ETHICS IN ETHICAL HACKING

IDIMADAKALA NAGARAJU
Associate Professor
Department of Computer Applications, Geethanjali College of Engineering and Technology
Cheeryal (V), Keesara (M), Ranga Reddy, Andhra Pradesh – 501 301, India.
igiriraj@yahoo.com

Abstract- This paper explores the ethics behind ethical hacking and the problems that lie with this emerging field of network security. Since ethical hacking has been a controversial subject over the past few years, the question remains of the true intentions of ethical hackers. The paper also looks at ways in which future research could be looked into to help in keeping ethical hacking, ethical.

Keywords— Ethical hacking, hacking, hackers, education and training, risk management, automated security

I. INTRODUCTION

Ethical hacking technology is spreading to diversified fields of the life and especially to all walks of computer industry; the need to protect the important data of the same should be addressed with right technology. Ethical Hacking emerged as the latest and futuristic technology of the computers, because of the smartness of hackers. Every small or big company is adopting this as the front layer of security for protecting their data. Understanding the true intentions of the general public is quite a hard task in these days, and it is even harder so, to understand the intentions of every single ethical hacker getting into vulnerable systems or networks. Technology is ever growing and people are encountering tools that are beneficial to them. If these tools falls into the wrong hands they can create great controversy, breaching our basic right to privacy, respect and freewill. The constant issues highlighted by the media always reporting some type of cyber crime, a study showing that nearly 93% of attacks happened inside of the organization raising concerns of how easy it is to be working inside to be able to infiltrate attacks [1]. Is ethical hacking finally come to the rescue for solving the problems or has it created new ones?

2. DISCUSSION

A. Education and training

The problem of teaching students to hack is still a very serious issue that we are facing today; experts feel that they will teach students how to improve intrusion which unfortunately not happening so [2]. Understanding the true intentions of the students is very hard to pinpoint the reason why ethical hacking should be used. Teaching students to hack and later discover that the knowledge used to hack, will definitely have an impact on society as to why they are allowed to understand how to hack in the first place, but we cannot, simply, pinpoint our argument to say that it is the fault of the instructors that allowed him to undertake the course [2]. If that is the case, then we would have major problems in other areas, such as when cars are constructed they are crash tested to fully understand areas of improvement to give users a reliable car, if companies did not test the issues, would it be the fault of the manufacturer if the car was involved in a crash?. Teaching students to hack in effect gives them a global knowledge of how to hack into computer systems with the help of subject matter experts. The threat they pose is unimaginable. With the current state of mind students are in, it is easy to imagine what kinds of threats they pose, some in the past have gone on gun sprees, killing innocent students, some starting terrorist plots and now the University helps in causing damage to networks, essentially giving students of “how to do it” directly, showing tools that can be used to do such crimes, similar to giving a burglar a crowbar to break into house. “A problem with the under graduate students using this approach is that the instructor is effectively providing them with a loaded gun” [3], [4].

Once the students acquires new skills they may use them for good or for bad intentions, certain policies that are not being applied at university which need to address issues for students conducting malicious acts. However these can be rectified by applying security checks on individuals which Universities do for certain courses such as ethical hacking. A criminal background check, the requirement of some sort of professional certification, and student interviews are few measures that could potentially weed out several, if not all, students with potential malevolent intentions [5]. With an array of training courses that are available around the world it would be a difficult task to understand the reasons behind their interest in the course. It could be the fact that the individual has been interested in security for a long time and that his main objective is to perfect his CV for better job prospects

and a better salary; the fact cannot be ignored that ethical hackers are highly paid individuals. To a certain extent ethical hacking is ethical. If we did not have such measures in place we would need to manually ensure that our systems are safe, so ethical hacking can ensure safety of our systems if conducted ethically.

