checklist

6.2.1 Do you have an existing threat that you are concerned about or need to research?

If the answer to this question is no, consider why you are implementing a honeypot. If no specific research motive exists and there is no obvious threat, the implementation of a honeypot is generally being done for interest's sake. If this is the case consider the implementation of a low interaction honeypot.

In this case, if this system is compromised then the chances of the attacker reaching and misappropriating other systems resources is reduced and with this the chance of being implicated in any liability action that may arise from the incursion.

6.2.2 Can this threat be addressed by the implementation of an IDS or IPS?

Setting up and monitoring a honeypot can be time intensive. With the focus on returns within the corporate environment the emphasis is generally on systems that are updated automatically, can be deployed in an appliance type fashion and come with a service level agreement.

In these situations a commercially available Intrusion Detection System or Intrusion Prevention System may be preferable. For research, where funds may be limited there are many shareware and freeware honeypot implementations. A good place to start in this regard would be www.honeynet.org, the organisation founded by Lance Spitzner.

6.2.3 Is your threat external or internal in origin?

Determining whether your threat is external or internal has an impact on the next couple of questions. An internal threat can be dealt with through Human Resources when the perpetrator is caught. An external threat could involve

the authorities depending upon the nature of the breach and the actions taken by the attacker during the course of the incursion.

6.2.4 If internal – do you have a formalised IT Policy guideline that is made available to users?

Any internal threat can be responded to under the governance of the Organisation's Acceptable Usage Policy. Within this policy the Organisation should stipulate what constitutes proper use of the IT systems and which actions will attract sanctions.

Appendix B contains example text from an Acceptable Use Policy document, in this case it is from the Dimension Data staff policy governing interactions with computer systems. An acceptable use policy should be placed in a position where the user has to click on it to proceed with normal system usage.

A good place to implement the policy is during the login process where a pop up window can detail the policy, or a link to the policy and inform the user that by proceeding they agree with the provisions of the policy.

6.2.5 Have you contacted the authorities in regards to this threat?

The Internet Service Provider's Association of South Africa (2013) released their 'Reporting Cybercrime' advisory in April of this year. They detail that there is no set process for reporting a crime committed within the IT environment and suggested the following process contained within the advisory which is attached in Appendix A.

The South African Police Service Directorate for Priority Crime Investigation is tasked with the investigation of cybercrime within the country's borders (http://www.saps.gov.za/_dynamicModules/internetsite/OPbuildBP3.asp?myURL=132). However as they are also tasked with the investigation of serious crime, organised crime and corruption cases, with the currently stated 381 SAPS members and 158 civilian specialists, it should be noted that unless the actions committed by the attacker have led to serious financial loss or have compromised national security, any trespass on networks is likely to be prioritised accordingly.

6.2.6 If external – have you included a disclaimer on your external interface stating that activity on the web site may be recorded and monitored?

One deployment mode of honeypots mentioned in Chapter 2 is that of Intimidation. In this mode you make an attacker aware of the fact that his actions are being monitored and recorded. For the majority of script kiddies and 'white hat' hackers this warning will be enough to try their luck elsewhere. State sponsored and organised crime cyber-espionage is on the increase.

Freed (2012) gives figures of attacks against American targets increasing by 129% from Central and South Asia, by 75% from the Near and Far East and by 60% from Europe and Eurasia from 2010 to 2011. This type of attack will in all probability be multi-pronged and incorporated both technological and social vectors. If you suspect that your organisation may be being subjected

to this form of attack it would be best to inform the Directorate of Priority Crime Investigations as soon as possible.

6..2.7 Have you specified what data is being captured and how it relates to the Protection of Personal Information Bill?

Section 3.8 highlighted the portions of the Protection of Personal Information Bill of 2009 which are pertinent to the implementation of a honeypot. In order to avoid compromising yourself and / or your organisation Principle 7 of the Bill should be noted and the data gathered regarding a system incursion should, as the Bill states, secured by taking 'appropriate, reasonable technical and organisational measures' to prevent the data being accessed by another third party, be they internal or external.

