

Managing security attacks and network intrusions for better network performance in Zimbabwe.

M. Velempini

mvelempini@nust.ac.zw

National University of Science and Technology, Zimbabwe

Abstract

Organizations are ill quipped to deal with intrusions, and revenue is lost unnecessarily on expensive security tools. Planning and prevention of security attacks coupled with secure and stable operating systems is the best line of defense. Unfortunately crisis management is the order of the day. The most unfortunate part is the level of security expertise available in the country. There is need to train more computer scientists with a strong bias in computer security. Of note is the relation between network design, network performance and the availability of security experts. The three parameters are positively correlated. To this end specialized security courses coupled with planning and good network design could be an answer to poor network performance and to countless security breaches unleashed through design security holes that are created by network designers unknowingly.

Keywords. Security, Intrusion, Network design, Network Performance, Security Experts, Network Attack.

1.0 Introduction

Institutional and corporate networks are normally compromised by intrusions, security attacks and a host of vulnerabilities. Institutions have to re-engineer their operations and have an in-depth understanding of the operations of network security attackers for them to carefully plan their networks. Most organizations are losing millions of dollars through fix tools, patches, and anti virus software, for attacks that can easily be dealt with, using relatively cheaper means or free tools. Network security is a concerted effort to prevent attackers from striking, if they do strike, the damage should be kept at its very minimum level. The effects of successful intrusions and attacks should be minimized all the time and the damage should be contained.

It is hoped that the research is going to open doors for a wide ranging and interesting security research at various levels, leading to novelty, knowledge accumulation and dissemination in the area of network security, at the same time generating a lot of interest in area of network security leading to the development of local expertise.

The research will assist a number of corporate organizations and tertiary institutions such as National University of Science and technology (NUST) to put into place good and sound security measures that will greatly improve network performance through the use of best practices and security standards. The research will help organizations to

adequately plan for attacks well before they strike at the same time saving money through the use of cost effective means. Security budgets can also be streamlined with organizations going for cheaper and long lasting security solutions. The findings of the research can also be used by NUST in a bid to service the community, an embodiment of the university's mission. IT security experts in the country are very few, and this research seeks to encourage the development of this expertise.

The major problem with a number of organizations is ill preparedness for security attacks as they do not anticipate and plan for them until they are hit. With crisis management organizations are losing their hard earned cash at the same time opening themselves to more future intrusions and security attacks. It is also unfortunate that the legal system in the country does not give room for suing and claiming compensation for damages as a result of intrusions. For example the United State of America has such legal instruments that have been successfully used by Microsoft to claim for damages worth US\$7 million from a self Professed Spam King (2005). With such legal instruments, the ability to trace back intrusions to source becomes critical and may lead to reduction of intrusion incidents. Daring attackers risk to be caught and fined heavily, and they are likely to avoid monitored sites and computer networks. Following their anti Spam battle victory, Microsoft hopes that their victory will scare a number of would-be attackers. Unfortunately a number of organizations are not victims of security attacks, but are their own enemies. They tend to ignore basic security standards such as drafting and implementing usage and network security policies and by coming up with a number of security awareness programs design to raise awareness among systems users (Stanford Students, 2002). Adams and M.A. Sasse (2004) seem to be providing the foundation to the Stanford University student research on user involvement in drafting security policies. They argue that users do sometimes compromise the security of the system unknowingly. They propose that users should be involved in every aspect of security so that they become more informed. **Users lack security knowledge and motivation, the aspects that has to be tackled by computer security officers.** In addition to motivation and security awareness, tools such as password cracker programs should be used to enable users to be more security conscious and be in positions to identify secure tools and approaches. However this papers looks at security issues and parameters pertinent to

corporate organizations in Zimbabwe. Computer security is a must for all organizations big or small.