B. Trusting the potential enemy

No two individuals in this world are same in nature, behavior and attitude. Their looks, shape, size and even mental states and the actions they do may not be same for any one individual, cannot be perceived as one would hope to. To remedy problems of two totally different individuals would need to be hired to run tests for companies so that no one individual can have total freedom with any one system. The need for secure information is important and maybe an important factor in ethical hacking. Concerned individuals would want to understand certain things about themselves or society in general; this information can lead to major problems of who can obtain that information and who should see it. Hacking is wrong for any gain whether that is financial or personal or for the fact ethical. It can be argued that after working on big projects with one of the countries, big financial companies to find security flaws to help remedy problems, can help to reinforce the knowledge of a ethical hacker and sometimes in the future out of curiosity or through spite breach his contract and sell his ideas to criminals. It was argued that this can be achieved and that this is one of the many problems ethical hacking faces. It is believed that Christians and Muslims feel that committing adultery is wrong and is a major sin. Fundamentally, there is a distinction between ethics and religion, but the urge of wanting you not to do it does not prevent you and you may go ahead and do it anyway. "…used to explain how different people have different perception of right or wrong, depending on their religion, culture or society."[6]. Hackers have a tendency of gaining access to systems and may well know that it is wrong but for that same religious reason, make them want to do it for pleasure or other means.

With the growth of the technological aspects of the business, it is fast growing that all our data is to be made electronic. All business transactions are done electronically to try and bring us into the next generation. eBay for example is a global auction site that persuade businesses to sell their goods, allows an auction room in the comfort of our own homes. Ethical hackers can and may use their abilities to try and avoid paying for items they have brought because they know they can. They use their power to "help themselves" without being caught, at the expense of others, and can be seen as ethical hackers occasional job, essentially in this sense ethical hackers by day and wear black hats when they need to! Unfortunately, some of the skilled professionals use their abilities to harm the society, by finding the vulnerabilities in the companies systems and attacking them, creating and distributing viruscontaining codes, finding the ways to avoid payments for the desired services [7].The idea of corruption can be seen as a major issue in ethical hacking and who we can trust to do the job for us. An ethical hacker may do the job and do it well, but to understand his true intentions may be justifiable. If the ethical hacker is corrupt then maybe the company is corrupt if they deny any mishaps in checked securities that is when an ethical hacker has produced his report and the company gets hacked, the company would turn to the security testers who tested the system. It is understood that the idea here is rather extreme but we need to understand the possibility.

C. Risk Management

Ethical hackers are highly paid professionals with a legitimate status and a means of access. They can minimize the risk of impact, clearly identifying benefits and flaws helping senior company directors to understand if such activities should be undertaken. Ethical hackers could explore vulnerabilities in advance to minimize the risk. The company could undertake penetration tests to find if they are vulnerable to attack. Finding vulnerabilities for companies not only helps the company but also minimizes the risks of attacks. However ethical hackers have five days in general to perform tests, what happens if vulnerabilities are overlooked. If an ethical hacker fails to deliver results to the business and assumes the system is safe and that it has no problems, who will be liable for legal actions if a malicious hacker gets into the system? Surprisingly, a journal by IBM on ethical hacking reports, "….the client might ask "So, if I fix these things I'll have perfect security, right?" "Unfortunately, this is not the case. People operate the client's computers and networks, and they do make mistakes. The longer it has been since the testing was performed, the less can be reliably said about the state of a client's security. A portion of the final report includes recommendations for steps the client should continue to follow in order to reduce the impact of these mistakes in the future." [8]

There is a little possibility of ethical hacking in work places if information is not accurate. If a company has been hacked ethically, what is the colour of the individual's hat is it black or white? Giving special privileges to users then to return with non-accurate information as Palmer [6] describes we can ask ourselves what the differences are, as opposed to using normal security software to do the job for you. Deeper analysis showed that correctly programmed systems initially would help to improve

