Selected Computing Research Papers

Volume 1

June 2012

Dr. S. Kendal (editor)

Published by
the
University of Sunderland

Edited, typeset and printed by
Dr. S Kendal
University of Sunderland
David Goldman Informatics Centre
St Peters Campus
Sunderland
SR6 0DD

Tel: +44 191 515 2756
Fax: +44 191 515 2781

Contents Page

An Evaluation of Anti-phishing Solutions

Arinze Bona-Umeaku

Abstract

Phishing as an online threat has resulted in the development of currently available anti-phishing solutions. Most of these solutions are automated web-based tools that warn users against phishing sites and protect users from third party invasion on their details when accessing a genuine website. In this paper we closely evaluate the performance of a web content system and a password protection system using documented evidence to summarize findings and offer a proposed solution.

1 Introduction

One of the major internet threats is phishing. Phishing which has turned out to be a major problem in the advancement of e-commerce bringing doubts to the minds of customers on the use of internet as a business tool. It has been noticed that phishing attacks progressively increases year after year, (Chen et al. 2011) this has also been seen in more recent attacks against Sony's Play station network and Epsilon. This has resulted in several businesses and organisations investing substantial amount of research to find lasting solution (APWG, 2011). For example companies like Cyveillance anti-phishing is dedicated to providing anti-phishing solutions to organisations to enable them prevent, detect and recover from phishing attacks. Some software vendors offer toolbars that help users identify genuine sites (Zhang et al. 2007).

In this paper we evaluate methods that have been proposed through series of research and how they have performed towards the anti-phishing crusade. Among other methods mentioned here we would take a close look at two systems, a content web-based automated system and an authentication system that prevents a preset password. After which a practical solution from evaluations made, based on tangible evidence, implementation and tests that has been carried out in previous research papers.

2 Web Content Systems

2.1 Anti-phishing Toolbars

In respect to this paper where we evaluate automated phishing solution, research has been done in the area of automated anti-phishing detection solution for example the spoofguard (Zhang et al. 2007) which checks the website for certain characteristics like the host name, traceable spoofing techniques and checking against previously marked images. Various software vendors have developed anti-phishing tool bars that identify a page as a phishing site or legitimate site using methods of blacklisting (list of fake websites), whitelisting (list of genuine websites) and user ratings (Cao et al. 2008). Some of such examples are outlined below; Google makes available the source code for the safe browsing feature and claims that it cross-checks URLs against a blacklist. E-bay also developed a toolbar that uses both heuristics and blacklists to identify fraudulent URLs, It was also developed in a way were users can report newly identified fraudulent sites. In internet explorer Microsoft also embedded a phishing filter which uses heuristics as well as depends largely on the blacklist hosted by Microsoft and option for users to report suspected sites. The Netcraft toolbar which was built to use a log of blacklisted websites hosted by Netcraft and a list of sites identified by users but confirmed by Netcraft.

Having evaluated this using publicly available information provided by the toolbar download websites (APWG, 2011) it was discovered that majority of the tool bars mentioned above used blacklists to identify fraudulent sites, but not all were able to accurately identify phishing sites (Reddy, 2011). This could be as a result of the size of blacklist used by each toolbar therefore a list with more tagged and user updated sites will perform better than that with fewer list of phishing sites. Also the heuristics used could have been used to detect other sites that have not been put in the blacklist. Although spoofguard was the only tool bar that did not use blacklist instead it used heuristics still missed some phishing sites and had a high rate of false positive (genuine sites mistaken for fraudulent) this could probably be improved by the addition of whitelist (list of genuine sites)

2.2 Automated Webpage Detector

Meanwhile the solution Presented here by (He et al. 2011) is a heuristic solution to determine if a website is a genuine or a phishing page, based on its content, HTTP transaction and search engine results. According to He et al (2011) this solution identifies phishing sites without using the blacklist technique. This is done by converting a web page into 12 features which are selected based on exisiting normal and phishing page. This method claims to help users identify a phishing website before it is blacklisted or shutdown as is the case with the blacklist-based anti-phisihng toolbar mentioned above. Also claiming that the solution is able to extract a webpage identity using the famous *tf-idf* (frequency-in-verse document frequency) method and this identity would be the basis for determing a phishing or legitimate webpage using an SVM (support vector machine) classifier.

Two different experiments were conducted using two different testing data-set to evalute the method. There are two metrics used to evalute the performance; true posititve(TP) rate and false posititve (FP) rate where the true positive rate measures the percentage of phishing site which correctly labeled as positive phishing and it is computed by (Figure 1) (He et al. 2011).

$$\mathrm{TP} = \frac{n_{\mathrm{phish}\to\mathrm{phish}}}{n_{\mathrm{phish}}},$$

Figure 1

Where $n_{\mathrm{phish}\to\mathrm{phish}}$ is number of phishing pages which are rightly labelled as phishing, and n_{phish} is number of phishing pages. The higher TP value the better the detector. While false positive rate measures the percentage of legitimate sites which are falsely labeled as positive phishing and it is computed by (Figure 2) (He et al. 2011).

$$\mathrm{FP} = \frac{n_{\mathrm{legitimate}\to\mathrm{phish}}}{n_{\mathrm{legitimate}}},$$

Figure 2

Where $n_{\mathrm{legitimate}\to\mathrm{phish}}$ is number of legitimate pages which are wrongly labeled as phishing and $n_{\mathrm{legitimate}}$ is number of legitimate pages(He et al. 2011). This means that when there is a lower FP value the betterr the detector.

Experiment 1

100 login pages of top targeted legitimate websites (He et al. 2011) were collected. Another 100 webpages consisting the following were collected;

35 Homepage of top targeted websites, 35 Top pages, 30 Random pages from a list of 500 pages used in 3Sharp's phishing study. (He et al. 2011)

From the 200 legitimate and 325 phishing pages, 50 legitimate and 50 phishing pages as the training set. The 50 legitimate pages consist of:

- 10 login pages of top targeted websites
- 15 Homepages of top Alexa websites
- 10 Homepage of top targeted websites
- 15 pages from 3Sharp list.

Therefore classification result is shown below as:

True positive rate of the method is 97.33% and false positive rate is low at 1.45%. Although most of the phishing pages used here were already shutdown at the time of the test.

Below is the graphical representation of the performance on the first dataset.

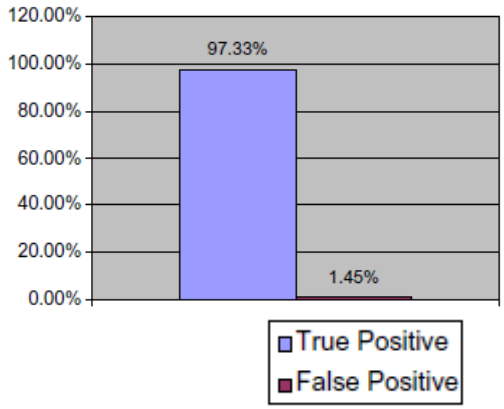


Figure 3

Experiment 2

Using the same training set as the first experiment the proposed detector is tested with a different set. 100 legitimate webpages are collected along with another 100 phishing pages from live phishing pages from phishTank (PhishTank). The legitimate webpages were also changed to evaluate the stability of the proposed detector (He et al. 2011). Below is a graphical reperesentation of the results when compared to other methods like CATINA (Zhang, 2007).

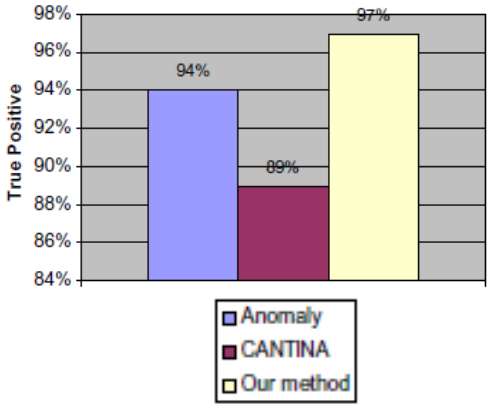


Figure 4
True Posititve comparison (He et al. 2011).

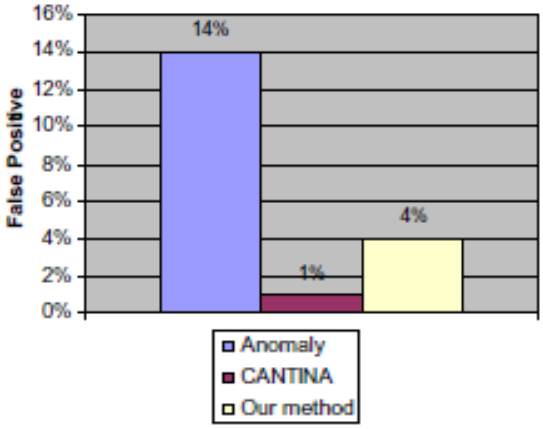


Figure 5
False positive comparison (He et al. 2011)

Having evaluated the webpage detector (method 1) used to detect phishing sites here, it was discovered it has some limitations which include that *tf-Idf* (frequency / inverse document frequency) does not work with other languages other than English so an Asian phishing site cannot be identified, according to the results done were gotten from only English data sets. And in the case of a false positive (legitimate web page that is detected as fake) a user will be misinformed. Another issue of this method is that it could suffer from performance problems due to the time lag involved in querying database, there were no experiments to represent timing.

3 Authentication System

3.1 One-Time Password

Here we evaluate in details the solution proposed by Huang et al (2011). Here they introduce a solution that eliminates the possibility of a user having a preset password by leveraging on existing infrastructure on the internet –specifically the instant messaging service. The study also shows that the solution can uniformly integrate with openID service which will enable websites that support openID use the solution. Huang (2011) believes that using content based approach is limited in solving the phishing attack on websites "List-based and heuristic-based methods cannot detect all phishing sites" Huang (2011, pp.1293) going

ahead to claim that heuristic-based mechanisms uses one criteria to assess web sites thereby bringing limitation for a list-based method to identify and prevent all phishing sites. Therefore claiming how possible it is to manage password phishing attack by delivering OTP via a secondary real-time channel also that this method is attack proof against IP-spoofing, safe authentication in an unfamiliar environment. In this solution a user is given a one-time new password every time the user wants to access the web. It was designed such that a trusted secondary channel will be needed to communicate the password, in this case the instant messaging service.

The one time password (OTP) will be communicated through a trusted secondary communication channel. There will be a user database in the server side and this will match with the user's matching identity on the secondary channel. Once person A wants to access a web service, an OTP is sent by the server to person A through the secondary channel. Person A is expected to use password within a space of time before it expires. One of the things the researchers claimed that is unique about this solution is that it provides three levels of security protection. An attack can occur only if the phisher knows I) account name; II) the secondary communication line were the user receives the OTP; III) password for secondary channel service. Huang et al (2011) decided to use instant message service as the best communication channel for the solution. This is majorly because it is cost effective as this can be downloaded and installed for free or is pre-installed on most operating systems e.g. Microsoft's messenger (Microsoft corporation) Generally the website will need to setup an identity management database and run an IM bot program to send the one-time password solution.

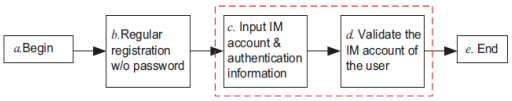


Figure 6

The user registration process, the areas marked in red rectangle are the extra steps required for this solution.

According to the researchers, for this solution to be implemented there are parties involved and assumptions used. For example it is assumed that the HTTP protocol for the IM is secure, this assumption is believed to be considerable (Huang, 2011) because a lot of commercial websites use the SSL protocol for encryption of HTTP. Another assumption was that the website has incorporated an instant messaging service. The user will have to install an (IM) service supported by the website. The parties involved are; websites, users, phishers and instant messaging (IM) service providers. There are two processes involved in this solution;

Registration Process

The registration is same with any other online registration process except for the two added section in order for the user to effectively use the solution. (as seen in Figure 7) Series of exchanges take place between the website. A) the page containing the IM account of the website and string *t* which is a session token with the space field were the OTP will be inputted B) If the account is new confirmation to add to database is obtained. C) When IM account is verified a message is sent to the user through the IM service. This message will contain the session token *t* and a one-time password *p.* (D) Finally the user confirms that IM account and token are same with previous page.

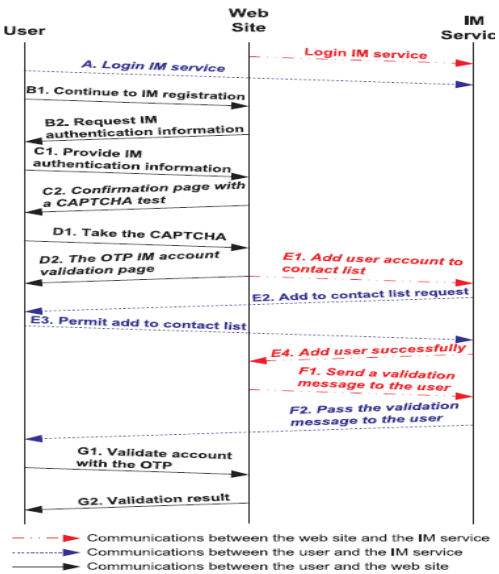


Figure 7: The instant messaging registration process

Login Process

As indicated in (figure 3) the login process comprises of five steps, A-E As an addition to the OTP field as requested by the website the page also contains a randomly generated session token *t* and the IP address used by the user. Once the account name is valid the website checks the user's IM account and sends an authentication message to the account. This message will contain the former generated session token *t* as well as the generated OTP *p* (In figure 4) shows a sample confirmation message. At the end of the process when the authentication message has been received the user can check the validity of this message by checking if the token *t* received by the IM client and the one shown on the OTP input page are same; If the user confirms the authentication message, the user supplies the OTP on the available OTP input page. When this is done the website has to confirm that the user has submitted the OTP from exactly the same IP address the user made a request to login from, then the website authenticates the user using the OTP entered if same as formerly assigned OTP i.e. if user enters *p'* in the password field of the input page, then the login will be successful if *p'* is the same as the OTP generated by the website. During the process of registration and login, the life span of the password is limited. This means that if a user inputs a wrong OTP more than a certain time *n* or a given OTP has not been used within *m* period of time, the website will invalidate the current password and stop process. In this case *n* has to be a very small number and *m* a short period of time for example *n=3* and *m=30s*. Additionally each OTP will comprise of a variety of letters including upper/lower case and numerals to reduce probability guessing.

Having evaluated the One-Time Password method (method 2) it is discovered that the OTP solution has a good mutual authentication feature were the server authenticates the user and the user authenticates the server. The OTP solution strength lies in the hidden relationships between three components and the fact that it is difficult (considering all assumptions made (Huang, 2011)) to compromise the components which are the user's account, the website's IM account and the user's Instant Messaging account. So claims made by Huang et al (2011) that the OTP solution can only be compromised if the attacker knows the components that are associated with each other and target them accordingly has no concrete evidence of implementation in the work done to prove this. The test method does not necessarily show that the method will always work on claims made also no substantial experiments where presented to considered the fact that the proposed solution can be compromised by the attacker if able to acquire the user's account name identity from a third party to log into the website and successfully making a user submit their OTP were is believed to be legitimate.