6.3 Conclusion

The framework outlined above provides an initial departure point for security professionals wishing to deploy a honeypot in a legal and ethical manner within South Africa. Whilst the focus of the research was on South Africa, issues such as Personal Information legislation have been highlighted. .Use of this checklist should be done outside of South Africa in conjunction with a legal team to ensure that the relevant Privacy and Monitoring laws are followed.

This check list should be considered a work in progress as legislation is changing to adapt to a more interconnected society, as such the check list will need to be kept up to date or it will risk becoming more of an inhibitor to good security practice than a promoter thereof.

Chapter 7: Conclusion

7.1 Introduction

This section reiterates the objectives of the study and determines if these were met. It details the main contribution that the research intends to deliver and then looks at the implications for the implementation of honeypots in South Africa by Security Professionals. Finally, future research recommendations within this topic are outlined.

7.2. Accomplishing the Objectives of the Study

The objectives of this study were to examine the currently extant legal and ethical implications involved with the deployment of a honeypot within a networked environment and to apply globally sourced best practice within a South African legislative framework. In particular the study examined the Electronic Communications and Transactions Act and the Protection of Personal Information Bill to determine any inhibitors to honeypot installation. This was done to see if there were any regional differentiators with regards to the subject matter and deriving a setup checklist for the South African IT professional implementing a honeypot.

7.3 Main Contribution

The main contribution of this research is the creation of the Checklist to be used by security professionals when they are unsure of, or naïve about, implementing a honeypot. It is envisioned that this checklist will provide some direction with regards to ensuring that, as far as possible the honeypot is implemented for ethical reasons and an a legal manner.

7.4 Implications for Practice

The implications for security researchers within South Africa of this research is that it makes them aware of the possible defence strategies that could be utilised at trial when systems that they have implemented to study hacking are used as a springboard for hackers to access external systems.

Security professionals will need to ensure that their honeypots are either patched to current levels, therefore only capturing zero day exploits, or will need to ensure that once an attacker penetrates their honeypot, that there is no way that it can be used to launch an attack on an external system.

7.5 Future Research

Particular frameworks for the ethical and legal implementations of honeypots and honeynets under different jurisdictions and legal systems need to be developed. These frameworks will not only protect the researchers and professional IT staff who are doing work in the field but also apprise would be attackers of their legal status with regards to the attempted access of systems not under their control.

The next phase of research on this topic will need to incorporate a survey to determine the installation base of operational production and research honeypots in South Africa. A questionnaire based on the checklist in Chapter 6 would be sent to educational, governmental and private sector security practitioners to gauge the level of awareness of legal and ethical issues involving the deployment of honeypots. This research would provide insight as to whether training is required in the field for security professionals in this regard.

The taxonomy outlined in Chapter 5 will need to be enhanced to cover any new legislation promulgated by government and any technologies that impact

upon this field of research. The ethics section needs to be expanded to incorporate best practice from around the world which may be based in foreign languages and were therefore not covered during the researching of the subject.

A framework with the common elements of these solutions can be consolidated to provide a neutral set of ground rules, or checklist, covering the ethical and legal aspects of honeypot use. The checklist put forward within this research can be implemented as a guideline by those professionals wishing to implement honeypots in a responsible manner.

7.6 Conclusion

Security research is on-going as technology within the IT field changes rapidly. Research such as this and the associated checklist output need to be revisited on an on-going basis to determine whether they are still germane to the topic. It is hoped that with the research of honeypots tied to the investigation of the current legislation, a platform has been provided for both technical and legal researchers to conduct future studies.

References

Advisory on Reporting Cybercrime. (2013, April 1). Retrieved July 11, 2013, from CyberCrime: http://cybercrime.org.za/docs/Advisory_on_Reporting_Cybercrimes_April_2013.pdf

Abbasi, F. H. (2013). *An exemplar-based learning approach for detection and classification of malicious network streams in honeynets.* Chichester: Wiley.

