National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS)- Dec 2017

RESEARCH ARTICLE OPEN ACCESS

HACKING AND CYBER TERRORISM: THE REAL THREATS OF NEW AGE?

Amit Kiran Dasgupta[1], Ashrith Pawar[2], Nikhath Jeelani[3], Sundaresha[4]
[1,2,3,4](BCA, St. Joseph's Evening College, Bangalore)

Abstract:

As the new age approaches, our society is increasingly becoming dependent upon information technology. However, as technology can deliver a number of pros, it also introduces new cons that can be exploited by persons with the necessary technical skills.

The paper discusses the problems posed by hackers and information compromisers considers the kind of responses necessary to protect our society.

Keywords — **hackers, cyber terrorists, information dissemination.**

I. INTRODUCTION

As we approach the new age, a lot has been done of the so-called 'Year 2000 Problem' or 'Millennium Bug'.[1] Concern over the problem is definitely justified in many ways and demands appropriate action to be taken to avoid significant disruption to everyday services. However, in a bigger picture, the millennium bug panic should act as a 'wake-up call' to general public and modern society's dependence upon information technology and communications systems. This statement is in no way intended to portray IT as a negative influencer, but it must be understood that it brings new threats to the society.

For someone who wish to cause damage, there is now the capability to undermine a society without a single shot being fired or missile being launched. Let's consider how many essential areas of modern society are now so significantly dependent upon technology that its unavailability could be disastrous,

For example:

- Healthcare
- Manufacturing;
- Banking / finance;
- Government.
- Transportation;

Undermine the technology and consider the infrastructure impact: manufacturing would stop, access to money would be denied and people in need of care or support would not receive it. The new industries of the next age, such as e-commerce, could be the first victims of this new style of problem.

All of the above could conceivably occur as a result of an accidental incident or a lack of precaution measure (e.g. in the same way as the Millennium Bug issue came about).

However, this research paper is to consider the potentially more alarming scenarios in which technology infrastructures or services are targeted deliberately. The protagonists in such a scenario could come from diverse backgrounds. For the purpose of discussion, however, the paper will consider them as 'hackers' and 'cyber terrorists'.

II. NEW THREATS OF THE INFORMATION AGE

The previously mentioned Millennium Bug represents a major threat to the information society and has the potential to cause considerable amount of damage if organizations are not prepared. However, it is a problem that is most likely forgotten by the majority of organizations in a few months after 1 January 2000. The issues of computer hackers and cyber terrorists should be considered in order to represent long-term threats to the Information Society. This section examines the same in detail.

A. *Hackers*

The term ‘hacker’ was originally coined to refer to individuals who had a low-level familiarity with the technological operation and were capable of devising technically elegant software solutions [2]. However, the usage of the term has changed over the past few years and is now used to refer persons who deliberately gain (or attempt to gain) unauthorized access to computer systems.

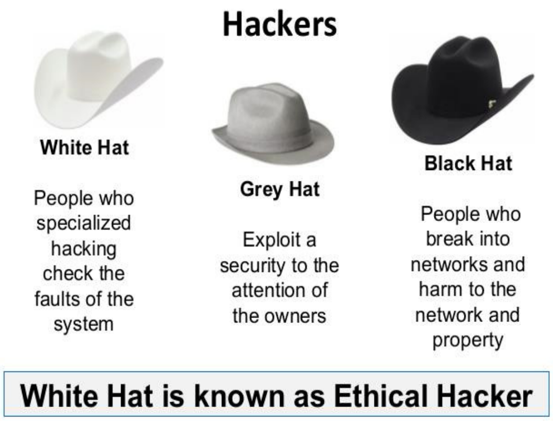
Hackers
White Hat
People who specialized hacking check the faults of the system
Grey Hat
Exploit a security to the attention of the owners
Black Hat
People who break into networks and harm to the network and property
White Hat is known as Ethical Hacker

Fig. 1: Types of Hackers

Hackers are by no means a new threat and have been in the NEWS during the last two decades. Indeed, they have become the latest ‘target’ of the media, with the standard approach being to present the image of either a ‘teenage kid’. In reality, it can be argued that there are different varieties of this problem. Some hackers are malicious, while few are merely naive and, hence, don’t appreciate that their activities may be doing any real harm. Furthermore, hackers may be seen to have numerous motivations for their actions (including financial gain, revenge, ideology or just plain mischief making). However, in any cases it can be argued that this is immaterial as, no matter what the reason is the end result is some form of adverse impact upon another party.