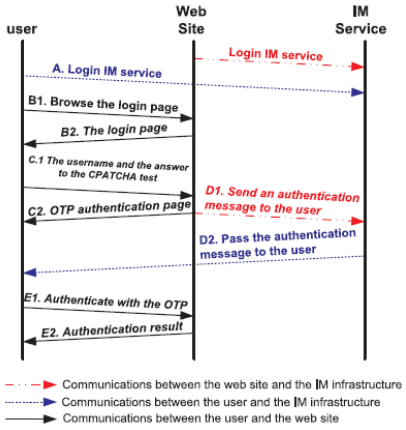


Figure 8: User login process

You have requested to log into the website holding the session token DwZ6EXgBREGT. You are connected from the IP address 11.22.33.44. Your pet's name is Max. Please log in with the one-time password gREduqmYz5QB.

Figure 9: Example of authentication message

4 Conclusions

In this paper we have carefully evaluated a web content based and one-time password anti-phishing solution. Although it may be impossible to completely wipe-out all phishing threats. The purpose of these solutions is to reduce the amount of phishing attack online. Having considered that the two major ways through which phishing attackers invade users are; having illegal authorisation into user account and deceptive website links. It would be recommended that using the automated webpage detector (method 1) as the major protection tool against phishing will be an effective way to

combat the phishing attack among businesses and social network sites. Based on the experiments carried-out on the webpage detector showing an average of 4-6% false positive which means that 1 out of every 10 phishing sites will be detected by the webpage detector as against the previous research done by (Zhang et al 2007) on phishing toolbar that uses the blacklist method showing a false positive of 15-20%. However the one-time password solution (method 2) compliments (method 1). If an attacker eventually succeeds in tricking a user into using a fake website, the authentication process will identify the phishing attack considering that the user will need to be assigned a one-time password after authentication confirmations are made from both ends. This method also has a reduced cost of deployment to almost zero by the installation of instant messaging bots at server side only.

References

Anti-phishing Working Group (APWG), 2011. APWG Phishing Trends Report. [Online] Available at: <http://www.antiphishing.org/phishReportsArchive.html> [Accessed 15 October 2011].

Cao Y., Han W., Le Y., 2008, 'Anti-phishing based on automated individual white-list', *Proceedings of the 4th ACM workshop on digital identity management*, [e-journal], pages 51, ISBN: 9781605582948. Available through: ACM Digital library [Accessed 10 October 2011].

Chen X., Bose I., Leung A. C. M., Guo C, 2011. 'Assessing the Severity of phishing attacks: A hybrid data mining approach', Decision Support Systems [e-journal], vol. 50, pages 662-672 ISSN: 01679236. Available through: Science Direct database [Accessed 11 October, 2011].

Cranor L., Egelman S., Hong J., Zhang Y., 2006, 'Phinding Phish: An Evaluation of Anti-Phishing Toolbars', CyLab Carnegie Mellon University Pittsburgh, [e-journal], Available through: CyLab Carnegie Mellon University digital library [Accessed 13 October, 2011.]

Gouda M. G., Liu A.X., Leung L.M., Alam M.A., 2007, 'An anti-phishing single password protocol', Computer Networks, [e-journal], Vol. 51, pages 3715 – 3726. Available through: Science Direct database [Accessed 2 November 2011].

He M., Horng S., Fan P., Khan M. K., Run R., Lai J., Chen R., Sutanto A., 2011, 'An efficient phishing webpage detector', Expert Systems with Applications, Vol. 38, Issue 10, pages 12018-12027, ISSN: 0957-4174.

Huang C., Ma S., Chen K., 2011, 'Using one time password to prevent one time phishing attacks', Journal of network and computer Applications, [e-journal], Vol. 34, pages 1292 – 1301. Available through: ACM Digital Library [Accessed 11 October 2011].

Kumaraguru P., Sheng S., Acquisti A., Cranor L.F., Hong J., May 2010 'Teaching Johnny not to fall for Phish', ACM Transactions on Internet Technology, [e-journal], Vol.10, Issue 2, Article 7, ISSN: 1533-5399. Available through: ACM Digital Library [Accessed 11 October, 2011].

Vishwanath A., Herath T., Chen R., Wang J., Rao H. R., 2011. 'Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model', Decision Support Systems [e-journal], Vol. 51, Issue 3, pages 576 – 586 Available through: ACM Digital library [Accessed 12 October, 2011].

Ye Z. (Eileen), Smith S., Anthony D., 2005, 'Trusted paths for Browsers', ACM Transactions on Information and System Security (TISSEC), Vol. 8, Issue 2, pages 153 – 186.

Zhang Y., Hong J., Cranor L., 2007. 'CANTINA: A Content-Based Approach to Detecting Phishing Web Sites', Proceedings of the 16th international conference on World Wide Web [e-journal], pages 638 – 648, ISSN: 978-1-59593-654-7. Available through: ACM Digital library [Accessed 11 October, 2011].

A Detailed Analysis of Current Biometric Research Aimed at Improving Online Authentication Systems

Daniel Brown

Abstract

One of the biggest problems with all online systems in this day and age, is security. Many security measures are implemented across various systems and throughout time we find that as technology advances, secure systems soon become exploited. In this paper the use of biometrics within online security will be analysed, looking at iris, fingerprint and facial recognition. From this, the efficiency and reliability of biometrics as an authentication method for online systems will be evaluated. The main vulnerabilities of biometric systems are how accurate this method is and the way in which data is transmitted from biometric devices to a secure authentication server. This paper looks at factors which could potentially affect the interpretation of key features by the biometric devices and will assess the overall security of biometric systems.

1 Introduction

For some time now, the technology industry has been searching for a method of security that will be impossible to compromise and with the integration of biometric systems into security we seemed to potentially have a solution. Already we have began to see biometric systems present in airports, in which your passport is scanned and vital measurements are taken such as the distance between several distinct features and Iris scanning takes place to verify the identity of the person standing before the system. It would seem impossible to deceive such systems however we cannot rule out the possibility that these systems are not 100% accurate and if they are not, what is the chance of a false rejection or even a false acceptance.

2 Biometric Systems

2.1 Fingerprint Recognition

Basic fingerprint security has been available for some time now, when it first appeared on popular products such as laptops it was seen as a gimmick and experienced difficulties with recognition. Users reported that they had set their fingerprint recognition yet when they attempted to unlock their system, it failed to recognise their fingerprint and other users experienced the opposite, in which they found other people could unlock their system. These systems have developed rapidly since this point and it is now a highly accurate authentication method as it is considered that no two fingerprints will ever be the same. Fingerprints are analysed based on certain patterns, there are three major patterns: loops (65%), whorls (30%) and arches (30%) (J.W. Osterburg et al. 1977).

The ridge lines present in a fingerprint will not change from birth until death therefore we can be sure that everyone has a unique fingerprint however we must determine every characteristic in each fingerprint to pinpoint what makes it unique to that person. These characteristics are named Galton characteristics after Sir Francis Galton who studied the individual characteristics within fingerprints. There are ten types of ridge lines within fingerprints which help with the characterisation of a fingerprint and these characteristics are analysed using grid over the fingerprint to help break down each section.

In a study (J.W. Osterburg et al. 1977) the probability of confirming an identity using a partial fingerprint is calculated, they display a

full table of probability values however do not conclude these findings in writing. They explain that naturally, there is a much lower chance of not being able to obtain a match in the database if only a partial print is given. Their research does not clearly state whether their results found the probability of confirming an identity to be less for a partial fingerprint in comparison to the full fingerprint although it is suggested throughout the paper.

2.2 Iris Recognition

Iris recognition is the latest biometric device to be implemented successfully into a full working environment, recently we have seen this technology added to airports as a passport control security feature. With the current level of security at such a high point throughout airports worldwide, it is fair to assume that a lot is resting on the shoulders of this particular system however you would expect that vast amounts of research have been done to conclude that this technology is suitable for this purpose. Similar to fingerprints, a human iris has a number of distinct features that make up a very complex pattern, these features include nerve rings, fibre thinning, pigment spots and other features (Rankin et al. 2011). Various factors need to be considered with iris scanning to ensure that an accurate image of the iris is extracted, as the human eye reacts accordingly to certain lighting then this could potentially affect the image that is extracted.

Low lighting is recommended as when there is a strain upon the eye, this is when we will see the image change. There should also be a certain point that each person should look at so that the device can obtain a consistent reading from the same angle each time, this also ensures that the most accurate reading can be taken each time. In a recent study (Rankin et al. 2011) it was found that the iris texture could be graded effectively into a manner in which the iris could be identified from finest to coarsest ranging from grade one to six respectively. This research was done to investigate whether the iris recognition system would fail over time as natural effects take their toll on the human iris and alter the way in which such a system would interpret the iris. In their investigations, they sampled images from 119 adults by capturing images of their iris from both left and right eyes. The adults that were tested were between the ages of 19 and 65. Binary iris codes were generated from features that had been extracted from the original iris images and then the binary codes are compared to see if they match. This calculation was done by using “a quantified dissimilarity measure called the Hamming Distance (HD)” (Rankin et al. 2011). From the comparison of the Hamming Distance, you can tell whether the patterns belong to the same iris. They obtained results which showed an overall recognition failure rate of 21% after sampling at 3 and 6 months where failures rates were 21.2% and 20.5% respectively. They conclude that as they only measured their results over a relatively short period for such a test, they could only predict that over time, rates of recognition failure will increase and that rates would vary depending on the value of the Hamming Distance. They discuss that if the Hamming Distance is set too low then users would experience an increased rate in failures whereas if it was set too high then there would be an increased chance of false positive results. At present, the only method of preventing failure caused by changes to the iris is to re-enrol the image of the iris into the system upon any changes however this method leaves the system vulnerable to security attacks.

2.3 Facial Recognition

Facial recognition systems consist of a soft and hard biometric system, both serving very different purposes. A soft biometric system will analyse features that are not unique to simply one person, they will be straight forward features that could apply to hundreds of thousands of people. Soft biometrics would not be used in a situation in which the security of a system should be strict, if personal details could be at risk or where an identity can be imitated. The features that are interpreted in soft biometric systems would be gender, eye colour, hair colour, skin colour, height and weight (Gian Luca Marcialis et al. 2009). Obviously there is a good chance that several people throughout the world will share all of the listed characteristics and therefore the system would be unable to identify one specific person. This means that the chance of unauthorised access is already above 0% which would be the target for any secure system.

Despite a serious lack of real security within soft biometrics in facial recognition, hard biometrics is right at the top of the current biometric security systems. As mentioned before with iris recognition systems being implemented within airports, facial recognition is also in place alongside previously mentioned systems. With security measures being so high, using multiple biometric systems together will ensure that the chance of a false acceptance or rejection is reduced wherever possible. Facial recognition systems look for unique characteristics just as all other systems, it will take measurements from vital points in a person's facial structure and compare it to measurements that it is currently reading from either a photograph or previous database entry.

3 Analysis of Current Research on Biometric Authentication Methods

A system must be found which is the most secure and efficient choice for online security, there will need to be a focus on what the probability of a mistake will be because in this day and age there is no room for error. A breach in security where IT systems are involved is considered a substantial failure because we have so much advanced technology available to us.

All of the biometric technology seems to provide excellent solutions for online security, for example fingerprints are unique to one person and they require no specific environment in order for the scan to take place due to the person having to physically interact with the scanner. In a study (J.W Osterburg et al. 1977) they discuss that the weakest fingerprint reading must have consist of 12 ridge endings and a partial fingerprint has a probability of around 20 (10^{-20}) of having 12 ridge endings. Therefore the probability of a false rejection in increased as the system would have less chance of matching the fingerprint. However it is safe to say that if the fingerprint scanner is used correctly and full fingerprint in taken then the room for error is very low.

Iris scanning is very similar in the way that a person's iris is unique to them and no one will ever have the same iris. Therefore it means that as long as the iris scan is interpreted by the system correctly then there will be no errors in identifying someone. In a recent study (Rankin et al. 2011) it is suggested that certain factors may affect the scanning of an iris such as the environment and how lighting can cause a strain on the human eye, causing the iris to dilate or contract to different angles and this would provide a different reading to other lighting levels. However the main, concern was not with getting the person into the correct environment, it was the concern that the human iris can be subject to change over time due to a number of factors.

In their research they found that a major factor that can affect the iris is ageing as well as medication, disease and surgery. The texture of the iris can cause a false reading if it changes from a previous reading, this is due to a change in the fibre pattern formation of the iris which eventually causes a variety of failure rates.

Facial scanning was either used as a soft or hard biometric system, however for the purpose of online security, it would appear that soft biometrics alone would not suffice. Soft biometrics may be useful to implement alongside another system as an extra measure of security, however with this system not being as advanced as others and you must expect that the system could be easily deceived. A hard biometric system could be used as a primary method of authentication for online security, due to its improved accuracy and interpretation of several key features of the human face.

By measuring vital features of a person's face it is possible to use these measurements to narrow down an identity search however there may be more than one person with the same measurements, meaning that the reading would not be able to match to a unique record such as a finger print or iris. It would be a great improvement to any of the proposed soft biometric methods but there would still question marks over how unique each of the characteristics are. As with the soft biometrics it may be a system that would be best used with another system, there is another factor that needs to be considered which is if there are any physical changes since their last scan. Weight loss, surgery or disease could cause a change in measurements which would be used to

determine whether the image matched who was meant to be gaining access to the system.

4 Conclusions

Biometrics within online security is without doubt the next step forward for many reasons, not only is there several biometric systems that could be implemented but it is truly an authentication method that is unique to one person. After analysing all of the systems in this paper, it is clear to see that still we can encounter problems with a system that would seem to be highly secure. Passwords are the current leading security method, almost every website has the option register and for this a password is required. This means that either people use the same password for everything which could lead to multiple accounts being compromised if that one password is revealed however having a separate password for each website could cause users to forget passwords. Passwords are easily compromised as they can be entered by anyone, obviously they need to obtain password first but there are methods of exploiting passwords so there is definitely a call for a new method of authentication.

Fingerprint recognition is a system that has already been implemented throughout many systems however reports suggest that false positives and negatives can occur with the system. The problem is however not with the system that reads the fingerprint as current research shows that it is highly accurate and comparison with database records is accurate and secure. The main problem seems to be with obtaining a full fingerprint scan when using the system, as research has shown, the probability of receiving a false reading is higher. This is a problem that could have a simple solution, if there was a method of securing the finger on the reader ensuring a full reading every time. If this could be done then there is no doubt that fingerprint recognition could be the leading biometric system for online security, we know that everyone has unique fingerprint pattern that will not change throughout their lifetime and therefore you can guarantee that whoever is authenticating, is actually the correct person.

Current research highlights what could be considered as major flaw in iris recognition systems in the way that the human iris changes throughout a person's lifetime and can be directly affected by other factors over time. It was found that the texture of the iris can change naturally as well as with the effects of medication therefore the system would fail to match the iris pattern with an image stored on a database. As mentioned, re-enrolling the iris into the database would currently be the only way in which the system would once again recognise that image and obviously re-enrolling regularly could present security issues as you would prefer not having to ever re-enrol an image. It is mentioned in the current research (Rankin et al. 2011) that if a more intelligent system which could deal with any physiological changes to the iris then it would be more accurate and would have less chance of being used for fraud. This statement is not suggesting that such system is currently being developed and from other research it appears that there are no current advances with this problem.