1.1 Related Work

Karp (2003) argues that there should be a separation between authentication and authorization in the access and use of computer resources and security features should be implemented at process level instead at the level of a user in attempt to minimize the effects of successful attacks. According to Karp a password should not be used for both authentication and authorization. Authorization can be done at lower levels and should be applied on every task or program where an authorization key has to be supplied before execution. An Operation Systems (OS) is being developed at Johns Hopkins University that implements this concept. The OS is better known as the Extremely Reliable Operating System (EROS) (2003). For Internet purposes an equally reliable web browser project is being developed by the DARPA (2003). On the other hand Berghel (2004) argues that keeping sockets closed all the time can prevent most attacks, closing ports is a standard security policy that dictates closing of all vulnerable ports to all traffic at firewall, or in the Operating System if no firewall is present. Unfortunately a number of companies have a tendency of closing all the ports even those, which are not of interest to hackers. This tendency coupled with IP address blocking tends to affect the performance of the network adversely. The best solution is to block only known undesirable IP addresses and to close only vulnerable ports. Port management is a very important tool that can be effectively used to limit the activities of hackers. Internal port scanners can be installments in attempt to improve the security of ports.

According to Berghe firewalls are vulnerable at the same time too slow, hence they tend to slow down the network. He argues that an outbound router must be installed to protect susceptible firewalls. A router may in turn be protected using network intrusion detection systems. Berghe proposes a seven-layer defense system applied on the server and client machines. This approach is the missing link in network design with a number of organizations. Organizations tend to put more emphasis on the defense of the server ignoring the client machines that are likely to compromise the security of the server

machine, at the same time creating a number of security holes in the network such as the establishment of a number of exit points.

Bayrak and Davis (2003) suggest that open source development is the answer to all our security concerns, a development initiatives dominated by “dedicated hackers”, hackers who are not wrong doers or outlaws, but a group of very passionate developers who attack their work as a team so as to identify holes in their software tools thereafter they close them to better secure the system. Bayrak & Davis (2003) say, “Torvalds was able to persuade thousands of top notch developers from around the world to collaborate on his project. Through chat rooms and news groups he was able to recruit the hacker masses. No one could question the cumulative intellect of the project, ...” (p. 99). They refer to Linux operating system as a hacker’s operating system. The selling point of Linux is that it is developed by a number of developers who have hacking expertise who hack into their own system to identify security holes and quickly closing them and distributing to the whole community an updated and more secure version for free. The operating system is available for free and offers enormous amount of help around the clock for free (Phillip & Bob, 2004). The graphical picture of how the Linux community or movement operates is illustrated by how Andrea Barisani, Mike Warfield, Andrew "Tridge" Tridgell & Martin Pool collaborated to solve a rsync attack in the University of Trieste's Gentoo Linux server (Phillip & Bob, 2004)].

T.D. Maswera (2003) did conduct a study on the prevalence of computer viruses in Zimbabwe. The results of the survey are very interesting more so to this study. It clearly shows that about 80% of companies in Zimbabwe are having hard times dealing with viruses for various reasons despite having an anti virus software. The most common source of viruses is secondary, removable storage media such as floppy diskettes. One wonders whether it is not easy to deal with the spread of viruses, since they are spread through physical means and to systems that are protected using up to date anti virus software. If users of a given network are security conscious, incidence of viruses will be greatly reduced. Raising awareness among users could be a solution to this problem. Unfortunately of late files are moved electronically leaving Institutions more vulnerable than they were during the floppy diskette era. This is a cause of concerns in terms of

computer security and does point to a number of problems this study seeks to highlight at the same time suggesting solutions to given problems. The most obvious questions are: Whether the country is aware of security threats, whether it does have the expertise, experience and adequate manpower to deal with computer security threats.

1.2 Research Design.

Corporate and institutional organizations such as NUST were used as case studies. NUST was used as a key organization for this research. The researcher worked closely with the university's ICTs department and a few international organizations were contacted for best practices, standards and comparison. Opinions of well-established local and international network security researchers were sought to verify collected primary data. Computer security journals were referenced and used in the research. Primary data was collected through interviews and questionnaires. The researcher is also researching on open source operating systems, Linux and other less vulnerable systems. Linux is an operating system, which NUST wants to use in the future as its network backbone.