TABLE I
SURVEY DETAILS OF HACKING INCIDENTS

Year	**1987**	**1990**	**1994**	**1998**
Abuse Reported	118	180	537	510
Number of Hacking Reported	35	26	15	56
Hacking as % of total	30%	14%	3%	11%
Resulting Loss	$100	$31,500	$16,220	$3,60,860

Table 1 illustrates the extent of the hacking problem, based upon data taken from a series of surveys by the UK Audit Commission [3, 4, and 5].

It is worth noting that the significant amount of increase in the ‘total incidents’ figures in the 1994 and 1998 surveys are largely due to widespread emergence of the virus problem. It should also be noted that these figures only points to the reported incidents - the true figures may be much higher than this, but organizations are opting to remain silent in order to avoid adverse publicity [6].

The list below pinpoints a small variety of the activities that hackers have been known to indulge in. In many cases there have been reports of hackers not only gaining unauthorized access but also altering data i.e. affecting integrity or availability:

- Modification of medical records [4]
- Breach of military systems [7]
- Monitoring and alteration of telecommunications services [8]

As seen, breaches in all the above categories offer significant opportunities to inflict damage (to both organizations and individuals) and, therefore, illustrate the nature of the hacker threat. Also, the evidence suggests that it’s possible to breach systems that we would expect to be more secure (e.g. military sites). The fact that these attacks have been successful leaves a lot of questions about systems vulnerable to more high profile threats, in which information systems become the target in a more sinister way.

B. *Cyber Terrorists*

Recent years have seen the widespread use of information technology by terrorist organizations. This has led to the emergence of a new breed of threat, termed as ‘cyber terrorism’. This is considered as distinct from ‘traditional’ terrorism since physical terror are null and efforts are focused upon attacking information systems.

Fig. 2: Representational image of Cyber Terrorists

When observed from the perspective of skills and techniques, there is very little to distinguish cyber terrorists from the general hackers. Both groups utilize variety of techniques in order to breach the security of target systems. From a motivational perspective however, cyber terrorists are notably different and are operating with a specific political agenda to support their actions. Firstly, the fact that cyber terrorists are part of an organization could mean that they have funding available to support their activities. This in turn would mean that individual hackers could be hired to carry out attacks on behalf of a terrorist organization where the hackers themselves may not know the terrorist’s cause, but will undertake the work for the sake of money.

Established terrorist groups are currently using the Internet for a number of purposes, as described below.

III. Publicity

Terrorist groups have traditionally had difficulty in portraying their political messages to the general public without being censored. However, they can now use the Internet for this job. Examples of where this is already the case include the Irish Republican Information Service (http://joyce.iol.ie/~saoirse/) and the Zapatista Movement (http://www.ezln.org/).

C. Fundraising

Some terrorist groups are even linked to political parties and are now using the Internet for fund raising purposes. This means, in future, smaller resistance groups may receive the majority of their funding through credit card donations.

D. Information Dissemination

It is also possible for the groups to publish sensitive information about a particular country. For example, Sinn Fein supporters at the University of Texas made details about British Army establishments within Northern Ireland publicly available on the Internet [9]. In addition, information about engaging in terrorist activities is also available. For example, the ‘Terrorist Handbook’ [10] instructs beginners how to make explosives and weapons and is widely referenced and available on the Internet.

E. Secure Communications

Terrorist uses advanced encryption methods [11] and their use of improved anonymous electronic re-mailers will result in a command system that is difficult to break and will allow controlling of groups anywhere in the world. This poses a major problem for the security services, as it means that they will need to spend more time and resources on trying to decrypt electronic messages.