security. The main concern would be the cost to both manage and administer to provide great solutions. The idea of self-improving can be another issue, so to whom we can allow these improvements, the company or the ethical hackers to increase their knowledge and thus getting enough information they can get hold of and then launching attacks from different parts of the world as a ethical hacking regime that would build knowledge by posing as ethical hackers and getting information to exploit. Another way to view this is, if legitimate ethical hackers who aims to remedy security issues, whether they should be allowed to access certain information and be entered into security barriers. In order to do the job we must have some leeway and be allowed to use certain tools to help them with their job. For example Randal Schwartz, who was sentenced for only doing his job, best describes the need to use tools without any question, to identify security vulnerabilities. Ethical hackers can identify problems, but to what extent, even they would not realise a normal virus eating away at data, they may miss it or let it go since they only have a limited time to perform test. It is the hacker's intention to bypass and deceive the network, the ethical hacker may be vigilant of this and compromise the network leaving it till problems arise, therefore raising the issue of "the insider".

D. Helping the enemy

Almost nothing is secure in our technological world. There is freedom of information and is out there for anyone hungry enough to want it. CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part) which is coined by Luis von Ahn, Manuel Blum, Nicolas J.Hopper and John Longford of Carnegie Mellon University, is a Turing test application which makes accurate distinctions between humans from computers, which can help us understand attacks more clearly and prevent them from happening. Making the distinction between humans and computers help us to rectify problems and to further administer them, are to say catch the human criminals and let the computers do their job. There are many tools available for ethical hacker's help to do their job effectively. It can be understood that there are different varieties of the same tool, a couple of tools can be used by the ethical hacker to hack systems is NMap to find open ports but this is readily available for anyone to download and use. Acunetix, another commercial package that tests for web application vulnerabilities is available to use unethically by a hacker using certain cracks which can be found on the internet. These tools can be used by a normal hacker as well as an ethical hacker, the hackers uses them for criminal intentions and the ethical hacker uses them for the benefit of the organization to help identify weaknesses and flaws in the security. Google is a great search engine which presents valuable and sometimes unwanted information to be obtained. Google causes privacy concerns, for the people to understand how to obtain such information by using clever commands. Is it ethical for Google to hold such information about certain individuals or companies? Certainly, the answer here would be no, it allows us to obtain sensitive information about our targets, good for the hacker, but bad for the target. Though it is still available, companies must ensure that all employees don't send any sensitive information across the internet. Google can play a major role for giving valuable and sometimes sensitive information. This causes great concern for the individuals that purchase or have web servers with valuable information. With further investigation Google allows retrieving valuable information. Let us take for example, shipping a valuable package and that it is decided to be sent using the online system to save time of having to go to the post office, UPS (United Parcel Service) makes this possible.

If a person makes a booking to send a parcel, UPS would collect the package and send it to the desired location. A would be hacker could intercept the booking and impersonate as the company and intercept the package. Using clever searches on Google, private video cameras are not so private, searches show that we can access information directly through Google allowing the would be criminals to execute a perfect crime without even doing field research (for example Google Maps and Google Earth). If a ethical hacker was able to track the day-to-day activities of a certain petrol station, he or she, as a thief could easily calculate the times of business and more importantly the amount of time he/she will take to commit the perfect crime, giving them a specific and accurate time window. The most important and widely obtainable information is that of passwords, a search "Index of /" +password.txt", can allow a range of different passwords searched from databases, allowing hackers in general to wide range of information to commit unsettling crimes. Google in general may be a very powerful tool that assists hacker in a major way, to help minimize the problem can be difficult as we would need separate servers to store information which can be costly and time consuming. Allowing individuals to do such activities helps increase knowledge of the enemy as to know whether they are terrorists or criminals by helping them to commit crimes. This raises concerns that Google may be blamed for allowing hackers for such information.