A sample size of fifty ICT personnel was targeted for data collection from various corporations. Some questionnaires were sent to non-ICT personnel for managerial viewpoint. Five non-ICT respondents were interviewed and were given a chance to discuss the data collection instrument. Four of them expressed satisfaction with the instruments and its relevance. Of the fifty questionnaires sent to IT personnel 25 were sent in hard copy form, and the rest were sent electronically after some of the responses of the first batch (hard copies) have been received. This was done deliberate since the instrument was never piloted. This might have affected the first batch but from the analyses, the results of the earlier batch are consistent with the results of the later batch were some form of interaction with respondents was made possible through the use of email for purposes of clarifying or explaining certain elements of the instruments. By and large data collected through these instruments will be used to draft a more specific instrument for the research to be carried out as a follow up to the results of this paper.

1.3 Research Findings

Gathered data was recorded and analyzed with the aid of bar charts, line graphs and scatter graphs, using relative frequency. On average there was a fifty percent response

rate. The objective was to find out whether there were interdependences or possible correlation between the variables being analyzed. The major parameters were as follows: Network performance, availability of security personnel, level of security awareness in the country including the number of security personnel, the availability of patches and the ability to track back intrusions and the ability to prosecute. The performance of the network was thought to be dependent on the parameters listed above. The following sections discuss in detail the variables under consideration.

A number of respondents indicated that they were able to source security patches in time to mitigate losses. They cited the Internet as the source of patches that can be downloaded and to updates they get from anti virus software sites such as Metcalfe and Symmetric. Respondents do source and use security patches oblivious of possible dangers posed by some patches. Patches can be sources of intrusion and vulnerability, concerns attested by Lauren Weinstein (2005), who argues that patches and upgrades can be sources of insecurity and should be treated with extra care.

However, forty five percent of the respondents have never managed to trace back to source security attacks a parameter that was regarded highly in this paper with the view of blocking offensive sites, and used to sue, and prosecute attackers. Knowing the identity of an attacker makes it possible for any retribution or recourse to be undertaken. Unfortunately the identity of an attacker is usually unknown, especial with the target population considered by this paper implying the country has a handicap in this regard. To make matters worse, there is no piece of legislation that empowers organizations that have been attacked to seek recourse in a court of law.

The paper also established that a number of companies do not have security personnel and the level of security in the country is not impressive in that regard. A few companies who have indicated that they have engaged computer security experts, were referring to the National University of Science and Technology graduates who take a fourth year one semester computer security course in partial fulfillment of their degree program. This is a theoretical course, a drop in the ocean. However it does introduce students to the fundamentals of computer security though it falls far below the expectations of the computer security industry. It should also be noted that computer security courses are not that popular with Zimbabwean tertiary institutions. On the other hand the industry is not

helping out by offering internship programmes in computer security. This explains the low level of security in the country. The correlation chart in figure 1.3 shows that there are few security personnel, at a number of organizations which translates to a very low level of security in the country implying that when companies start hiring and training security personnel the approach will definitely have a positive impact on the outlook.