Facial Recognition was discussed as there are hard and soft biometric systems with this specific method, both of these are suitable for online security however both for different situations. Soft biometric systems are not reliable enough to be used as a primary authentication method especially where sensitive information could be in question. Soft biometrics could be used as an extra layer of security alongside another method such as passwords, if a user enters the correct password then the system will then check if the user has blonde hair, blue eyes and white skin for example. Hard biometrics could be used as a primary method of confirming an identity by confirming vital statistics of a user which would be unique to them. Obviously it is a possibility that someone else could share these features however it is highly unlikely that someone would share multiple and therefore you would have a unique profile.

To conclude, the biometrics systems available for use with online security all have problems, some more than others. More than anything, the situation must be considered and with online security we have to be thinking that this system can be used in a variety of situations ranging from professional to home use. Fingerprint recognition systems have a minor problem in

which a full fingerprint is not always obtained by the reader, this is a human error by not placing their finger correctly onto the reader however in comparison to iris recognition systems which are proved to fail over time. The other major problem with facial and iris technology is that in order to capture the quality of image needed to process iris and facial recognition you would need a good quality system in place with the correct conditions. In terms of home use, this would not be a viable option in the majority of cases. Therefore fingerprint recognition is the best suited system for online security across all of the possible situations as well as proving to have the least problems with accuracy.

References

D.M. Rankin, B.W. Scotney, P.J. Morrow, B.K. Pierscionek (2011). "Iris recognition failure over time: The effects of texture", *Pattern Recognition*, Volume 45, Issue 1, January 2012, Pages 145-150, ISSN 0031-3203.

Gian Luca Marcialis, Fabio Roli, Daniele Muntoni (2009). "Group-specific face verification using soft biometrics", *Journal of Visual Languages*, Volume 20, Issue 2, April 2009, Pages 101-109, ISSN 1045-926X.

James W. Osterburg, T. Parthasarathy, T. E. S. Raghavan and Stanley L. Sclove (1977). "Development of a Mathematical Formula for the Calculation of Fingerprint Probabilities Based on Individual Characteristics", *Journal of the American Statistical Association*, Vol. 72, No. 360 (Dec., 1977), pp. 772-778

L.H. Chan, S.H. Salleh and C. M. Ting (2010). "Face Biometrics Based on Principal Component Analysis and Linear Discriminant Analysis". *J. Comput.* Sci., 6 :Pg 693-699.

Marcos Martinez-Diaz, Julian Fierrez, Javier Galbally, Javier Ortega-Garcia (2011). "An evaluation of indirect attacks and countermeasures in fingerprint verification systems", *Pattern Recognition Letters*, Volume 32, Issue 12, 1 September 2011, Pages 1643-1651, ISSN 0167-8655.

Muhammad Khurram Khan, Jiashu Zhang, Khaled Alghathbar (2011). "Challenge-response-based biometric image scrambling for secure personal identification", *Future Generation Computer Systems*, Volume 27, Issue 4, April 2011, Pages 411-418, ISSN 0167-739X.

Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, Vijayakumar Bhagavatula (2011). "A pitfall in fingerprint bio-cryptographic key generation", *Computers & Security*, Volume 30, Issue 5, July 2011, Pages 311-319, ISSN 0167-4048.

Tassabehji, R.; Kamala, M.A. (2009). "Improving E-Banking Security with Biometrics: Modelling User Attitudes and Acceptance," *New Technologies, Mobility and Security (NTMS), 2009 3rd International Conference on* , vol., no., pp.1-6, 20-23 Dec. 2009

An Evaluation of Current Intrusion Detection Systems Research

Gavin Alexander Burns

Abstract

This paper is looking at a number of new research journals on the subject of Intrusion Detection Systems. This is a system that at present monitors for known attacks on the system, but current research is looking into ways to update the system to allow it to find unknown attacks as well. A number of papers, dating from 2006 to the newest 2011, on the subject were found some of which have been looked at in more detail within this paper. The information examined explored testing on a university's network, testing datasets, and re-examining past research information to underline comparisons with other systems that appear to do what they set out to do. The Intrusion Detection System found anomalies on the university network. One of the research papers showed that no testing had been done. What was found is that there is a lot of diverse research on this technology some really well carried out, but none that on their own will solve the problem. What did come to light was that more research and testing will be needed to have a truly standalone system but progress is being made.

1 Introduction

Intrusion Detection Systems (IDS) can be classed as another level of protection which can sit behind the firewall as a secondary form of protection. They are software applications that monitor the network looking for malicious activities and also policy violations and can also produce a log and report for the network administrators. There are various forms of research going on at present. There is the construction of lightweight IDS which will detect anomalies in networks (Siva et al. 2011). There is also research into Swarm Intelligence which is a new bio inspired method that has taken its inspiration from the way swarms of bees and other insects work (Kolias, et al. (2011). There is also (Fang-Yie Leu. et al. 2009) who are doing research into enhancing their previous grid-based intrusion detection system. Then there is the research by (Xenakis, Panos et al. 2010) who are looking into the evaluation of intrusion detection architectures for the mobile ad hoc networks. For this paper we will look at a number of different research journals and try to analyse their findings

2 ULISSE Anomaly detection with intelligence

Unsupervised Learning IDS with 2Stage Engine (ULISSE) is the start point which according to Zanero (2008) "It uses two tier architecture with unsupervised learning algorithms to perform network intrusion and anomaly detection. ULISSE uses a combination of clustering of packet payloads and correlation of anomalies in the packet stream." (Zanero, 2008)

This method has come about because of our use of complex networked computer systems in our everyday life. This dependence has brought about the need to make the networks we use more secure which is where it gets more complex. He also states that "The majority of network IDS systems deployed today are misuse-based" (Zanero, 2008) which in effect the IDS systems just sit and wait till a known signature of an intrusion type happens. Unfortunately this makes them ineffective against new attacks and a great number of evasion techniques. Which means these systems can give a lot of false negative and possibly false positives.

However using this misuse-based system on critical networks where the numbers of threats are increasing is not the best solution anymore which is why ULISSE has been developed. ULISSE is a Two Tier network based anomaly IDS system designed to analyze the network packets and avoid discarding its contents with the use of the two tiers first by reducing the packets payload to a more tractable size, then with a traditional anomaly algorithm. (Zanero, 2008)

Similar approaches are being used by Tajbakhsh et al. (2009) who were looking into using fuzzy association rules for their method of intrusion detection, and Kamran et al. (2009) who were looking into an adaptive genetic based learning system for detection systems. Both of their methods were using a two tier system.

2.1 Why is it different?

At present there is a need to look at the packet flow in order to undertake packet level network intelligence. The packet header data is dealt with easily as it is a uniform size and can be mapped to a time series, but problems occur when dealing with the payload data of the packet as they are of varying size.

This problem is over come by most of the existing research using unsupervised learning algorithms for the purpose of intrusion detection by dropping the payload data and only using the packet header information. This leads to the development of ULISSE as dropping the payload data looses information that is needed to detect most attacks as they are only detectable by analyzing this payload data.

ULISSE is proposed as a two tier architecture solution that applies a clustering algorithm to the payload data which allocates a single value to them which is then added to information from the header then passed on to the second tier which is an anomaly detection algorithm. (Zanero, 2008)

2.2 Testing

According to Zanero (2008) the tests seem to have been carried out in a well organised and controlled way. To evaluate ULISSE in a repeatable manner it was ran over various days of traffic taken from the 1999 DARPA dataset as well as adding attacks against the Apache web server and Samba service using Metasploit. The results compare well and indeed outperform the results given for SmartSifter and PAYL which are two other prototype intrusion detection systems which used the KDD Cup 1999 dataset which is derived from the 1999 DARPA dataset for their testing.

2.3 Conclusion

Although the tests seem to be a success the noticeable problem is that they are not a direct comparison tests as the same testing dataset has not been used even though it is stated that KDD Cup 1999 dataset is taken from the 1999 DARPA dataset that was used. Also it would be useful to investigate if there are any newer evaluation tests available which could give a more up to date image of current network traffic, although this does give the opportunity for the team or a new team to continue the research in the future.

3 HawkEye Solutions A Network Intrusion Detection System Abstract

HawkEye Solutions is the name given to the development group's network intrusion detection system. It is a basic system that detects abnormal internet protocol (IP) packets which they say is "the basic building blocks of an IDS that include mechanisms for carrying out TCP port scans, Traceroute scan, which in association with the ping scan can monitor network health." (Mukhopadhyay et al 2011)

What it is described as is a libpcap-based packet sniffer and logger which are made up of three primary subsystems which are packet decoder, detection engine, and logging and alerting. Some of its features are rule based logging which allows it to detect a number of different types of attacks. It also includes real time alerting with the alerts sent to syslog, popup messages, or an alert file, and its configuration is done though command line switches. (Mukhopadhyay et al 2011)

3.1 How it works

The system is similar in looks to its peers but has a greater focus on the security of packet sniffing with its most important features being packet payload inspection. This is where the application layer of the packet is decoded and rules can be given to collect specific data within the traffic which allows the system to detect many different types of unwanted activity. The other big advantage is that the output data is of a more user focused format. Hawkeye Solutions is also set to a working principle which is an eleven step by step guide on how the system is coded to work from the beginning of the event to the eventual conclusion (Mukhopadhyay et al. 2011)

3.2 Testing and Conclusion

There has been no definitive repeatable testing using a recognised dataset all that seems to have been done is they have set Hawkeye off on different types of scans then explained the outcome within the text of the paper. Also there is what they claim to be a comparison of what type of features Hawkeye has and can do compared against a number of other basic IDS systems and the results that they give come out in favour of the Hawkeye system. So with the evidence that is presented with in this paper it is quite evident that a lot more testing is needed before the Hawkeye Solutions system can be said to work.

4 Hybrid honeypot framework to improve intrusion detection

To some a honeypot is intended as a way to make attackers believe they are somewhere within your system when in reality they are in a controlled part of the system, but to others it is a form of technology for the detection of attacks or in some instances real computer systems that are designed to be hacked into so as to gain information from about the hacker and how to stop them in the future. Honeypots get classed into two wide categories production and research. Production honeypots are there to reduce an organizations risk by keeping them away from real system. Research honeypots are used for information collection. Honeypots are also classified by the level of interaction they allow with the attacker the more interaction there is the more information can be collected. Low interaction which most are virtual operating systems and services these are relatively simple to deploy but are easy to detect, and high interaction which are a development of real systems. The outline for the work undertaken in this journal is to use low interaction honeypots that emulate operating systems or services and pass malicious traffic on to high interaction honeypots to analyze an intruder's activity then results can be used to take measures to protect the network. They are using the honeypot technology to try to get around the inherent problems of the traditional intrusion detection systems. As honeypots can be used to lure hackers into a controlled environment to protect the real system resources and use the time to analyze their activities and how defend against it. (Artail et al 2006)

4.1 Proposed hybrid honeypot

Artail et al (2006) suggest proposing an intrusion detection system with an adaptable low interaction honeypot that can adjust to the changes in the network. They will be deployed though unused IP addresses on the network to help them blend in and look like the real operating systems and services around them. In most instances the traffic that is directed to the low interaction honeypots will be passed on seamlessly to high interaction honeypots. This combination has the advantage of requiring a minimum of administrative intervention as the number of honeypots adjusts automatically around the state of the network and available IP addresses. It also magnifies the high interaction honeypots with the redirection of the traffic from the low interaction honeypots which also helps make the low interaction honeypots look like real systems to anyone trying to hack the system.

The system will need to use static IP addresses and a relatively large number of free IP addresses are required as the more available free IP addresses the higher chance there will be to detect any intruders.

4.2 Testing and Results

The test of the hybrid system was carried out by integrating it into the network of the Faculty of

Engineering and Architecture at the American University of Beirut which had at least four hundred computers. Their initial scan of the network indicated that a significant number of the honeypot virtual systems could be used. They performed two sets of tests effecting 75 computers to get an understanding of the impact the scans can have on the network and the length of time they take.

The first test was an Nmap load test to measure the data collection performance of the system and what sort of effect it has on the network. The second set of tests, nesses tests, which is an open source vulnerability tester which subjects the system to simulated attacks as well as verifying the performance.

The tests lasted for over two weeks and came up with some interesting results; it detected a hacking activity through the logs generated by the low interaction honeypots. The hacker used an IP address of a computer that was known to not be used implying that the address was spoofed. The low interaction honeypot logs came up with a possible attack by showing that unused IPs were being scanned by a hacker using nmap, and the system helped detect the presence of the Natche virus on one of the machines. (Artail et al, 2006)

4.3 Conclusion

This research seems to be well thought out and set up their testing looks to be of a very high standard and although their main test will not be repeatable as no know standard testing dataset or systems were used, they have carried everything out on a real University system and it did come up with some good results. They are also aware that the system needs more time spent on it to develop it more and as such it cannot be discredited totally.

5 Conclusions

Currently there is no Intrusion Detection System that can fully protect network systems from unknown attacks which means that at present it is a make do system as the system has to be kept up to date with the known attack signatures to make sure the system is protected in the most efficient way. Unfortunately that means the network administrator may have to update the system on a daily basis, and that still will not be enough if an unknown attack signature happens as this will just get straight through without causing any alarm or log entry.

The research which has been looked at is very interesting in that it is looking at different ways to allow the network intrusion systems that are being developed and adapted to catch the unknown attacks and intrusions that can occur before they have appeared on any update database or software update as for them to appear on those someone has to detect them in the first place.

Generally the current research looked at was of a good standard, but unfortunately some as in the case of HawkEye Solutions has not got enough depth to it as they have done no known repeatable testing. On a positive outlook for HawkEye Solutions if extra research and development can be done and achieve the results which is hoped then it will be a much needed improvement over some of the systems that it was compared against.

With the research done into the ULISSE network detection system it looks very promising as their way of looking into the packets contents and not just discarding it can be looked at as a great improvement as it means there will not be as many dropped packets which can be used to detect any attacks earlier. Also what is promising is the two tier system that has an anomaly detection algorithm which will help with any new attacks that happen. The testing that was done was of a good standard with good recorded out comes.

The research carried out on the honeypot framework was also very interesting as this method will help to protect the systems very well as the attacks can be controlled as they are not on the actual system. The testing for the honeypots was of a high standard as they were done on an actual real world system and not just a test bed. If their results can be replicated elsewhere on other systems it will prove very promising.

One thing stands out with all this research is there is still a need for more research to solve problems within some of the research or to

improve it even more. One possible way to go could be to add different research together to see if two or more methods could get to the solution that is being looked for. A possible solution that has came about with this paper is the possible outcome of merging ULISSE system with the honeypot framework as it looks like they could be beneficial together as the honeypot could give ULISSE extra time to catch new attacks.