Anagnostakis, K., Sidiroglou, S., Akritidis, P., Polychronakis, M., Keromytis, A., & Markatos, E. (2010, September). Shadow Honeypots. *International Journal of Computer and Network Security, 2*(9), 1-16.

Association of Computing Machinery. (1992, October 16). *ACM Code of Ethics and Professional Conduct* . Retrieved May 25, 2012, from http://www.acm.org/about/code-of-ethics

Baker, D. B. (1996). Fortresses built upon sand. *Proceedings of the 1996 workshop on New security paradigms* (pp. 148-153). Lake Arrowhead: ACM.

Bhumika, L., & Sharma, V. (2012, 06). Use of Honeypots to Increase Awareness regarding Network Security. *International Journal of Recent Technology and Engineering, 1*(2), 171-175.

Biggs, J. (2013, 03 25). *Bait Car: How Hollywood Has Found A New Way To Make Money*. Retrieved 05 12, 2013, from TechCrunch: http://techcrunch.com/2013/03/25/how-copyright-trolls-run-bait-car-operations-to-grab-pirates/

Briffaut, J., Lalande, J.-F., & Toinard, C. (2009). Security and results of a large-scale high-interaction honeypot. *Journal of Computers 4.5 (2009)*, 395-404.

Cenys, A. R. (2005). Implementation of Honeytoken Module in DBMS Oracle 9ir2 Enterprise Edition for Internal Malicious Activity Detection. *IEEE Computer Society's TC on Security and Privacy*.

CERT Poland, Grudzieki, T., Jacewicz, P., Juszczyk, L., Kijewski, P., & Pawlinski, P. (2012). *Proactive Detection of Security Incidents:*

Honeypots. Heraklion: European Network and Information Security Agency.

Cowan, C., Hinton, H., Pu, C., & Walpole, J. (2000). The cracker patch choice: An analysis of post hoc security techniques. . *Proceedings of the 19th National Information Systems Security Conference (NISSC 2000)*, (pp. 16-19). Baltimore.

Danielson, S. (2004). Work in Progress - Ethics in the Workplace. *Frontiers in Education*, (pp. S3E-6). Savannah.

Edmead, M. (2002, 08). *Using honeypots to fake out an attacker*. Retrieved 06 01, 2013, from TechTarget: http://searchenterprisedesktop.techtarget.com/tip/Using-honeypots-to-fake-out-an-attacker

Eskin, E., Arnold, A., Prerau, M., Portnoy, L., & Stolfo, S. (2002). A geometric framework for unsupervised anomaly detection. In D. Barbara, & S. Jajodia, *Applications of Data Mining in Computer Security* (pp. 77-99). Dordrecht: Kluwer.

Freed, A. M. (2012, 12 20). *Defense Report Reveals Spike in State Sponsored Cyber Espionage* . Retrieved 03 24, 2013, from SecurityBistro.

Gazette, G. (2002, 08 02). *Electronic Communications and Transactions Act, 2002*. Retrieved 06 01, 2012, from http://www.info.gov.za/view/DownloadFileAction?id=68060

Gazette, G. (2009, 04 01). *Protection of Personal Information Bill*. Retrieved 06 01, 2012, from http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionofPersonalInformation.pdf

Giakouminakis, A., Loder, C., & Li, R. (2010). *Patent No. US20120174228 A1.* United States.

Gibbens, M., & Rajendram, H. V. (2012, 12 01). *Computer Science Department*. Retrieved 10 15, 2013, from University of Arizona: http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/

References

Heady, R., Luger, G., Maccabe, A., & Servilla, M. (1990). *The architecture of a network-level intrusion detection system.* Department of Computer Science, College of Engineering, University of New Mexico.

Hoepers, C., Steding-Jessen, K., & Montes, A. (2003). Honeynets Applied to the CSIRT Scenario. *Proceedings of the 15th Annual Computer Security Incident Handling Conference.*

Jones, J. K., & Romney, G. W. (2004). Honeynets: an educational resource for IT security. *Proceedings of the 5th conference on Information technology education, ACM*, (pp. 24-28). Salt Lake City.