Fig. 3: Layout Design of Secure Communication

While all of the above might give cause for concern, they rarely illustrate how existing activities may be simplified via new technology. The real threat in the ‘cyber’ context is when the Internet becomes the medium in which a terrorist attack is conducted. Needless to say, the Internet is now itself a medium through which widespread damage can be caused to the new information society.

To see the potential for damage, one has to just look at the results of actions from individuals who have acted without a war motive and without government/official backing [12].

The most significant threats arrives from the integrity and availability aspects. Security breaches in these fields have the potential to do direct damage (e.g. by making systems unavailable or having them operate on the basis of incorrect data). Confidentiality breaches could have an indirect value in a terrorism. The term ‘information warfare’ has been used to describe the ways in which terrorist groups could use technology to attack the IT infrastructure of a particular company [13].

A denial-of-service (DOS) attack results when the access to a computer or network is intentionally blocked as a result of malicious action taken by another user. These attacks do not necessarily cause permanent damage to data, but they compromise the availability of the resources [14].

The first recorded cyber terrorist denial of service attack was carried out by Tamil Tigers against Sri Lankan embassies around the world [15].

For example, the US Department of Defense (DOD) claims that its WWW sites experiences around 60 attacks each week. In 1995 alone, the DOD claimed to have been attacked 250000 times [16].

The US military has now begun to rethink its attitude towards the use of the Internet and has been reviewing the material that is published on its Web sites in order to prevent sensitive information from being made available [17].

IV. METHODS OF RESPONSE

Having considered the nature of these threats, it is fairly appropriate to consider what is needed to address them and the extent to which appropriate action is already taken.

The hacker issue is now widely recognized and various countries already have some form of associated legislation. An example of this is the Computer Misuse Act in the United Kingdom, which specifies offences ranging from unauthorized system access to unauthorized modifications to programs or data [18]. However, just the presence of legislation is not sufficient - law enforcement and the judiciary must be suitably prepared to administer it. Few of the previously documented cases of hacker indicated that this may not be the case and the criminals often have a significant upper hand in terms of their understanding of technology. A good example of this is provided by Stoll [19] in his recounting of the experiences of law enforcement whilst tracking the so-called ‘wily hacker’.

Fig. 4: Cyber Security

It is difficult to predict exactly how terrorists groups may use the Internet in the future. However, it is assumed that cyber terrorism will become even more attractive to terrorist groups. The principal reasons for this are as follows [20]:

The risk of capture is reduced since attacks can occur remotely.

It is possible to inflict grave financial damage with- out any loss of life.

The expertise for these attacks can be hired.

A successful attack would result in worldwide publicity and failure would go unnoticed.

Terrorist groups can attract supporters from all over the world. They can use the Internet as a method of generating funds for their cause worldwide.

The Internet offers the ideal propaganda tool for a terrorist group, one that operates on a global basis and that individual governments cannot control or censor.

The capability to mount an attack can be developed both quickly and cheaply

Whilst the threats are serious, we must be careful to ensure that our methods of response are not taken too far [21]. Without appropriate control, it is possible that measures could be introduced that are harmful to society. [22].

It is seen that the activities of both hackers and cyber terrorists ultimately have the effect of restricting freedoms for the rest of us. For example, the United States continues to maintain a relatively restrictive policy on the use case of cryptographic technology. One of the key reasons for control is to prevent unregulated use of strong encryption techniques by terrorist groups [23].

V. CONCLUSIONS

Whether we like it or not, modern society has a significant dependence upon information technology. This paper signifies that, as a result of this, we face a number of immediate and long-term threats that need to be recognized in order for protective action to be taken. This discussion has focused upon the particular threats posed by hackers and cyber terrorists.

In the case of hackers we can, to some extent, take comfort from the fact that a huge proportion of them are not engaging in their activities for a malicious purposes. This is good news because, in many ways, the hacker threat is likely to be more difficult to the police rather than that of cyber terrorism. The reason for this is that the number of casual hackers exceeds far beyond the number of cyber terrorist organizations and their targets may be much less predictable. At the same time, however, the impact of any individual attack is likely to be less effective.

