Matriculation Number: [student ID removed]

Module Code: CS1005

Module Title: Computer Science in Everyday Life

Word Count: 1937 (not including Bibliography and Endnotes)

Title: Gary McKinnon is facing extradition to the USA because he hacked into the Pentagon system. Discuss the computer security issues raised by this case.

Gary McKinnon is facing extradition to the USA because he hacked into the Pentagon system. Discuss the computer security issues raised by this case.

It is beyond doubt that there are an increasing number of people using the internet every year and it is becoming a fundamental part of how we run our lives. The internet is used for personal socialising, general communication, business transactions, banking and government affairs. The original attraction of the internet was accessibility; this is such a powerful tool because it allows information to be available to everyone with no time or location boundaries. Only when we begin to consider the ways in which the internet is being used for private affairs in our increasingly modern society do security issues begin to raise their heads and we are faced with a serious flaw which could leave our money, identity and perhaps safety at risk. In recent years the case of Gary McKinnon has dragged security issues into the light and in this essay I shall address the problem and possible solutions of internet security.

McKinnon hacked into the Pentagon system but was only discovered due to not covering his tracks[i]. He was able to access dozens of US military computers which one would believe should be the most secure in the world and we can only imagine the repercussions if McKinnon had wanted to use the information he discovered for activities such as terrorism. If this man was able to access such information about the American defence system from the comfort of his own home then this leaves us seriously considering the, seemingly small in comparison, issue of where we stand with the safety of our own personal or business assets and identities and also contemplating the major issues concerning patriot and worldwide security. To illustrate the matter we can examine to the case of online banking;

we have entered a new generation in which criminals don't actually need to physically enter a bank to steal from it[ii], they are able to hack into computers and monitor them, acquiring all sorts of details such as passwords, screen names, credit card numbers and much more. Due to the rise in electronic transactions and processing of data in modern society, such as online banking systems and e-shops such as Amazon, there is high demand for internet security and until this is guaranteed then the internet will remain flawed and unable to reach its full potential.

So, now we know the necessity of security we can consider the idea that because the nature of the internet is such that "almost anyone can 'read' anything sent over it"[iii], security is therefore hard to achieve because things such as fraud, impersonation and tampering with data are relatively easy to pull off. For example, if I wanted to purchase something from Amazon, I would be entering details such as my name, credit card number and address; however, how do I know that this is the real Amazon server I am talking to and not a fake and vice versa? i.e. the server needs to establish that I am in fact a real client. This authentication is essential in order to combat security attacks; it is possible for a hacker to be able to direct you to a proxy server and then monitor communications between you, this is referred to as a man-in-the middle attack[iv]; the hacker is able to obtain the information that you think you are passing to the real and secure server. After authentication the details must be sent back and forth privately so that no other user can intervene and record or change the communication particulars. However, still are we faced with another issue: although I may be a real client, I may be an impersonator, i.e. I could be using someone else's password and user name. Thus, we need to have a number of security measures to ensure identity in order to allow for maximum security.

Firstly, in order to establish the connection safely we need to use client and server authentication. This means that there is an established link between two real machines, and then we need to consider the identity of these servers and clients. To try and diminish the risks of impersonation we introduce digital signatures in the form of usernames, passwords and security questions, however, there is always a risk of a hacker being able to monitor a certain machine and finding out this information. Therefore, the more digital signatures are used per transaction the more secure it is. Once the link between the client and server has been made then the data is sent across, we can use cryptography to encrypt the message into a code which will then be decrypted by the receiving computer so that if it is intercepted in transit then it is not able to be read; the better the encryption, the stronger the security. Sometimes, it is possible to have a double encryption where the clients' computer will encrypt the message before it is transmitted and then when the coded data is transmitted it gets encoded again. Finally, a hash function can be used to verify that the message has not been altered in transit[v]. All of the above needs to be done in order to achieve the maximum security levels currently possible and there are some devices and protocols which cover some aspects of these and I will discuss a few of them below.

SSL Protocol is a system which can make the secure connection between client and server; in short it "allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection"[vi]. Authentication and encryption means that the SSL Protocol is capable of providing a reliable connection and so avoids a hacker intercepting a message, altering it or providing a fake message[vii]. This kind of security is especially important in cases such as internet banking; the client wants authentication that the bank

server is real because he will be sending across his credit card details and the bank wants to ensure the client is real because it will be sending confidential information back, additionally encryption is a necessity so that the details are not intercepted via transit as then they can obviously be used for criminal purposes. Other examples of the SSL Protocol being used in everyday life involve things such as Universities allowing their students to safely log in and view and alter personal details, course grades and submit essays, e-Commerce companies such as Amazon and Tesco online where the client and server are exchanging details and large corporate businesses who communicate online due to location restrictions who will be exchanging private information. SSL can also use another security feature which is that of HTTPS. The Hypertext Transfer Protocol (HTTP) runs the SSL Protocol but through a secure port on the computer. The default port number for communication is port 80; however HTTPS will direct the message through the secure port of 443[viii].