References

Artail H, Safa H, Sraj M, Kuwatly I, Al-Masri (2006) 'A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks.' *Computers & Security 25*, Pages 274-288

Fang-Yie Leu, Chao-Tang Yang, Fuu-Cheng Jiang (2010) 'Improving reliability of a Heterogeneous grid-based intrusion detection platform using levels of redundancies.' *Future Generation Computer Systems*, Volume 26, Issue 4, Pages 554-568

Kamran S, Hussein A A., (2009) 'An adaptive genetic-based signature learning system for intrusion detection.' *Expert Systems with Applications*, Volume 36, Issue 10, Pages 12036-12043

Kolias C, Kambourakis G., Maragoudakis M., (2011) 'Swarm intelligence in intrusion detection: A survey.' *Computers & Security*, Pages 1-18.

Mukhopadhyay I, Chakraborty M, Chakrabarti S., (2011) 'HawkEye Solutions: A Network Intrusion Detection System.' *International Conference and Workshop on Emerging Trends in Technology*, Pages 252-257

Siva S. Sivatha S, Geetha.S, Kannan. A, (2012) 'Decision tree based light weight intrusion detection using a wrapper approach.' *Expert Systems with Applications*, Volume 39, Issue 1, Pages 129-141

Tajbakhsh A, Rahmati M, Mirzaei A, (2009) 'Intrusion detection using fuzzy association rules.' *Applied Soft Computing 9*, Pages 462-469.

Xenakis C, Panos C, Stavrakakis I (2010) 'A comparative evaluation of intrusion detection architectures for mobile ad hoc networks.' *Computers & Security 30 (2011)*, Pages 63-80.

Zanero S. (2008) 'ULISSE, a Network Intrusion Detection System.' *CSIIRW '08 Cyber Security and Information Intelligence Research Workshop Oak Ridge, USA*, (May 2008)

An Analysis of Current Research on Quantum Key Distribution

Mark Lorraine

Abstract

This paper is an analysis of current Quantum Key Distribution research, asking whether the protocol has a place in the future of security.

1 Introduction

1.1 The Problem with Quantum Key Distribution

Quantum Key Distribution (QKD) is one of the few aspects of quantum computing to be not only physically realised, but ultimately commercially available. Magiq Technologies, founded in 1999, sells quantum hardware from www.magiqtech.com claiming that their commercial versions of QKD are unconditionally secure, as of this paper being written. For some time, QKD had been regarded as being impenetrable. However, recent studies have shown that QKD has flaws as a security system.

This paper will be looking at the more recent papers on QKD and discussing how secure QKD really is and if it has a long term place on the market.

1.2 What is Quantum Computing?

A quantum computer is a device which meets most, if not all, of the following criteria:

Be a scalable physical system with well-defined qubits
Be initializable to a simple fiducial state such as |000...>
Have much longer decoherence times
Have a universal set of quantum gates
Permit high quantum efficiency, qubit-specific measurements
(DiVincenzo, 2000)

A qubit is any item to which quantum physics applies which can have at least two different states. Usually, these are particles which are spun either on the x or y axis to emulate 1s and 0s which are used in classical computing.

1.3 What is QKD?

QKD is a security protocol which combines the classical idea of key distribution and one-time pads with elements of quantum mechanics which are supposed to lend themselves to complete security.

Currently, QKD is being used very sparingly, but there is a major QKD network used for the most important governmental and financial data transfers, which require the utmost security. This is a massive responsibility for QKD and if the total security of QKD starts to falter and turns out to be a facade, then it is only a matter of time before it falls out of favour, or worse still, is exploited.

2 An Analysis of QKD

2.1 A Brief Introduction to QKD

QKD is widely accepted to be unconditionally secure (Lo et al, 1999).

There are several QKD protocols, but the oldest and most developed is BB84, named after the two creators, Charles H. Bennett and Gilles Brassard and the year of its creation.

In the networking scenario displayed in Fig 1., using photon polarisation, Alice chooses a random string of bits to send to Bob and then randomly selects one of two basis supported by the protocol. The rectilinear basis has horizontal and vertical photons representing 0 and 1 respectively. Similarly, the diagonal basis has 45-degree and 135-degree photons representing 0 and 1 respectively.

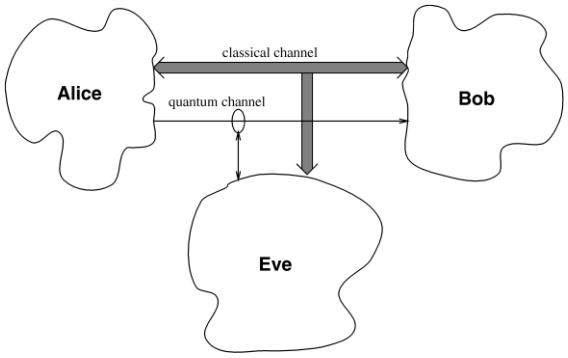


Figure 1. This shows a BB84 QKD network between two users, Alice and Bob, and Eve, who is an eavesdropper on the quantum channel. The quantum channel only transmits data in one direction, from Alice to Bob (Rieffel and Polak, 2000, p.307)

Once Alice has chosen a string and basis, the photon qubits are sent to Bob, via a one way quantum channel. Once Bob receives the qubits, he randomly, and independently of Alice decides to measure each qubit using a rectilinear or diagonal basis and interprets this back into binary. Attempting to read a rectilinear qubit using a diagonal basis will produce a random answer and all information is lost. Therefore, what Bob ends up with is meaningful data from the qubits he correctly guessed the basis for, which is on average, 50%.

After that, the remaining steps occur on the public channel. Bob and Alice determine which of the qubits were received successfully and correctly measured. Once the binary results have been verified by Alice, this becomes a key and is transmitted in small sections to make the results of potential interception negligible. A table of these steps is shown in Fig 2.

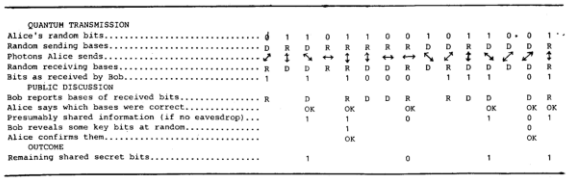


Figure 2. This table shows what actions are performed by Alice and Bob in the creation of the shared secret key. Note that, once the key has been generated, there is no further informtion on the quantum channel until all of the key has been used. (Bennett and Brassard, 1984, p.177)

If Eve tries to listen in on the quantum channel, because of the fact that you can't copy a quantum state, the mixed basis make it difficult to try to replicate the data reliably and send on to Bob without a high error rate (Bennett and Brassard, 1984 pp.175-178).

2.2 Discussing the Security of QKD

Bennett and Brassard's paper on QKD aimed to delve into the world of quantum mechanics to design a cryptographic system, creating a system on which it is theoretically impossible to eavesdrop. They decided to attempt to exploit the uncertainty principle in doing this. They proposed that current digital cryptography was flawed, as it cannot generate truly random numbers and that using quantum mechanics would also be a key advantage in this context.

Their idea was most certainly a very valid claim. This is the sort of thing that can have world-wide implications in the security industry. A definite break-through, built on the shoulders of previous research into making money which, in principle, cannot be counterfeited (Wiesner, 1981) and unforgeable subway tokens (Bennett et al, 1983). Both of these used quantum coding as a security measure. Cryptography is one of the many aspects of computing which is in a constant game of catch-up, with every new cryptographic method slowly sliding towards becoming obsolete. Hackers will always find a way around conventional classical security, because no computer generated number is ever truly random and it is only ever a matter of time

before the formula for generating it is calculated. Therefore, any progress towards a cryptographic method which would be impenetrable is an excellent idea. They do concede, however, that implementation of particles for data transfer is limited in practice because of how weak the signal has to be without any way to strengthen the signal.

Bennett and Brassard theorised that polarised light would be the form for their qubit to take. They reached this conclusion, because ordinary light is easily polarised by a filter, and the axis of the polarisation is determined by the orientation of the filter. Additionally, picking out a single polarised photon is also possible, simply by picking them from a polarised beam. They reason that while polarisation of a photon is a continuous variable, the uncertainty principle prevents more than one bit of data being obtained. Furthermore, polarised axes which are the same as the filter will always result in transmission and polarised axes which are perpendicular will definitely be absorbed. Any other value will randomly be transmitted or not. It is not possible to further measure axes, because after being transmitted, they will always have the same polarisation as the filter and because it is impossible to clone a quantum state reliably.

The beginnings of this element of their reasoning are logically sound. They put forward polarised light as their data transfer method and justify it well, highlighting the properties which make it well suited to the task. However, they do not compare using photons with using any of the other various particles which could potentially be put in their place.

Bennett and Brassard next moved onto the problem of cryptography. They proposed the idea of using a secure quantum channel to address the problem of secretly transferring a number for use in a one-time pad, or any other security application which require shared secret knowledge. They suggest that two users, Alice and Bob, should be connected by a quantum and a classical channel. A secret number can be generated over the quantum channel in such a way that there is a high probability that an eavesdropper (Eve) has disturbed the transmission. If the transmission is secure, then the shared secret is then used in whichever format is desired on the classical channel. If the transmission is not secure, then the outcome is discarded and the process repeated.

This is an excellent proposition for how to implement the secure quantum channel. The one-time pad is the most secure cryptographic method, but its big weakness is sharing a secret number before the encryption can begin. The combination of this cryptographic method with a quantum channel is therefore, theoretically completely secure. Additionally, the application of the convention of named users from cryptography, Alice, Bob and Eve, make the whole thing easier to follow.

Bennett and Brassard follow up their summary of how the quantum channel can be implemented alongside a classical one by going into more detail. They provide a detailed, step by step walkthrough of how Alice and Bob communicate over the quantum and classical channel to produce a shared secret key. (I again refer you Fig 2. which summaries this excellently.) They say that if an eavesdropper doesn't know the secret key after it has been generated, that they would have a minimal chance of being able to do any meaningful interception on the classical channel. An eavesdropper can prevent communication by suppressing either the classical or quantum channel, but this will not fool Alice or Bob into thinking the network is safe.

The protocols inner workings are obviously well reasoned out and do indeed create an unconditionally secure system. Also, the paper makes good use of tables to clarify and summarise the facts. The paper has no conclusion, only results of the logical reasoning. Reflecting on it from a current perspective, it reasonable to conclude that with the BB84 protocol having been conceived in theory, would have potential for error when practically implemented. It is logical that something created only as a concept should come across certain issues when it is first built. While minor improvements can be made to an idea before it is put into practice, it is only when it is truly tested by application of the idea that it can start to have its problems properly highlighted and addressed. As this is theoretical, the research

falls under the category of basic and the use of hard numbers means it is also quantitative.

It has been proven that it is possible to exploit the fact that a single-photon detector's pause after a detection event leave's it vulnerable to an attack without leaving any noticeable difference in the error rate (Weier et al, 2011). This research is valid, as QKD is used on a lot of high-security networks and any attacks on these networks should be addressed as soon as possible.

The paper claims that, using a standard BB84 protocol setup network, the single photon avalanche detector (SPAD) can be forced into dead time and effectively blinded, by well timed pulses sent by an eavesdropper.

This is an important idea being explored. If QKD is proven to have vulnerabilities, then it is important that they are addressed as quickly as possible if it is to have any long term presence as a high security product. It wouldn't take much to make people think twice about how many more weaknesses haven't been noticed yet after the first questions are raised about the no longer unconditional security QKD provides.

The paper goes on to discuss an experiment in which they used standard hardware found in almost all QKD networks and they also setup the pulse timing to a proper length for unbiased detections. They then proceed to use blinding pulses to blind the SPAD and while the SPAD is blinded, Eve can detect these instead without being noticed. After an attack, Eve then uses what she has learned about the secret key to decode information sent on the classical channel. The results are based on how well Eve can read the contents of the classical channel. After this, the experiment is repeated with increasing intensities of the blinding pulse and the results are compared.

This is a very fair and unbiased experimental method. It is also effective in getting to the nub of the issue, by actually having Eve listen in on the classical channel afterwards. If the experiment was limited to how much of the shared secret key Eve could discover, the results would be much more limited. It seems likely that each element was tested several times and that an average of the results was taken, but this is not specifically mentioned.

The outcome of the experiment shows that at the lowest pulse intensity, the classical channel's data was barely discernible from being random, but the best result demonstrated that 98.83% of the classical data could be correctly discerned (see impossible to eavesdrop. They decided to attempt to exploit the uncertainty principle in doing this. They proposed that current digital cryptography was flawed, as it cannot generate truly random numbers and that using quantum mechanics would also be a key advantage in this context.

Their idea was most certainly a very valid claim. This is the sort of thing that can have world-wide implications in the security industry. A definite break-through, built on the shoulders of previous research into making money which, in principle, cannot be counterfeited (Wiesner, 1981) and unforgeable subway tokens (Bennett et al, 1983). Both of these used quantum coding as a security measure. Cryptography is one of the many aspects of computing which is in a constant game of catch-up, with every new cryptographic method slowly sliding towards becoming obsolete. Hackers will always find a way around conventional classical security, because no computer generated number is ever truly random and it is only ever a matter of time before the formula for generating it is calculated. Therefore, any progress towards a cryptographic method which would be impenetrable is an excellent idea. They do concede, however, that implementation of particles for data transfer is limited in practice because of how weak the signal has to be without any way to strengthen the signal.

Bennett and Brassard theorised that polarised light would be the form for their qubit to take. They reached this conclusion, because ordinary light is easily polarised by a filter, and the axis of the polarisation is determined by the orientation of the filter. Additionally, picking out a single polarised photon is also possible, simply by picking them from a polarised beam. They reason that while polarisation of a photon is a continuous variable, the uncertainty principle prevents more than one bit of data being obtained. Furthermore, polarised axes

which are the same as the filter will always result in transmission and polarised axes which are perpendicular will definitely be absorbed. Any other value will randomly be transmitted or not. It is not possible to further measure axes, because after being transmitted, they will always have the same polarisation as the filter and because it is impossible to clone a quantum state reliably.

The beginnings of this element of their reasoning are logically sound. They put forward polarised light as their data transfer method and justify it well, highlighting the properties which make it well suited to the task. However, they do not compare using photons with using any of the other various particles which could potentially be put in their place.

Bennett and Brassard next moved onto the problem of cryptography. They proposed the idea of using a secure quantum channel to address the problem of secretly transferring a number for use in a one-time pad, or any other security application which require shared secret knowledge. They suggest that two users, Alice and Bob, should be connected by a quantum and a classical channel. A secret number can be generated over the quantum channel in such a way that there is a high probability that an eavesdropper (Eve) has disturbed the transmission. If the transmission is secure, then the shared secret is then used in whichever format is desired on the classical channel. If the transmission is not secure, then the outcome is discarded and the process repeated.

This is an excellent proposition for how to implement the secure quantum channel. The one-time pad is the most secure cryptographic method, but its big weakness is sharing a secret number before the encryption can begin. The combination of this cryptographic method with a quantum channel is therefore, theoretically completely secure. Additionally, the application of the convention of named users from cryptography, Alice, Bob and Eve, make the whole thing easier to follow.