E. Applying ethical hacking in practice

One memorized record that is not directly linked to the penetration tester at the time can be obtained and exploited, so the trust of information is again infringed upon. Ethical hackers working in banks would create another controversy, having access to valuable data ranging from student accounts to high senior executives, the desire to steal or memorize one account detail would

be enough to help. With many online frauds being committed it would create great problems in tracking down ethical hackers and pinning the blame, for having access to accounts will in effect blame the ethical hacker even if they did not commit the crime. In certain environments where fraud is likely to take place can indeed raise issues. This argument is very important to address since if a job was given to an ethical hacker to check vulnerabilities in banking systems, and a week later several accounts were hacked then who would be to blame is the banker or the ethical hacker?. Now let us imagine the scenario of a residential home and allowing access to systems for administration for safety measures. Members of any community, whether they reside in private homes, large public buildings or residential homes are entitled to a certain level of privacy. Most weaknesses occur more readily through humans rather than computers. But it can be argued that computer failure rates can be between 10-15% therefore allowing a hacker to explore the system within a given time period at the time of failure may not be ethical. One can assume that in this program each resident would receive a number and their daily routines and whereabouts could easily be accessed via the network, whether the patient is playing cards or taking a shower. Certainly no person would be comfortable knowing a network administrator who could easily decipher when they were showering, using the bathroom or getting ready for bed. This brings us to another potential ethical issue [11].

F. The problem inside!

Estimating and understanding the insider attacks is a big problem. Finding the reasons behind the attacks that take place are rather clear, is for shear greed of financial gain. Most cases deal with disgruntled employees who ask for raises and then commit fraud. Most frauds lure employees to steal vital information from their company and start their own company, with full knowledge of the potential profits. Ethical hackers can be presented with a great deal of information that could help, it is also suggested that people within the organization tend not to suspect insiders and focus the problem on outsider attacks. According t the latest consumer review by Deloitte, shows that nearly 4.6 million people over the years of which many frauds taken place from insider attacks (for example, the cases of Warren Buffet and Shiv Raj Puri's fraud in Citi Bank). This implies that most of the frauds committed are from inside which clearly imply that an insider attack contributes to most of the attacks that take place. Trust and knowledge being the most important factor from within the business that contributes to the attacks [1][12].

3. COUNTERING THE PROBLEMS

To counter problems, researchers are looking towards new ways of improving ethical hacking and hacking in general from inside the company. One approach is to use models to monitor employees closely to reduce the risk of impact. One solution is to use a model approach that can seriously help in ethical hacking. Not only does this model helps, but also tries to reduce the impact by identifying implications early enough to help reduce the impact of confrontation. The model depicted below gives us an insight in to the problem and how it can be helped to minimize risks and to further monitor the behavior of ethical hackers and to try to eliminate the problems as and when they occur.

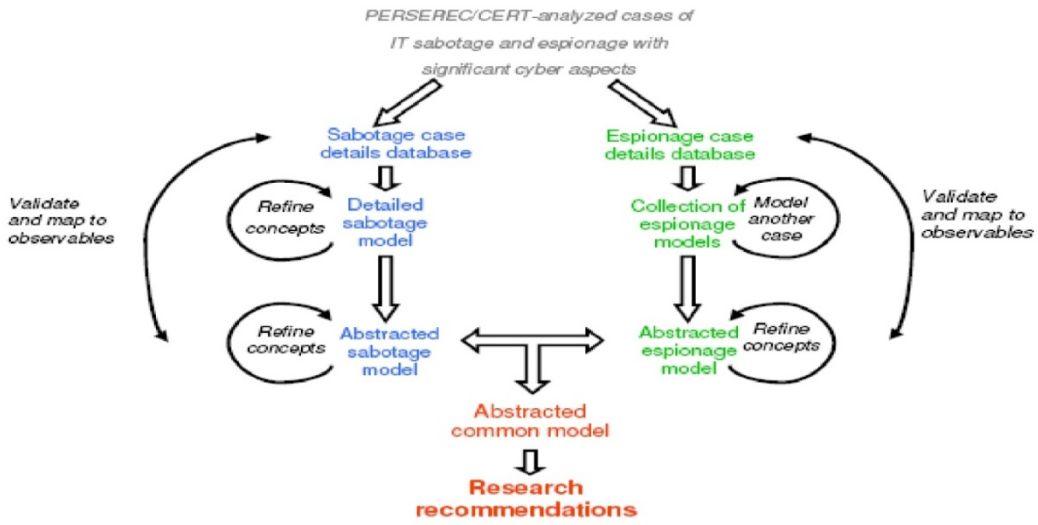

Fig.1 Insider attack analysis

Not only these models be used in the workplace but they can also be adopted in other fields of work such as education. Another solution could be to automate ethical hacking which causes great concerns in allowing machines take over jobs of humans, the biggest problem that lies here is that machines are prone to making mistakes and can sometimes even crash [10].