Cyber terrorists operate with a political agenda. This motivation will mean these types of attacks will be more specifically targeted and aimed at more critical systems.

In a way, any true society will always include elements that many of its other members would consider to be undesirable.

ACKNOWLEDGMENT

We wish to acknowledge Mrs. Annie Syrien, Department of BCA and other contributors from different class of BCA, St Joseph's Evening College for sharing their views and information.

REFERENCES

1. *Ulrich,W.M. and Hayes. I.S., The Year 2000 Software Crisis, Yourdon Press Computing Series, Prentice Hall, ISBN O-13- 655664-7., 1997.*
2. *Levy, S., Hackers: Heroes of the computer revolution. Anchor Press / Doubleday, 1984.*
3. *Audit Commission, Survey of Computer Fraud Abuse, 1990.*
4. *Audit Commission, Opportunity Makes a Thief: An Analysis of Computer Abuse, National Report, London, HMSO. 1994.*
5. *Audit Commission, Ghost in the Machine --AM Analysis of IT Fraud and Abuse. Audit Commission Publications, UK. February 1998. ISBN l-86240-056-3, 1998.*
6. *Nycum, S.H. and Parker, D.B, "Prosecutorial experience with state computer crime laws in the United States", in Security and Protection in Information Systems, A.Grissonnanche (Ed.), Elsevier Science Publishers B.V., North-Holland: 307-319, 1990.*
7. *Niccolai, J. "Israeli Arrested for Hacking U.S. Military Computers". IDG News Service, March 19, 1998. See http://www.infowar.com/, 1998.*
8. *Littman, J, The Watchman -The Twisted I+ and Crimes cd Serial Hacker Kevin Poulsen. Little, Brown & Company Limited. ISBN O-316-52857-9, 1997.*
9. *Tendler, S, "Ulster security details posed on the Internet", The Times, 25 March 1996, UK, 1996.*
10. *Anonymous. 7'/1r Terrorist's Handbook. Available on Internet / WWW, 1994.*
11. *Malik, I, Computer Hacking: detection and protection. Sigma Press, UK, ISBN l-85058-538-5, 1996.*
12. *NCC, The Information Security Breaches Survey 1996. National Computing Centre, Oxford Road, Manchester, UK, 1996.*
13. *Schwartau W, Information Warfare: Chaos on the Electronic Superhighway. Thunder's Mouth Press, New York, 1994.*
14. *Howard, J, An Analysis of Security Incidents on the Internet. PhD thesis, Carnegie Mellon University, USA, 1997.*
15. *Associated Press, "First cyber terrorist action reported", May 6th, USA, 1998.*
16. *McKay, N, "Cyber Terror Amend] Grows", Wired News, I6 October 1998. http://www.wired.com/news, 1998.*
17. *Booth, N, "Pentagon gets tough in war of the Web", The Times, Interface Supplement, 7 October 1998: 2, 1998.*

18. *HMSO, Computer Misuse Art I Y90. Her Majesty's Stationary Office, UK. ISBN O-10-54189O-0, 1990.*

19. *Stoll. C, The Cuckoo's Egg, Pan Books Ltd, London, UK. ISBN 0-330-31742-3, 1991.*

20. *Warren, M, "Cyber Terrorism", Proceedings of SEC-98 - IFIP World Congress, Budapest, Hungary, August 1998, 1998.*

21. *NIPC, Mission Statement, National Infrastructure Protection Centre. http://www.fbi.gov/nipc/nipc.htm, 1998.*

22. *Davies, S, Big Brother - Britain's web of surveillance and the new technological order. Pan Book Ltd, London. ISBN O-330- 34931-7, 1996.*

23. *FBI, Encryption: Impact art law Enforcement. Information Resources Division, Federal Bureau of Investigation, Virginia, US. 8 July 1998, 1998.*