Bennett and Brassard follow up their summary of how the quantum channel can be implemented alongside a classical one by going into more detail. They provide a detailed, step by step walkthrough of how Alice and Bob communicate over the quantum and classical channel to produce a shared secret key. (I again refer you Fig 2. which summaries this excellently.) They say that if an eavesdropper doesn't know the secret key after it has been generated, that they would have a minimal chance of being able to do any meaningful interception on the classical channel. An eavesdropper can prevent communication by suppressing either the classical or quantum channel, but this will not fool Alice or Bob into thinking the network is safe.

The protocols inner workings are obviously well reasoned out and do indeed create an unconditionally secure system. Also, the paper makes good use of tables to clarify and summarise the facts. The paper has no conclusion, only results of the logical reasoning. Reflecting on it from a current perspective, it reasonable to conclude that with the BB84 protocol having been conceived in theory, would have potential for error when practically implemented. It is logical that something created only as a concept should come across certain issues when it is first built. While minor improvements can be made to an idea before it is put into practice, it is only when it is truly tested by application of the idea that it can start to have its problems properly highlighted and addressed. As this is theoretical, the research falls under the category of basic and the use of hard numbers means it is also quantitative.

It has been proven that it is possible to exploit the fact that a single-photon detector's pause after a detection event leave's it vulnerable to an attack without leaving any noticeable difference in the error rate (Weier et al, 2011). This research is valid, as QKD is used on a lot of high-security networks and any attacks on these networks should be addressed as soon as possible.

The paper claims that, using a standard BB84 protocol setup network, the single photon avalanche detector (SPAD) can be forced into dead time and effectively blinded, by well timed pulses sent by an eavesdropper.

This is an important idea being explored. If QKD is proven to have vulnerabilities, then it is

important that they are addressed as quickly as possible if it is to have any long term presence as a high security product. It wouldn't take much to make people think twice about how many more weaknesses haven't been noticed yet after the first questions are raised about the no longer unconditional security QKD provides.

The paper goes on to discuss an experiment in which they used standard hardware found in almost all QKD networks and they also setup the pulse timing to a proper length for unbiased detections. They then proceed to use blinding pulses to blind the SPAD and while the SPAD is blinded, Eve can detect these instead without being noticed. After an attack, Eve then uses what she has learned about the secret key to decode information sent on the classical channel. The results are based on how well Eve can read the contents of the classical channel. After this, the experiment is repeated with increasing intensities of the blinding pulse and the results are compared.

This is a very fair and unbiased experimental method. It is also effective in getting to the nub of the issue, by actually having Eve listen in on the classical channel afterwards. If the experiment was limited to how much of the shared secret key Eve could discover, the results would be much more limited. It seems likely that each element was tested several times and that an average of the results was taken, but this is not specifically mentioned.

The outcome of the experiment shows that at the lowest pulse intensity, the classical channel's data was barely discernable from being random, but the best result demonstrated that 98.83% of the classical data could be correctly discerned (seeimpossible to eavesdrop. They decided to attempt to exploit the uncertainty principle in doing this. They proposed that current digital cryptography was flawed, as it cannot generate truly random numbers and that using quantum mechanics would also be a key advantage in this context.

Their idea was most certainly a very valid claim. This is the sort of thing that can have world-wide implications in the security industry. A definite break-through, built on the shoulders of previous research into making money which, in principle, cannot be counterfeited (Wiesner, 1981) and unforgeable subway tokens (Bennett et al, 1983). Both of these used quantum coding as a security measure. Cryptography is one of the many aspects of computing which is in a constant game of catch-up, with every new cryptographic method slowly sliding towards becoming obsolete. Hackers will always find a way around conventional classical security, because no computer generated number is ever truly random and it is only ever a matter of time before the formula for generating it is calculated. Therefore, any progress towards a cryptographic method which would be impenetrable is an excellent idea. They do concede, however, that implementation of particles for data transfer is limited in practice because of how weak the signal has to be without any way to strengthen the signal.

Bennett and Brassard theorised that polarised light would be the form for their qubit to take. They reached this conclusion, because ordinary light is easily polarised by a filter, and the axis of the polarisation is determined by the orientation of the filter. Additionally, picking out a single polarised photon is also possible, simply by picking them from a polarised beam. They reason that while polarisation of a photon is a continuous variable, the uncertainty principle prevents more than one bit of data being obtained. Furthermore, polarised axes which are the same as the filter will always result in transmission and polarised axes which are perpendicular will definitely be absorbed. Any other value will randomly be transmitted or not. It is not possible to further measure axes, because after being transmitted, they will always have the same polarisation as the filter and because it is impossible to clone a quantum state reliably.

The beginnings of this element of their reasoning are logically sound. They put forward polarised light as their data transfer method and justify it well, highlighting the properties which make it well suited to the task. However, they do not compare using photons with using any of the other various particles which could potentially be put in their place.

Bennett and Brassard next moved onto the problem of cryptography. They proposed the

idea of using a secure quantum channel to address the problem of secretly transferring a number for use in a one-time pad, or any other security application which require shared secret knowledge. They suggest that two users, Alice and Bob, should be connected by a quantum and a classical channel. A secret number can be generated over the quantum channel in such a way that there is a high probability that an eavesdropper (Eve) has disturbed the transmission. If the transmission is secure, then the shared secret is then used in whichever format is desired on the classical channel. If the transmission is not secure, then the outcome is discarded and the process repeated.

This is an excellent proposition for how to implement the secure quantum channel. The one-time pad is the most secure cryptographic method, but its big weakness is sharing a secret number before the encryption can begin. The combination of this cryptographic method with a quantum channel is therefore, theoretically completely secure. Additionally, the application of the convention of named users from cryptography, Alice, Bob and Eve, make the whole thing easier to follow.

Bennett and Brassard follow up their summary of how the quantum channel can be implemented alongside a classical one by going into more detail. They provide a detailed, step by step walkthrough of how Alice and Bob communicate over the quantum and classical channel to produce a shared secret key. (I again refer you Fig 2. which summaries this excellently.) They say that if an eavesdropper doesn't know the secret key after it has been generated, that they would have a minimal chance of being able to do any meaningful interception on the classical channel. An eavesdropper can prevent communication by suppressing either the classical or quantum channel, but this will not fool Alice or Bob into thinking the network is safe.

The protocols inner workings are obviously well reasoned out and do indeed create an unconditionally secure system. Also, the paper makes good use of tables to clarify and summarise the facts. The paper has no conclusion, only results of the logical reasoning. Reflecting on it from a current perspective, it reasonable to conclude that with the BB84 protocol having been conceived in theory it would have potential for error when practically implemented. It is logical that something created only as a concept should come across certain issues when it is first built. While minor improvements can be made to an idea before it is put into practice, it is only when it is truly tested by application of the idea that it can start to have its problems properly highlighted and addressed. As this is theoretical, the research falls under the category of basic and the use of hard numbers means it is also quantitative.

It has been proven that it is possible to exploit the fact that a single-photon detector's pause after a detection event leave's it vulnerable to an attack without leaving any noticeable difference in the error rate (Weier et al, 2011). This research is valid, as QKD is used on a lot of high-security networks and any attacks on these networks should be addressed as soon as possible.

The paper claims that, using a standard BB84 protocol setup network, the single photon avalanche detector (SPAD) can be forced into dead time and effectively blinded, by well timed pulses sent by an eavesdropper.

This is an important idea being explored. If QKD is proven to have vulnerabilities, then it is important that they are addressed as quickly as possible if it is to have any long term presence as a high security product. It wouldn't take much to make people think twice about how many more weaknesses haven't been noticed yet after the first questions are raised about the no longer unconditional security QKD provides.

The paper goes on to discuss an experiment in which they used standard hardware found in almost all QKD networks and they also setup the pulse timing to a proper length for unbiased detections. They then proceed to use blinding pulses to blind the SPAD and while the SPAD is blinded, Eve can detect these instead without being noticed. After an attack, Eve then uses what she has learned about the secret key to decode information sent on the classical channel. The results are based on how well Eve can read the contents of the classical channel. After this, the experiment is repeated with

increasing intensities of the blinding pulse and the results are compared.

This is a very fair and unbiased experimental method. It is also effective in getting to the nub of the issue, by actually having Eve listen in on the classical channel afterwards. If the experiment was limited to how much of the shared secret key Eve could discover, the results would be much more limited. It seems likely that each element was tested several times and that an average of the results was taken, but this is not specifically mentioned.

The outcome of the experiment shows that at the lowest pulse intensity, the classical channel's data was barely discernable from being random, but the best result demonstrated that 98.83% of the classical data could be correctly discerned (see Fig 3.)

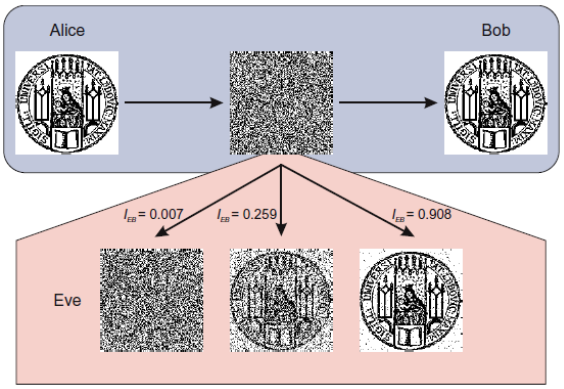


Figure 3. This image shows examples of increasing intenstity using blinding pulses to attack the quantum channel in a QKD network. It is clear that, there is a significant amount of data intercepted at the highest intensity (Weier et al, 2011, p.8)

This falls in line with the predictions that were made, with the exception of some of the higher values not quite matching up in real life because of the greater chance of interference caused by generating the more intense pulses. To conclude, they point out that the attack is currently potent and applies to the vast majority of QKD networks. Its strengths are in how easy it is to perform. However, the ease of implementation also leads to an ease of detection. If Bob checks for detection events outside of the pulse timing that Alice is sending with, then they are probably a pulse attack. However, Eve can instead send blinding pulses at random times during the window in which Alice's pulses arrive and simulate background noise. They suggest a more efficient countermeasure would be to monitor the voltage of the SPAD to be sure there is nothing malicious going on.

This outcome is a good and unbiased interpretation of the results and it is always most useful to see a security breach with a well reasoned idea to patch the security hole. This vulnerability is a significant one, and until it is countered by adding new elements to the standard QKD networks, there is definitely a real threat. The paper uses an actual scientific experiment generating hard data to reach its conclusions and therefore falls under applied and quantitative research.

(Wang et al, 2009) Proposes that is possible to perform a man-in-the-middle attack on the BB84 protocol. Again, much like Weier's paper, this is a valid research topic, as it deals with a threat to QKD, which has a lot of security responsibility and finding and stopping exploits is important.

They say this attack would involve a malicious Mallory, in place of the eavesdropping Eve, intercepting the secure quantum messages between Alice and Bob. To do this, Mallory must place herself in between Alice and Bob on the quantum channel. When Alice sends Bob the first random bits with their random polarisations, Mallory intercepts this and sends a separate random set of bits with random polarisations to Bob. Bob then replies with the series of detectors he randomly selected and sends this information to Alice, but again, this is intercepted and Alice is sent Mallory's detector information instead. At this point, Bob and Alice only keep the bits that were properly detected and therefore have two different secret keys. Finally, Bob and Alice send each other part of their key and verify that they match, in order to be sure there were no eavesdroppers. At this point, Mallory can receive Alice's key bits and confirm Mallory's with Bob. Then Mallory confirms Alice has the correct code. At this point, they will start to use the shared secret on the classical channel and Mallory can

intercept data from one user, decrypt it and encrypt it with the other key before sending it to the other user.

If this is true, then it would be a severe threat to the security of QKD. However, while there is no reason to doubt that it is possible to perform a man-in-the-middle attack like this one, it is not proven either by backing it up with existing evidence, or demonstrating any sort of experiment.

The paper continues to discuss means of preventing man-in-the-middle attacks on a quantum system. It claims the core of this problem is not being able to verify who the users are communicating with. It then lists a number of possible solutions. First, they suggest that digital certificates could be used, to verify the authenticity of a sender. Secondly, they recommend using a secure key to encrypt the authentication message with. Thirdly, they put forward the idea of using Einstein-Podolsky-Rosen pairs, being shared between Alice and Bob. Alice would send her pairs with the very first set of random bits and tell Bob which is entangled. Bob would then detect the interrelated pairs and see if there is correlation. The next option would be to check that Alice and Bob's completed shared secrets match by sending then by phone or email, which is at lower risk of interception. Alternatively, the shared keys could be compared on the classical channel. Finally, they mention that a man-in-the-middle attack is difficult to practically implement, because information is difficult to intercept at each stage. If anything is not intercepted, it is possible that the attack will be discovered and the key discarded.

Once again, while these claims seem to make sense, they are not backed up by any evidence. Furthermore, there are elements which are written in such bad English that it is difficult, or impossible, to make useful sense of.

The paper concludes by saying that QKD is vulnerable to man-in-the-middle attacks, but could be protected from this by introducing elements of classical cryptography. It also suggests it might be possible to include other elements of quantum cryptography, like security based on Quantum non-cloning theorem or the uncertainty theory. They also mention that Quantum non-cloning theorem has a big role in quantum computing, but has been truly proven, because research cannot claim that there is no way of cloning at all. They make a comparison to human beings, and that before discovering the gene, nobody would have said human cloning was possible. They say it may be possible to, in the future, discover a quantum gene, which will allow us to clone quantum states, at which point, the security of QKD would be severely threatened.

They have not come up with a strong conclusion or with any discernible new knowledge in this paper, the whole paper is a list of events, without any proof that any of the elements core to the title, 'Man-in-the-middle Attack on BB84 Protocol and is Defence'. There are six references in the paper, two are on QKD in general and feature in the introduction, while the other four are in the conclusion, and two of those are on quantum non-cloning. The introduction of Quantum non-cloning into the paper was a deviation and bears no relation to the title. The paper skips from the introduction, to the attack and defence of man-in-the-middle, and finally to the conclusion. In general, this paper seems thin on useful information and none of what it claims is proven by referencing or by experiment. This paper technically falls into a basic approach to research, in that there is no physical testing, however there are no examples of quantitative nor qualitative research at any point.

3 Conclusions

Bennett and Brassard's paper on QKD is a well written concept, and while it may not live up to the idea of unconditional security in reality as well as it does in theory, it is at least providing a platform for securing further against attacks. It is unlikely that the authors envisaged a time where there protocol would be fully realised and implemented.

The papers of Weier and Wang both put forward problems within a QKD system, which can be exploited, but more importantly, protected against. Both of their topics have equal validity, but only Weier really seemed to do the title justice. Additionally, Weier's

contribution has a more feasible problem to discuss, and has a problem which is put into context with evidence.

Weier's research has a fair and un-biased experiment, which has relevant results, while Wang has no experiment. While, they cover different enough topics that both of their suggestions to solve the issues they covered could be implemented together, this still leaves the concern that one might question implementing the man-in-the-middle protection based on a lack of evidence.

In the context of the commercial side of QKD, the idea that QKD was unconditionally secure was the biggest draw, and this is no longer true. It was probably not a good idea to herald a new era of complete security so quickly, without giving it a chance to be properly tested. Obviously, the holes in the QKD network can be patched, but ultimately, now that there have been successful breaches, it is highly likely there will be more, based on the common trends in classical security. Certainly QKD is not a bad security protocol, as it is a very specialist attacker who has the tools and ability to hack a QKD system. This is the most significant redeeming quality of the network at the moment.