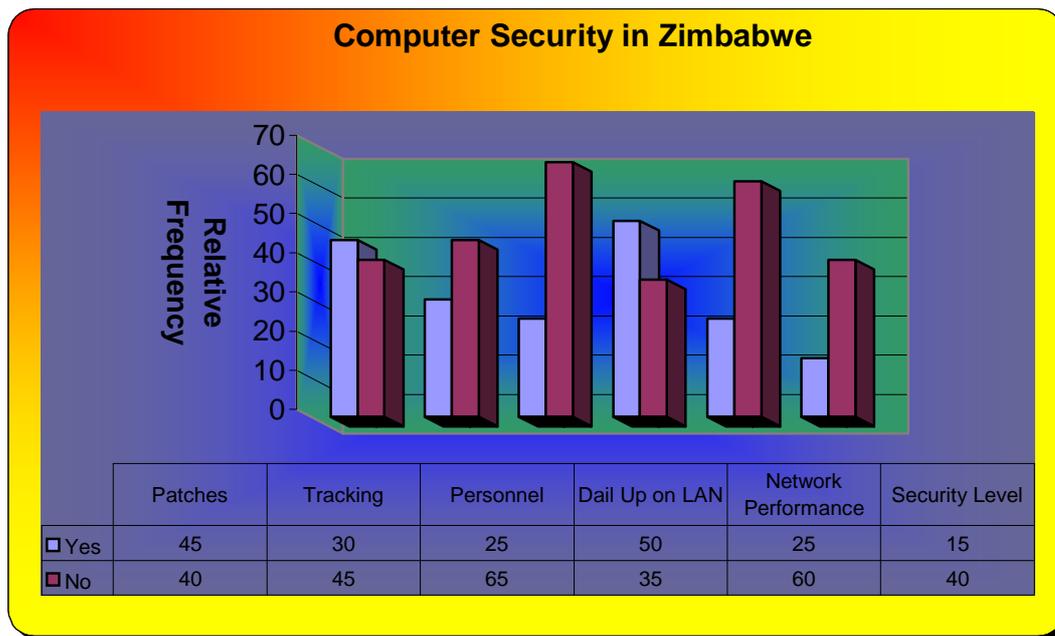


Figure 1.1 Bar Chart Depicting security awareness in Zimbabwe.

Chart 1.1 depicts a sixty-five percentage point companies/organizations that do not have trained and experienced security personnel with only twenty five percent of respondents trying to address the situation one way or the other.

The most interesting observation that the paper made is the correlations that exist between network performance to security personnel and to network design. For example if the network is not well structured it gives rise to incidents of insecurity, if users are not security conscious they may insecurely structure the network there by affecting negatively the performance of the network owing to high incidents of security breaches. With such a low level of security personnel in the country with a number of companies designing their networks in a manner that provides numerous entry and exit points that can not be easily managed due to amount of financial and technical resources required

and an availability of skilled and experienced security personnel. At the same time network performance is compromised in the process. An increase in security personnel will promote a one-gateway approach in network design and an approach, which is a bit more secure, and this will have a ripple effect on network performance. Charts 1.2 and 1.3 clearly model these relationships, which are a cause of concern.