Joshi, R., & Sardana, A. (2011). *Honeypots: A New Paradigm to Information Security.* Enfield: Science Publishers.

Kalogridis, G. (2011). *Preemptive mobile code protection using spy agents.* London: Dissertation, University of London.

Kassner, M. (2011, 07 29). *Myth or not: Most security breaches originate internally*. Retrieved 05 11, 2013, from TechRepublic: http://www.techrepublic.com/blog/it-security/myth-or-not-most-security-breaches-originate-internally/

Lakhani, A. D. (2003). *Deception Techniques Using Honeypots. (Master's thesis).* London: Royal Holloway, University of London.

Liability. (n.d.). Retrieved 10 20, 2013, from The Free Dictionary: http://legal-dictionary.thefreedictionary.com/liability

Mairh, A., Barik, D., Verma, K., & Jena, D. (2011). Honeypot in network security: a survey. *Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM*, (pp. 600-605). Odisha, India.

Martin, W. W. (2001, May 25). *Honeypots and Honeynets: Security through deception.* Retrieved 10 20, 2013, from SANS Institute InfoSec Reading Room: http://www.sans.org/reading-room/whitepapers/attacking/honey-pots-honey-nets-security-deception-41

McRae, C., & Vaughn, R. (2007, January). Phighting the Phisher: Using Web Bugs and Honeytokens to Investigate the Source of Phishing Attacks.

References

Proceedings of the Fortieth Annual Hawaii International Conference on System Sciences, *40*, p. 270c. Maui.

Mohammadzadeh, H., Mansoori, M., & Honarbakhsh, R. (2013). Taxonomy of Hybrid Honeypots. *Proceedings of the Eleventh Australasian Information Security Conference* (pp. 59-66). Adelaide: CRPIT.

Mokube, I., & Adams, M. (2005, Jun). Honeypots:Concepts, Approaches and Challenges. *Proceedings of the 45th annual SouthEast Regional Conference of the ACM*, *4*, pp. 321-326. Winston-Salem.

Oates, B. J. (2005). *Researching information systems and computing.* Los Angeles: Sage.

Pelletier, R., & Kabay, M. (2003, 05 12). *Honeypots, Part 1*. Retrieved 05 14, 2012, from http://www.networkworld.com/newsletters/2003/0512sec1.html

Pelletier, R., & Kabay, M. (2003, 05 15). *Honeypots, Part 2*. Retrieved 05 14, 2012, from http://www.networkworld.com/newsletters/2003/0512sec2.html

Pelletier, R., & Kabay, M. (2003, 05 20). *Honeypots, Part 3*. Retrieved 05 14, 2012, from http://www.networkworld.com/newsletters/2003/0519sec1.html

Pelletier, R., & Kabay, M. (2003, 05 22). *Honeypots, Part 4*. Retrieved 05 14, 2012, from http://www.networkworld.com/newsletters/2003/0519sec2.html

Peter, E., & Schiller, T. (n.d.). *A Practical Guide to Honeypots*. Retrieved 05 07, 2012, from www.cs.wustl.edu/~jain/cse571-09/ftp/honey.pdf

Pouget, F., Dacier, M., & Debar, H. (2003). White paper: honeypot, honeynet, honeytoken: terminological issues. *Rapport technique EURECOM*, 1275.

Raval, V. (2012). Ethics in Cobit 5. *ISACA Journal Volume 5*, 9-11.

Sarabadani, E. (2012, 01 26). *What are Honeypots ?!!* Retrieved 10 20, 2013, from Security Dreams May Come True...: http://esihere.wordpress.com/2012/01/26/what-are-honeypots/

Schneier, B. (2000). *Secrets and Lies.* New York: John Wiley and Sones.