The real question is, how long will it be before hackers either start to learn the elements of the security system well enough to perform an attack? Or how long before someone who already has this knowledge is lured by greed or bribery or force to attack a QKD network? This is a real unknown. Despite all of QKD's problems, it remains secure more out of ignorance than out of it putting up a good defence. The only thing that is for certain is that it will not stay this way forever.

References

Bennett, C.H. and Brassard, G. (1984) 'Quantum cryptography: Public key distribution and coin tossing' *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, Bangalore India, December, pp.175-179

Bennett, C.H., Brassard, G., Breidbert, S. and Weisner, S. (1983) 'Quantum Cryptography, or Unforgeable Subway Tokens' *Advances in Cryptography: Proceedings of Crypto 82 Plenum (New York)*, pp.267-275

Lo, Hoi-Kwong and Chau, H.F. (1999) 'Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances' *Science* Vol. 283, pp.2050-2056

Rieffel, E. and Polak, W. (2000) 'An introduction to quantum computing for non-physicists' *ACM Computing Surveys*, Vol. 32, pp.300-335,2000

Wang, Y., Wang, H., Li, Z. and Huang, J (2009) Computer Science and Information Technology, 2nd IEEE International Conference on 2009, pp. 438-439.

Weier, H., Krauss, H., Rau, M., Furst, M., Nauerth, S., Weinfurter, H. (2011) 'Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors' New Journal of Physics vol. 13

Wiesner, S. (1983)'Conjugate coding', *Sigact News*, vol. 15, no. 1, pp. 78 - 88

A Critical Review of Current Distributed Denial of Service Prevention Methodologies

Paul Mains

Abstract

This research paper is in the field of improving online security. It will be narrowing the focus on defending against distributed denial of service attacks. This is a well-documented area with high profile attacks perpetrated by 'hacktivist' group 'anonymous' and mischief makers 'lulzsec'. These aren't the only groups or individuals that attempt these attacks. Anyone with the ability to download simple software packages like the 'Low Orbit Ion Cannon' can execute an attack at a web server or someone's internet connection. That is the main obstacle to overcome that the attacks can be made so simple that any Joe Blogs can participate in a mass illegal destructive activity. There are more advanced approaches that are harder to predict. It could be the more advanced 'High Orbit Ion Cannon' package or the manipulation of the 'Conficker' virus. A DDoS can even be produced by a single individual manipulating a distributed hash table directing a massive amount of traffic towards a target. How these attacks can be avoided will be the focus of this research paper. Attention will be around 'Genetic Algorithms', 'Neural Classifiers', 'P2P defending' and how to defend the future of cloud computing from the frustrations of DDoS attacks.

1 Introduction

One of the most well-known approaches to antagonise a person (a person using a computer that is) from a significant distance away is to undertake a DoS or DDoS attack against them. This is starting to move over to the newer sensation called RefRef, but we'll only concentrate on the DDoS problem. The biggest problem is that DDoS is not produced from a highly refined complicated methodology, it is a simple crude annoyance distributed to people with no substantial hacking skills, therefore easy to undertake. So why hasn't this issue not been handled yet? Well technically DDoS is just one of many approaches being utilised, but none of the other approaches are considered to be impressive or even remotely complex either.

"The low level of skills displayed is a worry in itself. If hacktivists are achieving this level of mayhem, imagine what real hackers might do." (Mansfield-Devine 2011). The damage these people inflict is difficult to measure but side effects of having a weapon so easily obtainable can be easily facilitated to dark acts. Having a system vulnerable to such a basic attack causes damage in many ways.

- Loss of money
- Invasion of privacy
- Loss of time
- Mental anguish
- Increase in Crime

(Kim et al. 2011)

In 2004 the ground work was already set in the paper "A taxonomy of DDoS attack and DDoS defense mechanisms" (Jelena & Reiher 2004). It has been 7 years since that research was carried out and it is now time to see where the research has progressed.

2 DDoS Prevention Research

In this area research papers will be analysed in the field of DDoS prevention. 4 Papers have

been chosen to be the focus of the investigation. These will be critically evaluated to determine the knowledge behind the approaches. The 4 areas are covered in the following research papers:

- "Detection of DDoS attacks using optimized traffic" (Lee et al. 2011)
- "Distributed denial of service attack detection using an ensemble of neural classifier" (Kumar & Selvakumar 2011)
- "Preventing DDoS attacks on internet servers exploiting P2P systems" (Sun et al. 2010)
- "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks" (Chonka et al. 2011)

2.1 Traffic Matrix

The research by (Lee et al. 2011) is an applied quantitative piece of research dedicated to the goal of the detection of DDoS attacks. It continues on from the previous work "Detecting DDoS attacks using dispersible traffic matrix and weighted moving average" this is a heavily mathematical driven approach to a network security issue.

Analysis

The problem that it is trying to tackle is the rise in DDoS threats effecting networks. It clearly identifies the different fields of DDoS defence. "Defense mechanisms against DDoS attacks to cope with them can be classified into four categories: prevention, detection, mitigation and response." (Lee et al. 2011) This research project is designed to detect the anomalies that indicate a DDoS attack is occurring. They verify their approach by undertaking an experiment and analyses process. The tests that are performed involve the use of advanced mathematical data sets. The research from a graphical perspective is quite revealing. What the experiment is exploring is the validity of the equation below.

$$V = \frac{1}{k}\sum_{j=0}^{n}\sum_{i=0}^{n}(M_{(i,j)} - \mu)^2, \quad \text{if } M_{(i,j)} \neq 0$$

$$\text{where, } \mu = \frac{1}{k}\sum_{j=0}^{n}\sum_{i=0}^{n}(M_{(i,j)})^2, \quad \text{if } M_{(i,j)} \neq 0$$

Figure 1 Variance Equation (Lee et al. 2011)

That is what is made to identify the variance which is value 'V'. Basically if V exceeds the designated threshold the system is alerted to this occurrence. This is then identified as an anomaly and the mass generation of these anomalies aided by visual referencing is the detection measure. The steps are illustrated below.

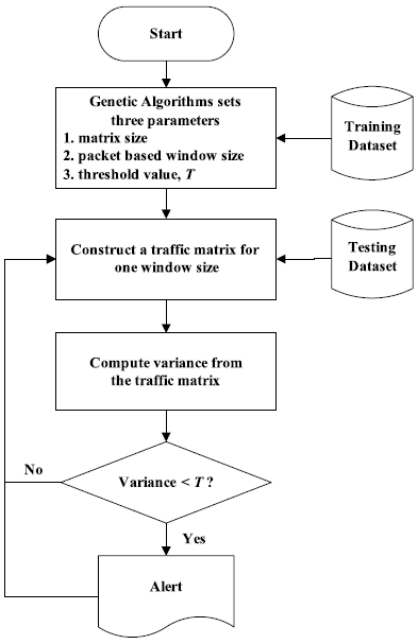


Figure 2 Overall flow of proposed model (Lee et al. 2011)

The approach does in fact display a visual aid to identify when the attack takes place. This is illustrated in the diagram on the next page which identifies the difference between a normal set of traffic results and a set of DDoS attack results.

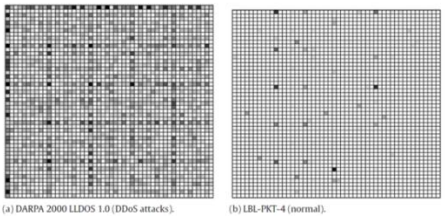


Figure 3 Visualisation results of traffic matrix (Lee et al. 2011)

The image above identifies the difference between a DDoS attack and a normal trend of traffic. How the normal traffic is scaled is not made apparent, whether that is an operation intensive network or if it is a particular calm timeframe. Seeing how this matrix is identifying anomalies it may not be important, but could be elaborated upon in further research to find the limits of its capabilities. Another feature of further research could be in the format of the IP addresses used. "We converted these sanitized source IP addresses to Ipv4 format, since our proposed model needs Ipv4 format as source IP addresses to construct a traffic matrix." (Lee et al. 2011) Now that the experiment has produced results to be analysed it could progress to new environments to test the limits of this approach. This may warrant testing it in tandem with the IPv6 format.

Conclusion

The quantitative method of research displayed here is appropriate for the desired result. The resulting data sets do illuminate the success of the theory discussed prior.

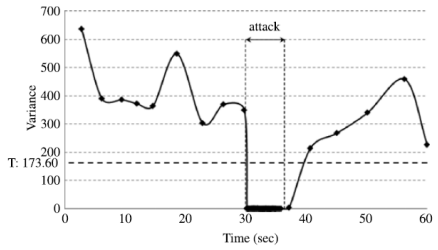


Figure 4 DARPA 2000 LLDOS 1.0 with LBL-PKT-4 (Lee et al. 2011)

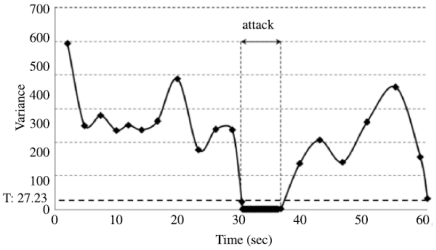


Figure 5 16 bit subnet spoofed attack with LBL-PKT-4 (Lee et al. 2011)

The graphs above display how the traffic matrix detects the DDoS successfully. The method is described as having a low amount of computational overhead and must have a minimal detection delay while producing high detection results. The way the experiment is conducted displays the trend between low overheads and high rate of detection. So the statistical evidence proves the authors proposed detection model has achieved its goal. The only thing to be raised is how it compares to other methodologies in this field. There is a neural classifier approach that I will use to compare this approach with. But as it stands now the detection model has reliably informed the reader of its inception and practicality and then justified through experimental trial. "We showed that our proposed approach satisfies the major requirements of the detection approach such as low processing overheads, short detection delay, and high detection rates" (Lee et al. 2011) How this is implemented into real world situations hasn't been experimented on as far as it has been covered in this research paper. A passing comment in the conclusion says that it is easily done, and elaborates slightly on how this can be done but as far as can be read it hasn't gone through a thorough testing phase. "our model can be used in a real-time network environment and it can be implemented easily" (Lee et al. 2011) It would be interesting to see how this approach fits with other detection models and security packages, whether it could be implemented into an operational security policy or not.

2.2 Neural Classifier

The research by (Kumar & Selvakumar 2011) is an applied quantitative piece of research, dedicated to improving the detection rate of

DDoS attacks by reducing the amount of false alarms. This is targeted at the network security audience that wish to progress their defences against resource draining attacks. This is also a method built primarily to detect attacks rather than prevent or respond.

2.2.1 Analysis

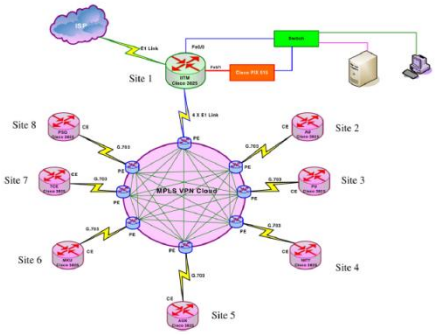


Figure 6 SSE environment (Kumar & Selvakumar 2011)

This method triggers an alarmed state that communicates to other machines on that security network. This is a method that is already implemented and the focus of the research is to improve it by modifying the mathematical side. The obstacle at hand is to decipher what is malicious traffic and what is safe traffic. "Real Challenge lies in distinguishing the flooding attacks from abrupt change in legitimate traffic." (Kumar & Selvakumar 2011) This is the main focus of what the algorithm is designed to achieve. It is created to differentiate between various kinds of traffic, by training the classifier to recognise current signatures and learn new traffic trends that can be gauged as a threat. How the method is implemented is illustrated on the top right of this page, the diagram at the start of this analyses section displays how it appears on a large scale. It is examined on a large distributed network and it is this large to give the method as much training data as possible. It is also useful as the experiments can be analysed in the larger context of the whole network or minimised to see how it operates at its smallest computational level.

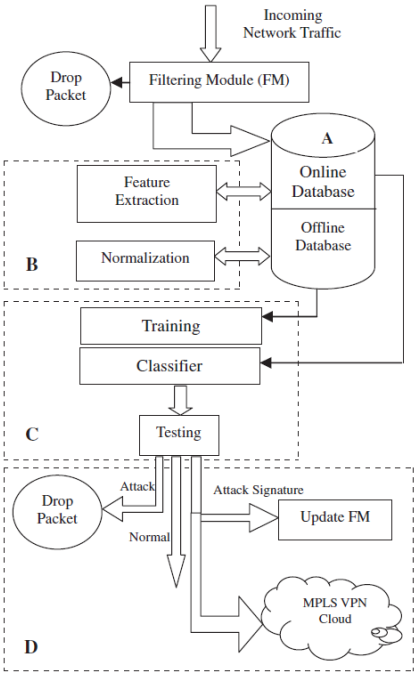


Figure 7 Architecture for DDoS attack detection and response system (Kumar & Selvakumar 2011)

2.2.2 Conclusion

The experiments that took place (there was multiple) were very detailed and rigorous. The proposed system uses a classifier named RBPBoost built off the RBP classifier. It was tested in 2 experiments using a range of data sets to give us an idea of how faster the algorithm is at detecting attacks while obtaining fewer false alarms. There are diagrams over the next page that shows us just a few of the results of how the algorithm faired against other current algorithms. The results can be hard to take in because of the amount of results that were presented. But the overriding consensus is that the proposed algorithm has a better detection rate, less false positives and lower cost. The cost is defined as the occurrence of misclassifying data. "Cost function is based on the number of samples that are misclassified." (Kumar & Selvakumar 2011) This was previously identified during the work of Devi Parikh and Tsuhan Chen in their cost minimization paper. "the cost of a false alarm may be much higher than false detection" (Parikh & Chen 2008)

Algorithm	True Positive rate	False Positive rate	Cost per sample
Bagging	90.6	4.0	0.334
Boosting	93.4	3.2	0.258
AdaBoost	96.8	3.8	0.260
RBPBoost	97.2	3.6	0.244

Table 1 Simulation results of classification algorithms of conficker dataset (Kumar & Selvakumar 2011)

Algorithm	True Positive rate	False Positive rate	Cost per sample
Bagging	93.7	3.9	0.297
Boosting	96.9	3.7	0.253
AdaBoost	97.4	3.6	0.242
RBPBoost	98.5	2.9	0.189

Table 2 Simulation results of classification algorithms for SSE dataset (Kumar & Selvakumar 2011)

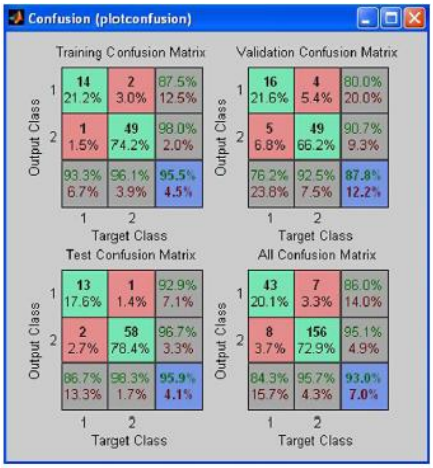


Figure 8 Confusion matrix for the K-Means Clustering (Kumar & Selvakumar 2011)

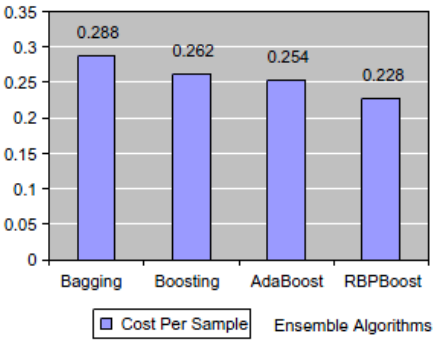


Figure 9 Cost per sample for existing ensemble classifiers and RBPBoost (Kumar & Selvakumar 2011)

So from what is gathered from those examples above (table of results, cost bar chart and the result matrix) it is evident that improvements have been made against other detection models. Progression is valuable for the online security field to keep up with the constant security threats that are conceived constantly. The methods of procuring these results were rigorous and detailed as evident by the range of results that have been discovered. The experiments were conceived with real world situations in mind having the large scale set up that was used create the precise results we have seen. "These applications/projects have inherently geographically distributed centers carrying out specific task/research, networked together to achieve the common goal." (Kumar & Selvakumar 2011).