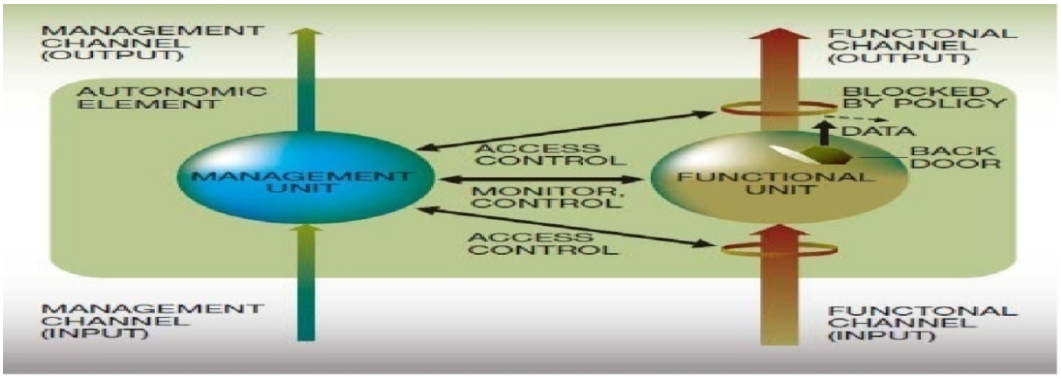

Fig.2 Blockage of backdoor leak by autonomic system

4. CONCLUSIONS

Technology has continued to grow at a high rate over the years and continues to do so; scholars are putting themselves in vulnerable positions by helping individuals to hack. The mind is a very powerful tool that has no control, the control will continue to grow proportionally with the desire to get knowledge of something that is impossible to achieve in its entity, but not forgotten in its entirety. Hackers will always find ways of getting into systems, whether they are doing it for good or bad.

5. REFERENCES

[1] A. Durant, "The Enemy Within", BusinessXL, pp 48-51, 2007.
[2] RD. Hartley, *"Ethical Hacking: Teaching Students to Hack"*, East Carolina University, http://www.techspot.com/news/21942-universityoffers-ethical-hacking-course.html, , 2002.
[3] T. Wulf, "Teaching ethics in undergraduate network", Consortium forComputing Sciences in College, Vol 19 Issue 1, 2003.
[4] Jeffrey Livermore, *Walsh College, Member, IEEE Computer Society 2007.*
[5] Logan and Clarkson, Is it Safe? Information Security Education: Are We Teaching a Dangerous Subject?, Proceedings of the 8th Colloquium for Information Systems Security Education, West Point, NY, 2004.
[6] SA. Saleem, Ethical Hacking as a risk management technique, ACM New York, NY, USA, 2006.
[7] N.B. Sukhai, *"Hacking And Cybercrime"*, AT&T, 2005.
[8] C.C. Palmer, *Ethical hacking*, IBM systems journal, http://www.research.ibm.com/journal/sj/403/palmer.html, 2001.
[9] S. Band, D. Cappelli, L. Fischer, AP. Moore, RF. Trzeciak and E. Shaw, *"Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis"*, Carnegie Mellon University, 2006.
[10] D. M. Chess, C. C. Palmer, S. R. White, Security in an autonomic computing environment, IBM Systems journal, Vol 42, No 1, 2003
[11] http://research.microsoft.com/apps/pubs/default.aspx?id=144888
[12] http://www.computerweekly.com/news/2240179350/Bank-fraud-claims-over-four-million-victims-in-UK