References

Scottberg, B., Yurcik, W., & Doss, D. (2002). Internet honeypots: Protection or entrapment? *Technology and Society International Symposium, (ISTAS'02)* , 387-391.

Seifert, C., Welch, I., & Komisarczuk, P. (2006). *Taxonomy of honeypots.* Wellington: Victoria University of Wellington.

Siles, R. (2007). *HoneySpot: The Wireless Honeypot*. Retrieved 05 17, 2012, from http://flambers.com/papers/honeywifi.pdf

Spitzner, L. (2002). *Honeypots: Tracking Hackers.* Reading: Addison Wesley.

Spitzner, L. (2003, 07 17). *Honeytokens: The Other Honeypot*. Retrieved 04 18, 2012, from http://www.securityfocus.com/infocus/1713

Spitzner, L. (2010, 11 02). *Honeypots: Are They Illegal?* Retrieved 04 28, 2012, from http://www.symantec.com/connect/articles/honeypots-are-they-illegal

Stoll, C. (1990). *The cuckoo's egg : tracking a spy through the maze of computer espionage.* New York: Bantan Doubleday Dell Publishing Group Inc.

Thakar, U., Sudarshan, V., & Ramani, A. K. (2005). HoneyAnalyzer–analysis and extraction of intrusion detection patterns & signatures using honeypot. *Proceedings of the Second International Conference on Innovations in Information Technology.* Thakar, Urjita, Sudarshan Varma, and A. K. Ramani.

Thornton, L., Carrim, Y., Mtshaulana, P., & Reyburn, P. (Eds.). (2006). *Telecommunications Law in South Africa* (1 ed.). Johannesburg: STE Publishers.

van der Walt, J. C. (1970). A Few Thoughts on the Basis of Delictual Liability. *The Comparative and International Law Journal of Southern Africa*, 1-17.

Warren, M., & Hutchinson, W. (2003, May). Australian Hackers and Ethics. *Australian Journal of Information Systems, 10*(2), 151-156.

White, J. &. (2009). Implementing PII honeytokens to mitigate against the threat of malicious insiders. *Intelligence and Security Informatics ISI'09*, 233-233.

References

White, J. (2010). Creating personally identifiable honeytokens. *Innovations and Advances in Computer Sciences and Engineering*, 227-232.

Whitman, M. E. (2003, August). Enemy at the gate: threats to information security. *Communications of the ACM , 46*(8), 91-95.

Zhang, F., Zhou, S., Qin, Z., & Liu, J. (2003). Honeypot: a Supplemented Active Defense System for Network Security. *4th International Conference on Parallel and Distributed Computing Applications and Technologies* (pp. 231-235). Chengdu: IEEE.

Appendix A

Internet Service Provider's Association Advisory

Title	Reporting cybercrimes
Last updated	April 2013
Applies	to All members
Source	Criminal law, especially Chapter 13 of Electronic Communications and Transactions Act 25 of 2002
Note	This advisory is intended to provide guidance on lodging criminal complaints with SAPS and attempting to ensure that these are properly taken up and investigated. ISPA obviously cannot vouch for SAPS' acts and failures to act.

Introduction

ISPA is receiving a growing number of queries from members and consumers on the correct process to follow when reporting a cybercrime. This Advisory is intended to provide simple advice on lodging a criminal complaint where you or your client is the victim of a cybercrime.

Section 86 of the Electronic Communications and Transactions Act 25 of 2002 ('the ECT Act') sets out criminal provisions relating to unlawful access to or interference with data. Crimes of this nature are often encountered by ISPA members, both directly and indirectly through their clients. Members providing voice services and their subscribers are also frequently the target of various kinds of fraud.

Suggested process

There is no set process: the advice below is based on ISPA's consultation with senior SAPS personnel.