2.3 Exploiting & Defending P2P

This is a problem that has more to do with the general public as they can be used to target web servers and domestic connections. The P2P operations are quite common among the general public as software like 'µTorrent' is well established among internet users. Using large-scale distributed hash tables brings many unsuspecting participants into DDoS attacks as their traffic can be directed towards victims (As illustrated by the diagram below and on the next page). The research by (Sun et al. 2010) identifies the threats and discovers the defence against these approaches.

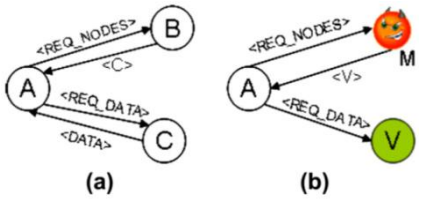


Figure 10 (a) Normal operation and (b) attack (Sun et al. 2010)

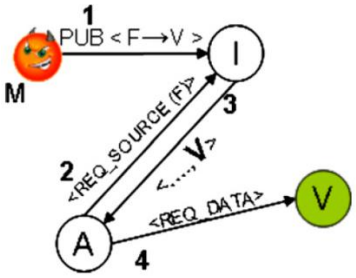


Figure 11 Index poisoning attack in Overnet (Sun et al. 2010)

2.3.1 Analysis

This was inspired from the monitoring of DNS traffic which came up with some curious results.

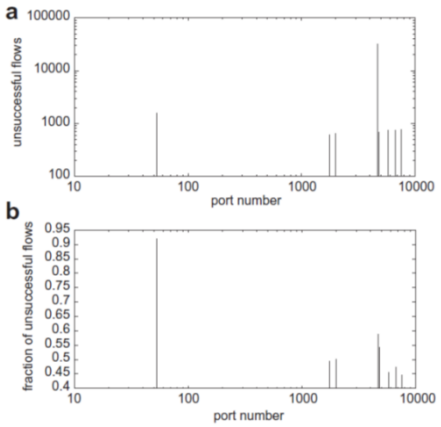


Figure 12 (a) Number of unsuccessful Kad flows sent to ports that received more than 500 unsuccessful flows. (b) Fraction of unsuccessful Kad flows to port that received more than 500 unsuccessful flows (Sun et al. 2010)

How these processes are combatted against in this paper is by 1st knowing the range of amplification methods that can be deterred. Then afterwards the stage of enhancing the resilience against these kinds of attacks is enacted. "the key principles involved in limiting DDoS amplification is validating membership information." (Sun et al. 2010) So from this insight a scheme was produced to mitigate the vulnerabilities within the P2P systems. The sequence of this scheme is illustrated at the top right of this page.

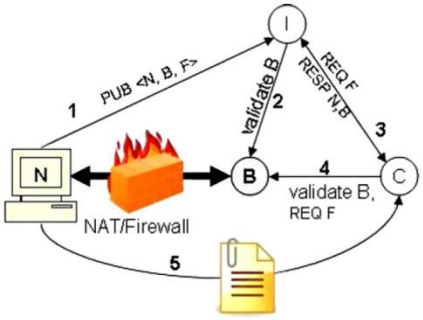


Figure 13 Complete sequence of steps for normal buddy operations with probing-based validation mechanisms (Sun et al. 2010)

The main points considered in this scheme are select criteria as to what methods will need to be used. These are implemented to enhance the P2P system's resilience against DDoS manipulation. The sequence displayed above is designed to be implemented in current P2P systems and the areas it covers are as follows:

1. Use of centralized authorities
2. DHT-specific approaches
3. Corroboration from multiple sources
4. Validating peers through active probing
5. Preventing DDoS exploiting validation probes
6. Source-throttling
7. Destination-throttling
8. Avoiding validation failures with NATs

(Sun et al. 2010)

The experiments implemented to test this scheme were utilised in real world conditions. Planetlab and the Kad network were the areas picked to test this method.

2.3.2 Conclusion

The data that has been produced in these environments are around how these methods impact performance within these systems. So the focus shifts from having a scheme that shields against the vulnerabilities inherent with P2P to also wanting to comply with achieving good system performance while doing so. There is a multitude of graphical data on display that won't be shown too much of in here. But the data does appear to be succinct in what it is presenting. There are many variables to consider in this experiment which is why the testing had to be very broad. In some instances the network

address translation (NAT) delay had increased around 9 times longer than when it was not under attack. By implementing their modified kad system (Resilient Kad) they reduced this delay to around 1.5 to 2 times the not under attack value. An improvement of between 4.5 and 6 times the original systems performance.

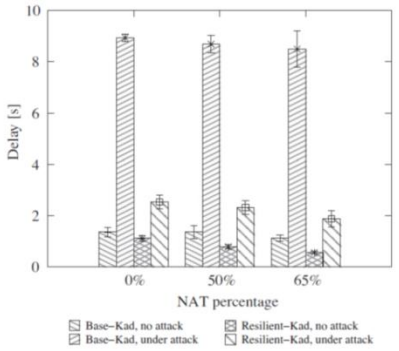


Figure 14 Average time a search takes to locate the index node, with different NAT percentages. Each bar is the average over fine runs. The error bars show the standard deviation. Measured in Kad (Sun et al. 2010)

Now from that diagram it may be misunderstood as not a big deal, changing NAT response rates from 9 seconds to 2 seconds. But in that experiment it was only 5 attackers that were present. In real world scenarios attacks can be participated by hundreds maybe even thousands of different nodes. "There are five attackers that stay through the entire experiment and there is a single victim." (Sun et al. 2010)

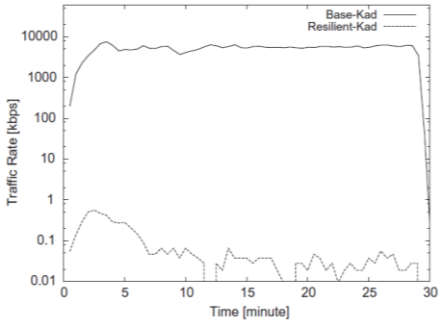


Figure 15 Traffic seen at the victim as a function of time, with five attackers and 50% of the nodes behind NAT. Measured in Kad (Sun et al. 2010)

The diagram above displays the massive difference in attack traffic between the base and the modified system. The difference being so large it is evident that this approach has had a dramatic effect on the impact of the DDoS attack. So the conclusion can be made that this applied research using quantitative methods has achieved its goal in reducing the impact of the DDoS attack.

2.4 Cloud Security

Cloud security when it comes to DDoS is in its infancy. An attack on a cloud infrastructure would have a crippling effect as the attack targets the cloud architectures main weakness. Cloud systems rely on the network infrastructure to function and by attacking it in this manner the resources become so depleted the cloud stops functioning. The research being undertaken is specifically against HTTP-DoS and XML-DoS kinds of attack. This is researched in depth by (Chonka et al. 2011).

2.4.1 Analysis

The system being proposed is a cloud trace back and a neural network called 'cloud protector'. How this operates is illustrated below. This is called the Service-oriented traceback architecture (SOTA) model.

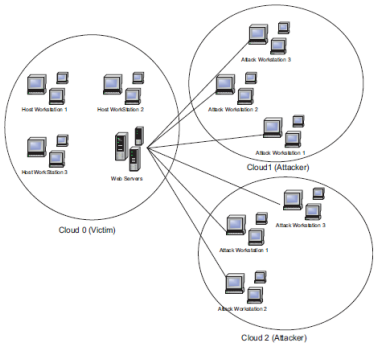


Figure 16 Distributed XML-based Denial of Service attack, where an attacker has taken control of 2 cloud networks and starts sending huge amounts of XML-based messages to Cloud 0 Web Server (Chonka et al. 2011)

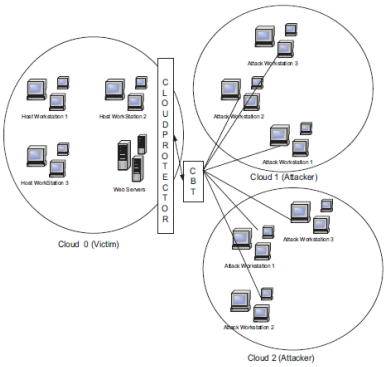


Figure 17 Distributed XML-based Denial of Service attack, where CTB and Cloud Protector are located just between each cloud Web Service, in order to detect and filter X-DoS attacks (Chonka et al. 2011)

The problems this approach is meant to solve is what happened in the Iranian election in 2009. "the Iranian opposition coordinated an ongoing cyber attack that has successfully managed to disrupt access to major pro-Ahmadinejad Iranian web sites" (Danchev 2009). They even used this scenario in their experiment. The image on the next page displays how they thought this attack was perpetrated. "Demonstration of our three virtual machines with 20 Firefox browsers and 20 tabs open to the Page Reboot Website. The purpose of our demonstration was to replicate the attack that brought down the Iranian website." (Chonka et al. 2011)

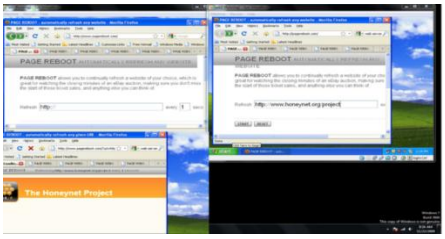


Figure 18 Demonstration of Iranian attack

2.4.2 Conclusion

This was actually one of many works headed by Mr Ashley Chonka covering his PhD thesis "Protecting Web Services from Distributed Denial of Service Attacks". So this an area he is improving on and in this paper he takes his previous research on "Chaos theory based detection against network mimicking DDoS attacks" (Chonka et al. 2009) and implemented it into the context of cloud computing. So that should explain why the conclusion isn't completely conclusive when it comes to verifying the success of the approach. He leaves the door open for future work in this area. This may be due to the results of his experiment not being concrete enough to be implemented on a larger scale. "We detected and filtered between 88% and 91%, but we achieved a very large response variance due to a problem with the neural network settings" (Chonka et al. 2011) the findings of the cloud protector are that it isn't as powerful as it needs to be to be a reliable defense. The findings of the CTB are a bit different as it has been proven to work, but with a stipulation. The system is under greater strain when the CTB is identifying the attackers. "an increase in response time was generated by thirty percent. This increase means that during a DDoS attack, more processing time is required to handle the extra burden" (Chonka et al. 2011). So what is required is a more stable cloud protector to mitigate the strain of the CTB. More research into this is needed because as it stands the system isn't reliable therefore not viable for commercial implementation.

4. Overall Conclusions

Taking all of the previously discussed research papers into consideration the future of DDoS prevention seems strong. As is evident by the results from the various papers is that DDoS can be mitigated quite effectively. It is down to finding the right application of security and discovering what is portable to different architectures. Whatever system this may be it needs to have cloud computing at its foundation. "it is important to design distributed detection and defense system where heterogeneous nodes can collaborate over the network and monitor traffic in cooperative manner." (Tariq et al. 2011) The only way to combat any kind of distributed attack is with a distributed defence. It seems that the agenda of all of the research previously discussed are compatible, and that is what is needed to put an end to this threat. The detection matrix, neural classifier, concepts of P2P defence and the SOTA model all can be unified to strengthen the future systems from malicious resource draining attacks.

All 4 of these areas have established a clear purpose in their investigation which has been relatable with each other. Whether it was focused on the detecting, mitigating, preventing or responding sides of the issue, the purpose is local to the need to defend against DDoS.

All 4 have been rigorous with their quantitative experimental methods. Not only highlighting the successes derived from their hypothesis, but also discussing the issues that needs to be tackled. In the cloud defence research Mr Ashley Chonka identifies that his approach was not as effective as he liked it to be. Also the amount of rigor does vary. We can compare the experiments of (Lee et al. 2011) and (Kumar & Selvakumar 2011) and notice that the degree of which these 2 research groups worked can be seen to be at different levels of rigor. The experiments used to verify the operations of the neural classifier had more layers and covered a larger range of outcomes. Whereas the traffic matrix only used data sets to analyse its effectiveness. One used a large operating network when the other was observed in a smaller detached environment. Due to this more in depth approach the results of the neural classifier tests are deemed to be more reliable.

Because content is quite advanced the testability is based on the skill set of the researcher. The methods have been outlaid in the research and have followed quantitative techniques to evaluate the validity of their research. In these experiments the measurement was always in how it can reduce the effectiveness of DDoS by measuring the reduction in traffic and responses. In all cases there was significant reduction to be seen as a technique to combat DDoS. How these can be reproduced can be quite difficult as previously mentioned the research is advanced in practise. But allowing for the same skill sets the reproduction of results is possible. In the case of the research by (Chonka et al. 2011) the experiment was a scenario dictated by twitter posts over the internet roughly discussing how the original attack was executed. So the experiment has the possibility of being flawed as the original circumstances could be different to what was casually discussed. "the attackers went on Twitter and various discussion forums announcing how to use the Page Rebooter website, by opening it up in many browser tabs and just leaving them to refresh the Iran Government website." (Chonka et al. 2011). So in this case the reproducibility may be relying on false information. The other cases are mostly repeatable with standard equipment but the way the distributed neural classifier method by (Kumar & Selvakumar 2011) was approached was so large it would require large investment to replicate the same results.

The precision of the discussed research is substantial due to its quantitative approach. The empirical data that lead to their conclusions was collected by measuring network traffic and going in to significant enough depth to ensure precise data relating to the detection or prevention of DDoS. Also elaborating on the collected data as to why the data has behaved in that specific way has helped decipher precision. For example in preventing DDoS exploitations of p2p the author explains how the network address translator has been improved because of the precise nature of the data. "Thus, its routing table could include nodes behind NAT, and many search messages could fail since nodes behind NAT are contacted, leading to longer search times." (Sun et al. 2010) Without the precise measurement of how long the NAT

delay was, that conclusion could not be validated.