In addition to using SSL to establish a secure connection between clients and servers we can use, for example, Chip-and-Pin devices to authenticate the identity of these clients and servers. This covers the idea that I cannot go to Amazon and type in someone else's username and password and establish a secure connection; the Chip-and-Pin device is confirming that I am in fact that person I claim to be. This is necessary because currently computer hackers are able to discover a person's user name and password by monitoring certain computers and recording the information, the criminal then has your details and can, for example, withdraw money from your bank account. The device's success[ix] is claimed to be the idea that there is no connection between the device and your computer, so the device is generating a completely random number which is then entered in to the computer. So, if someone is monitoring your computer they will have access to that random number

but there will only be a small amount of seconds between you entering the number and then being logged onto the system and obviously next time you wish to log in, the number will change. Other companies have begun to introduce technology of a similar nature to Chip-and-Pin devices; for example PayPal has begun to introduce a security token[x] which produces a random 6-digit code which must be typed in alongside a password in order for customer login and companies now have to option of purchasing things like the RSA SecurID® [xi] key fobs and cards in order to add an extra security layer in addition to passwords.

Above I have addressed the need for security and some of the things which can be done to ensure it is implemented. However, it is questionable how, even though we know how to provide maximum internet security, hackers are increasingly accessing more data every day. It seems that either there is a problem with our solutions to security i.e. the authentication we are using doesn't work etc, or we are not using the devices we have correctly. Education is necessary because people must be aware of the actions that they need to take; one example is password strength and protection. Passwords are used on every secure internet site, often in addition with other information, and if one's password is simply one's name or date of birth then it is providing extremely weak protection. In relation to using the device we have correctly; SSL protocol, chip-and-pin devices, secure passwords can all be used for protection and we can use various methods to try and ensure server, client and message authentication, a secure connection and an encrypted communication; however, all of these must be used together to provide security and even then we never know if there will be a new way of hacking through these features.

McKinnon hacked into a system which one would think had the highest security measures in place, so either these are not good enough or they were not used correctly; a combination of education and technological ability is necessary. The USA are seeking to punish McKinnon, however, in a way we should be glad that he has highlighted the issue in a relatively harmless way for all we know people could have hacked into this system before him and just not left any evidence behind and this is a worrying thought. The internet is an amazing invention but until this serious flaw of security is rectified then it will remain impossible for businesses and individuals to bloom by using it; there will always be a risk of fraud, identity theft, businesses being destroyed and terrorism operating. Much more needs to be done. Until we have full security then we should know the full risks involved and use the internet accordingly. We must be prepared for intrusion and have adequate laws and processes in place deal with it.

Perhaps we need to consider exactly what information we do surrender to the internet; even if we may trust a company's ethical policies, i.e. that they won't release our data; can we really trust their technological expertise in our protection? Perhaps we need to consider just whether the ease and speed of the internet is really worth the risk.

BIBLIOGRAPHY:

Books:

McDaniel, H. (2007). *Bank Robbers Now Use Computers.* Outskirts Press

Tan, M. (2004). *E-Payment: The Digital Exchange.* Singapore University Press

Online References:

BBC. (2007). *PayPal introduces security token*. Retrieved October 18, 2009, from http://news.bbc.co.uk/1/hi/technology/6357835.stm

BBC. (2009). *Profile: Gary McKinnon*. Retrieved October 18, 2009, from http://news.bbc.co.uk/1/hi/uk/7839338.stm

CMU notes. (n.d.). *Security4* and *Security5.* Retrieved October 18, 2009, from http://euro.ecom.cmu.edu/program/courses/tcr763/2002pgh/

Content Verification. (n.d.). *Man in the Middle Attack.* Retrieved October 18, 2009, from http://www.contentverification.com/man-in-the-middle/index.html

Hussain, A. (2007). *Internet Banking: security.* Retrieved October 18, 2009, from http://www.crime-research.org/analytics/Internet-banking-security/

Introduction to SSL. (n.d.). *Introduction to SSL.* Retrieved October 18, 2009, from http://docs.sun.com/source/816-6156-10/contents.htm

Rescorla, E. (2000). *HTTP Over TLS.* Retrieved October 18, 2009, from http://tools.ietf.org/html/rfc2818

RSA. (n.d.). *Technical Specifications*. Retrieved October 18, 2009, from

http://www.rsa.com/node.aspx?id=1311

SSL Tutorial. (2001). *Introduction, Protocol Overview, Why is SSL secure?, SSL Use Examples.*

Retrieved October 18, 2009, from http://www3.rad.com/networks/2001/ssl/index.htm

---

[i] BBC. (2009). *Profile: Gary McKinnon*.
[ii] McDaniel, H. (2007). *Bank Robbers Now Use Computers.*
[iii] SSL Tutorial. (2001). *Introduction.* (para. 1)
[iv] Content Verification. (n.d.). *Man in the Middle Attack.*
[v] CMU notes. (n.d.). *Security4.*
[vi] Introduction to SSL. (2001). *The SSL Protocol.* (para. 2)
[vii] SSL Tutorial. (n.d.). *Introduction, Protocol Overview, Why is SSL secure?*
[viii] Rescorla, E. (2000). *HTTP Over TLS.* (2.3 Port Number)
[ix] Hussain, A. (2007). *Internet Banking: security.*
[x] BBC. (2007). *PayPal introduces security token*.
[xi] RSA. (n.d.). *Technical Specifications*.