1. Draft as short and as simple an affidavit as possible which sets out why you believe a criminal act has taken place (you may want to obtain legal assistance to do this). The affidavit should:

1.1. Set out the identity and contact details of the complainant;

1.2. If available, set out the identity and contact details of the alleged perpetrator;

1.3. Set out the facts which led to the complaint being lodged and refer to or incorporate any available evidence such as IP addresses and log files;

1.4.Set out the sections of the criminal law or ECT Act which have been breached. The full text of Chapter 13 of the ECT Act which deals with cybercrime is contained in Annexure A to this Advisory.

1.5.Make a clear statement that you wish the matter to be investigated further and to be kept informed of process.

2. Lodge this affidavit with your local police station. Be patient and polite at all times. Due to their workload and priorities the desk officer may not want to receive your complaint: be firmly insistent and ask to escalate the matter internally.

3. Ensure that you obtain a reference or CAS number. This is critical in allowing you to follow the matter up.

4. According to internal SAPS procedure, your complaint should be referred to a duty detective within 24 hours. If possible obtain the name and contact details of this detective, either when lodging the complaint or when following up at a later time.

5. Request that the complaint be escalated to the SAPS cybercrime division as soon as possible. Typically the duty detective should recognise that the he

or she is not able to investigate the matter and refer it to the cybercrime division.

6. You will need to accept that it is up to you to follow-up and create pressure for the matter to be handled professionally – it is not going to be sufficient to go through the motions of lodging a complaint without actively pursuing the matter.

7. If, despite your best efforts, you are not able to obtain the kind of progress you are looking for, you may choose to consult with a lawyer or send mail to regulatory@ispa.org.za and we will see if we can help with escalation.

Conclusion

ISPA is aware that this process can be difficult given the differing priorities of SAPS and the lack of specific training on cybercrime issues. Nevertheless, the more complaints that are lodged and pursued, the easier the process should become.

Over the past few years there have been an increasing number of convictions in South African courts for cybercrimes and that there are some extremely competent SAPS personnel involved in detecting and prosecuting cybercrimes. There is also a process under way to increase the penalties which may be imposed.

Members are encouraged to provide feedback to regulatory@ispa.org.za on their experiences in reporting cybercrimes so that this advice can be improved over time. ISPA will also engage further with SAPS to try and streamline the process.

Version history

Date	Document Version	Revisions
	1.0	

Appendix B

Acceptable Use Policy

Any organisation employing knowledge or information workers should deploy an Acceptable Usage Policy. Amongst other regulations the policy should define sanctions for offences and cover the act of trespassing on non-authorised systems.

Sample text for an acceptable use policy should be along the lines of the following example implemented by a large Information Technology organisation in South Africa:

'*Certain actions identified as generally unacceptable, may be required as part of an employee's approved job function and at management discretion, will be deemed acceptable. In such cases management authorisation must be in a written or electronic format. General conduct is underpinned by more specific requirements as detailed further in this policy document. Generally acceptable conduct is characterised as follows:*

1. Employees shall not access computers, software, information or any network / network resource without the proper authorisation, regardless of who owns the resource or information.

2. Employees shall not transmit, store, process, distribute, use or view any information considered abusive, pornographic, distasteful, threatening, libellous, hateful or in contravention of local, common law, state, national or international laws…' – Dimension Data Acceptable Use Policy v12 (January, 2011)

Appendix C

Sample Banner

The following information should be displayed on a banner when the system is accessed from an external address on commonly used ports:

- The system is private property
- The system makes use of auditing controls to monitor usage
- By accessing the system the user agrees to this usage information being turned over to the authorities to be used in any civil, criminal or arbitration process
- By access the system the user agrees to the laws of South Africa being used as a basis in any legal proceedings

In this way the user is made aware that he is being monitored and that essentially he is accepting the Cyber equivalent of being read his Miranda Rights.

An example of this type of banner, based on Spitzner (2002, Figure 15-1) is shown below:

PLEASE READ BEFORE ACCESSING THIS SYSTEM

By using this system and its resources and communication links you consent to having your activity monitored, recorded and passed on to third parties in the event of any disputes arising from your use of the system. Furthermore you agree that any disputes arising from your access shall be governed by the appropriate South African Law