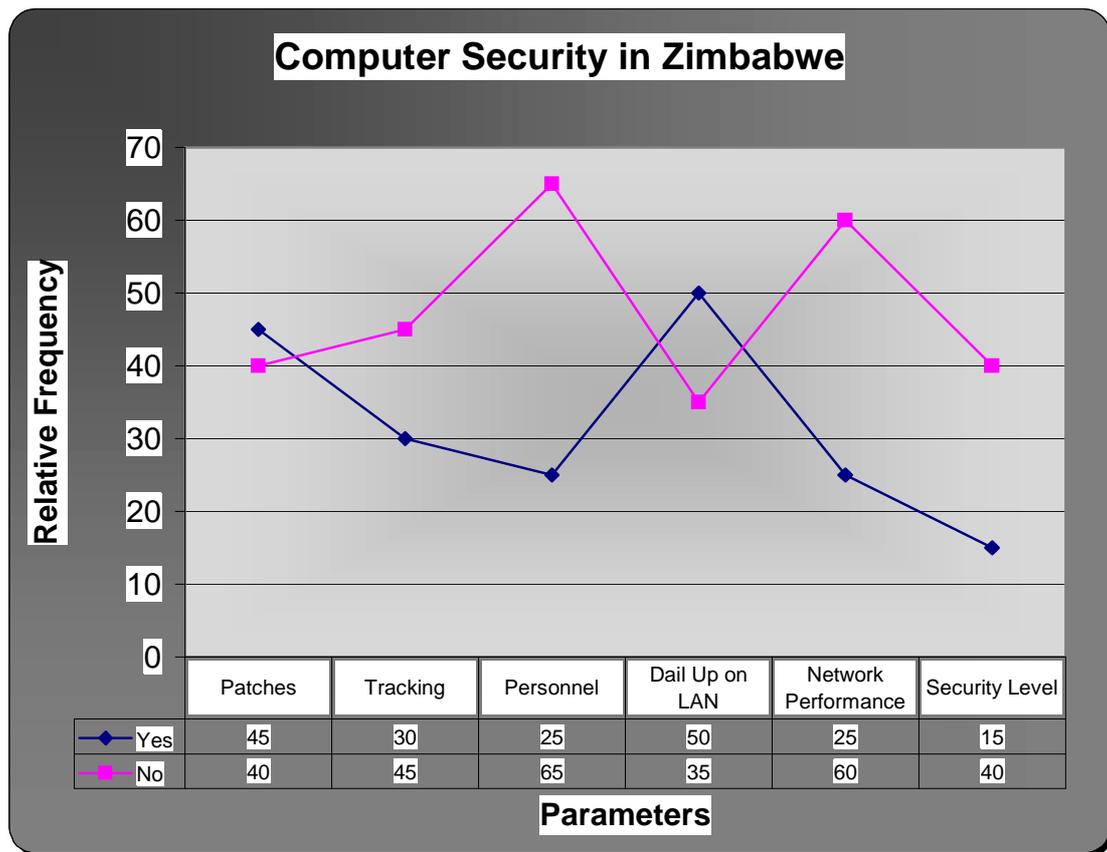


Figure 1.2 Line Graph Depicting Parameter relationship.

The security level in the country owing to unavailability of skilled and experienced security personnel are also hampering organizations in their attempts to track back to source security breaches. With no expertise organizations cannot track attackers and cannot adequately plan for future attacks. The three diagrams used in this paper all show that when there are few skilled security personnel, there are equally few organizations which will be able to investigate attacks. On the other hand when there is a desirable level of security expertise in the country more organizations will be able to investigate

and prosecute the security attackers. This means that a deliberate increase in the number of security personnel has a positive impact on the ability of a country to mitigate incidents of intrusions and security attacks through recourse. Of all the parameters that have been correlated, security personnel parameter remains fundamental in addressing the security problems organizations are facing. A slightly change in security personnel will automatically cause other linked parameters to move up and down. It is a shaker that shakes other parameters with a slight move. More attention should be given to the security personnel parameter, it has to be moved up the scale and should register a big leap so that it can positively influence the other parameters. However the security personnel parameter should be able supported by network design in improving the performance of any network. There seem to be no culture of designing networks with both security and performance in mind. There is great need to look at these issues if the security level in the country is to be improved.

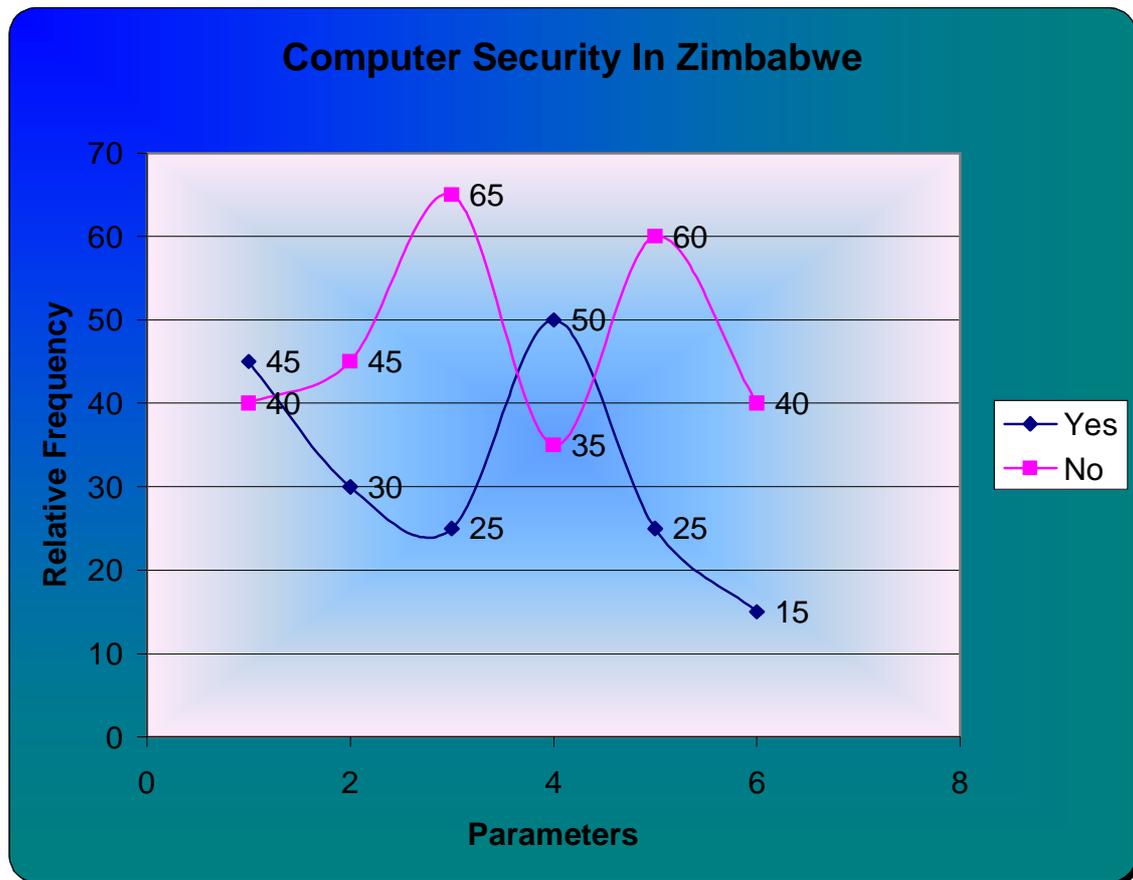


Figure 1.3 Correlation Scatter Chart.

1.4 Recommendation.

The country needs to take a deliberate effort in addressing the security concerns. There is a need for statutory instruments to be enacted to policy and prosecute security attackers and to come up with policy instruments to govern the activities of computer personnel, including computer companies.

There is also a need for a body that oversees the activity of the industry. This body may be an autonomous or can be affiliated to international organizations.

More and more educational institutes should be opened and given a mandate to offer specialized security certification courses. All IT personnel should be encouraged to undertake such courses before any employment is sought. On the other hand employment should be on the basis of such certifications or qualifications.

A collaborative body should be set amongst IT practitioners for networking, sharing of ideas, and for fostering the idea of teamwork for speedily security breaches remedial.

There is also a need for a follow up research that will look at secure network design, designs that are ideal for better network performance, possible security solutions that are ideal, suitable for organizations, and the nature of attacks that are common and how best they can be countered. The sample population needs to be increased to include almost all universities in the country and big corporate organizations.

1.5 Conclusion.

The research concentrated on a few organizations in Bulawayo including the national university of science and technology. An attempt was made to include the university of Zimbabwe through email; unfortunately, no responses were received from the university. However the sampled population does reflect the security status of many organizations and the country at large, hence the results can be extrapolated to the rest of the population. Above all, a follow up research is to be undertaken as per the last recommendation where the sample population will be considerable increased. The second research will have an inclination or bias towards addressing the solution space, over and above exploring the magnitude of problems being faced.

1.6 Reference

- [1] Bill Gates goes after the 'Spam King' (11 August 2005).
http://www.mg.co.za/articlePage.aspx?articleid=247714&area=/breaking_news/breaking_news_business/.
- [2] Ruchika Agrawal et al (2002). The Stanford Student Computer and Network Privacy Project, Communications of the ACM, Vol. 45, No. 3, pp23 – 25.
- [3] A. H. Karp (2003). Enforce POLA on Processes to Control Viruses, Communications of the ACM, Vol. 46, No.12, pp. 27 - 29.
- [4] H. Berghel (2004). Malware Month, Communications of the ACM, Vol. 47, No.2, pp. 11 - 12.
- [5] A Adams & M.A. Sasse (2004). Users are not the enemy, Communications of the ACM, Vol. 47, No.2, pp. 11 - 12.
- [6] Bayrak and Davis, Communications of the ACM, Vol.46, No.12, pp. 99 – 102, December 2003.
- [7] Philip Evans & Bob Wolf (2003). How Toyota and Linux Keep Collaboration Simple, Harvard Business Review/ <http://hbswk.hbs.edu/topic.jhtml/technology>

- [8] T. D. Maswera (2003). The Prevalence of Computer Viruses in Zimbabwe, Zimbabwe of Science and technology, Vol.3, No.1, pp 45 – 50.
- [9] H. Berghel (2003). Communications of the ACM, Vol. 46, No.12, pp. 15 - 19,
- [10] M. Matic (2005). To Block Spam, Demand Sender Authentication, Communications of the ACM, Vol. 48, No.3, pp. 144.
- [11] L. Weinstein (2003). The Devil You Know. Communications of the ACM, Vol. 46, No.12, pp. 114.