The discussed research projects did have all the positives discussed in this conclusion but only two have the right to be praised for its generalizability. The way (Sun et al. 2010) utilised the Kad network and (Kumar & Selvakumar 2011) managed the SSE are examples of how experiments need to incorporate real world situations. Although the other 2 research projects can fit quite comfortably under the DDoS prevention umbrella, their experiments concentrated on the detection aspect in a more specific smaller environment.

The confidence in these results is high based on their precision and rigorous approaches. But to bring some parsimony into the equation none of these individually are meant to solve the problem of DDoS. They require other areas to synchronise with these areas to produce a product that can cure this threat. The cloud defense approach needs a better neural classifier method and (Kumar & Selvakumar 2011) may already have that in their RBPBoost. Also to see the merits of the traffic matrix by (Lee et al. 2011) then it could be valuable to test it under the conditions of a large neural network like (Kumar & Selvakumar 2011) utilised. If all these systems can be harmoniously linked together to produce a distributed defence network, then DDoS's days may be numbered.

References

Chonka, A., Singh, J. & Zhou, W., 2009. 'Chaos theory based detection against network mimicking DDoS attacks.' *IEEE Communications Letters*, 13(9), pp. 717-719.

Chonka, A., Xiang, Y., Zhou, W. & Bonti, A., 2011. 'Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks.' *Journal of Network and Computer Applications*, 34(4), pp. 1097-1107.

Danchev, D., 2009. 'Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites.' [Online]
Available at: http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadinejad-sites/3613
[Accessed 26 October 2011].

Jelena, M. & Reiher, P., 2004. 'A taxonomy of DDoS attack and DDoS defense mechanisms.' *ACM SIGCOMM Computer Communications Review*, 34(2), pp. 39-53.

Kim, W., Jeong, O.-R., Kim, C. & So, J., 2011. 'The dark side of the Internet: Attacks, costs and responses.' *Information Systems*, 36(3), pp. 675-705.

Kumar, P. A. R. & Selvakumar, S., 2011. 'Distributed denial of service attack detection using an ensemble of neural classifier.' *Computer Communications*, 34(11), pp. 1328-1341.

Lee, S. M., Kim, D. S., Lee, J. H. & Park, J. S., 2011. 'Detection of DDoS attacks using optimized traffic.' *Computers and Mathematics with Applications. doi:10.1016/j.camwa.2011.08.020.*

Mansfield-Devine, S., 2011. 'Hacktivism: assessing the damage.' *Network Security*, 2011(8), pp. 5-13.

Parikh, D. & Chen, T., 2008. 'Data Fusion and Cost Minimization for Intrusion Detection.' *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, 3(3), pp. 381-390.

Sun, X., Torres, r. & Rao, S., 2010. 'Preventing DDoS attacks on internet servers exploiting P2P systems.' *Computer Networks*, 54(15), pp. 2756-2774.

Tariq, U., Malik, Y., Abdulrazak, b. & Hong, M., 2011. 'Collaborative Peer to Peer Defense Mechanism for DDoS Attacks.' *Procedia Computer Science*, Volume 5, pp. 157-164.

An Evaluation of Current Computing Methodologies Aimed at Improving the Prevention of SQL Injection Attacks in Web Based Applications

Niall Marsh

Abstract

SQL Injection attacks are now common place within the World Wide Web and the development of online applications utilizing web based databases. Combating these attacks is the responsibility of designers, programmers and developers who must use a myriad of techniques in their arsenal to neutralise the threat of these attacks. This paper examines new methodologies being researched for combating SQL Injection Attacks (SQLIA) through detecting vulnerabilities in an applications source code and discussion is given to the use and deployment of these techniques..

1 Introduction

Online security is a key fundamental factor that must be considered by any company or organization that utilizes online functionality in its application. Information security breaches can have significant ramifications for both users and developers of a system typically loss of personal data, legal proceedings through the introduction of the Data Protection Act 1998, financial and or fiscal costs through fraud/theft and loss of revenue, compensation pay-outs, company/brand reputations and market integrity.

Research carried out by Impervia (2011) claimed that as of July 2011, 357,292,065 individual sites make up the internet. From December 2010 through to May 2011 Impervia's Application Defence Centre monitored more than 10 million individual web application attacks, 23% of these attacks were categorized as SQL Injection Attacks Impervia (2011).

Programmers and developers must be aware of current up to date hacking techniques and research aimed at defending against them. Research strategies can be categorised into two main common areas, Vulnerability Detection/Identification and Assault Detection and Prevention. This research review will focus on different research methods for both strategies.

2 Vulnerability Detection Identification

Vulnerability detection for SQLIA is the first line defence in preventing attacks and involves analysing source code for SQL insertion most commonly through black box testing or static analysis within the development environment. Several systems have been proposed in current research to address vulnerability detection such as "Patching Vulnerabilities with Sanitization Synthesis" (Yu et al. 2011) and "CANDID: Dynamic candidate evaluations for automatic prevention of SQL injection attacks" (Bisht et al. 2010) which uses similar methodology in its approach to the SAFELI model discussed in the next section. Additionally primary research has been carried out into creating automated test generators purely for testing the integrity of a DBMS web application "Generating Effective Attacks for Efficient and Precise Penetration Testing against SQL Injection" (Kosuga et al. 2011) discusses a novel approach and although relevant to the research covered in this literature review, further discussion of the topic will not be conducted in this paper as the Kosuga et al. (2011) research focuses on developing strategies

for creating attack patterns across multiple web platforms and applications live on the web and does not interrogate the source code directly or detect vulnerabilities .

2.1 SAFELI

Xiang Fu et al. (2007) have carried out research into building an automated framework called SAFELI to dynamically inspect bytecode of ASP.net applications identifying insertion points for SQL. Once detected, SAFELI scrutinizes the code identifying uninitialized variables and replaces them with symbolic constraints. Tags are added to the SQL insertion point to trigger the constraint solver. When ran through the constraint solver, satisfiability is checked against the constraint and values are assigned for the variable. Now modified the SAFELI framework activates a Test Case Generator which posts the variable in HTML format to a web server and then monitors the result sent back. If vulnerabilities are detected in the response, error message traces are created and flags are tagged to the event, identifying the error.

The researchers in this paper have focused their research into the adapting applications in the .NET framework, SQL injection methodology and development of data security. In order develop an effective strategy to create their detection system, particular attention has been paid to identifying and highlighting an anthology of SQL injection attack methods and have given explanations as to how methods adopted by the SAFELI framework counteract these threats. The research team give supposition that other current systems either in production or development for vulnerability detection are less accurate than the SAFELI framework however, no comparative study, analysis or justification is given for the statement. As SAFELI is still in current development no real-time evaluation of productivity or effectiveness of the framework has yet been conducted, however, the research team have stated that they intend on testing the system on several open source applications available on the internet and developed a test suite to verify the accuracy and ability of SAFELI. Theoretical examples have been used throughout the paper to demonstrate the model and formal proof has been used to validate the results of the framework in action. Xiang Fu et al. (2007) state “the technique can handle hybrid constraints that involve Boolean, integer and string variables” which would enable the framework to detect true/false inputs on system flags and inputs as well as detecting number variables not inputted as strings. Contradictory to this, evidence shown within the examples of the article only use one string variable, throughout and no demonstration of opposing data types are given demonstrating the handling of Boolean or integer variables.

Adopting this method of initially scanning the bytecode of a .NET application for insertion of SQL parameters allows this method to test any .NET application in particular the ASP.net framework which processers user input from web applications typically through POST and GET transactions from form fields within HTML script. ASP.net handles the SQL statements which communicate with an online database. SAFELI is currently not in production and therefore cannot be adopted or adapted to a current operational .NET system or application. Performance and efficiency of the framework currently cannot be guaranteed until further testing and development has been completed. SAFELI has only been designed to work in parallel with .NET applications and would not be able to test contrary frameworks or languages such as PHP or JavaScript as SAFELI performs its algorithms in conjunction with the Microsoft Information Server. The framework currently has only been designed to detect vulnerabilities within an application and it is left for the developer/programmer to patch any errors retrospectively. To further advance the framework and enhance its usability, a solutions module could be introduced into the framework such as in the PSR Generator method, which would automatically fix any subsequent vulnerability that was detected; this would further reduce the possibility of an attack penetrating the application or database.

2.2 PSR-Algorithm & Generator

Thomas et al. (2009) have devised a unique approach for automatic vulnerability detection within a class object orientated environment. The PRS algorithm identifies SQLIV from

within the source code through dynamic analysis. Once detected the PRS algorithm separates the SQL statement into structure and input using prepared statements, these prepared statements are created by the PSR Generator. Reformatted, the SQL statement still has its structure but the inputs have been replaced with placeholders resulting in the vulnerability being removed. Converting SQL to prepared statements can be time consuming especially for large complex applications and models as each line of code needs to be physically analysed by the developer or tester, searching for SQL inputs and modifying the statements accordingly. Using the PSR model can significantly reduce this time through its automation which in return can have significant cost implications when developing an application as less time spent coding is needed to bring the application to market. Automating this process also reduces the potential for human error-prone actions however, for the system to be effective the developer must conform to strict coding practices. Poor coding structure and syntax could lead to a potential risk of vulnerabilities being undetected in the application. Running within the ECLIPSE IDE the algorithm has been written in JAVA for use in native or web driven applications. One of the primary reasons for this is that JAVA and Eclipse are both open source and free to use and adapt by developers. Being open source would allow this solution to be accessible to many programmers as JAVA and Eclipse are both widely used throughout the software industry Capra et al. (2011). Due to the method and structure in which the system has been created using common syntax methodology, PSR could easily be adapted to other object orientated programming language, Thomas et al. (2009). Allowing this adaptation would enable the system to test and fix a greater number of applications such as programs created in PHP, ASP, JavaScript or Pearl, again all open source, readily available software solutions.

As with the researchers of the SAFELI model, Thomas et al. (2009) conducted extensive research in SQLIA and evaluated the current techniques that are being adopted in similar solutions. An outline of how PSR has been designed to counteract these threats and how it differs from other methods has been comprehensively documented and the concept of PSR has been well structured in several subsection of the paper, explaining the logic and action of the algorithm, its implementation and its limitations. To demonstrate the effectiveness of the model the research team carried out tests of 4 online open source applications using the PSR Algorithm and Generator to analyse the source code of the applications, detect the vulnerabilities and modify the code appropriately. To measure the validity of the experiments, test case suites were devised ensuring the security of the replaced code had been achieved and the original functionality of the SQL statement was still intact. Results from the test showed that the PSR model removed 94% of SQLIV and justification was given for why the model did not manage to achieve 100% detection. Recommendations are also given into how the model can be developed in the future to further improve its reliability and accuracy with speculation that 100% detection rates may be possible.

PSR researchers Thomas et al. (2009) have demonstrated in the paper a successful and efficient approach for detecting SQLIV and performing countermeasures directly into the source code. Adopting this model allows the developer to conventionally write the code in their normal style. Providing the programmer adheres to conventional language syntax protocols they can then run the algorithm and see the changes that have been made verifying back that the vulnerabilities have been fixed and the application will be secure and ready for release. At this point using the SAFELI method the coder would now need to concentrate and spend valuable time on fixing the vulnerabilities detected within the application; this however would be taken care of by the PSR Generator. A benefit of the PSR model is the ability to run the algorithm on pre written code allowing any JAVA application to be tested and secured. Software production companies who may have developed many applications would need to invest a considerably large percentage of their resources to evaluate the security risks embedded within their applications. PSR has the potential to offer a solution to reduce this resource allocation considerably with a high success rate. As currently there is only a guaranteed success rate of 94%, programmers will need to be made aware of the limitations of the system and compensation efforts will need to be made in these instances using an alternative

method to prevent the SQLIA when developing or modifying an application.

3 Assault Detection and Prevention

Assault Detection and Prevention is a methodology that monitors a system or application at runtime for injection attacks and performs an action to prevent the database or application being compromised during operation. Research carried out in this approach focuses primarily on communication between backend database management systems and the web based application. "A Specification-based Approach for SQL-Injection Detection" (Konstantinos 2008) is research carried out in 2008 that looked at creating a simple interface between the two mechanisms, monitoring and comparing the structure of the SQL statement inputs against a stored library of validated SQL structures. Further developments in this area of research were conducted by Felt et al. (2011) who have progressed with a similar system method with the introduction of a proxy driver between the two mechanisms called DIESEL.

3.1 DIESEL

A separate approach conducted by researchers at Berkley University investigate the use of Proxy based Architecture and User Based Access Control to prevent SQLIA with a system called DIESEL. The model adopts a policy of "least privilege state" (Felt et al. 2011). When invoked the framework breaks down an application into modules and assigns database privilege access to the minimum requirement needed for the successful operation and function of the module, essentially providing a restricted connection to the database. The second component to the functionality of DIESEL is its proxy driver. The proxy driver becomes the link and detection system between the web application and the database. Using Data Separation the proxy sets restriction policies on the module's connections and then the proxy communicates and monitors the requests and responses from the database detecting any anomalies, removing an attack statement if detected, Felt et al. (2011).

To conduct the research and development of DIESEL, the team have focused on existing research into SQLIA methodologies, countermeasures for prevention of SQLIA, database authentication, database access control, data pooling, multiplexing and proxy services. To evaluate the performance and eligibility of DIESEL, 3 popular web based applications were retrofitted with the prototype framework through modification of the applications source code. The applications were then evaluated against one know documented SQLIAV previously detected within its own framework. Results shown from the test, did detect an intercept the attack successfully. No extended testing had been conducted by the team to test if all vulnerabilities and possible attack patterns could successfully be intercepted by the model; however, theoretical examples were given demonstrating the actions of the DIESEL in action. Before DIESEL could be adapted to live operational web applications, additional testing would need to be completed, especially on large modular applications to verify the performance and efficiency of the multiplexing proxy, and user access control driver. Examples and statistics have been given depicting the modifications DIESEL performs during retrofitting, showing the total lines of code that need modification and the total number of policies created to secure the application. Applications such Drupal and WordPress showed only a minimal amount of modifications were needed to be implement the model, however, one application, JForum needed over 80% more modifications than the previous two. This neither proves nor disproves the success of the research or the application but does demonstrate that the system could prove to be complicated and time consuming when retrofitting a large complex application. The preliminary research has shown relatively positive results in the areas tested; demonstrating the concept and benefits of data separation and how they can be applied in preventing SQLIA. Discussion has been given on the models limitations notably a high computational overhead on performance of 73% during operation and a description is given on the inability to modify certain code in specific instances.

Application of the DIESEL framework cannot yet be guaranteed as a successful candidate for the detection of SQLIA due to inconsistencies in

the testing and further development is required to patch the limitations of the model. Testing of the DIESEL model has shown a high computational overhead that may be inappropriate for large or high level usage web application, adding additional resource requirements to the database server. Due to the methodology and system implementation of the model, access to the application source code is needed and cannot simply interact between application and the database. In addition, code verification of the policies library needs to be independently tested to ensure security and functionality has been achieved; again potentially very time consuming for large complex or multiple applications.

4 Conclusions

Articles examined in this literature review have explored research into varying methods currently being adopted in software engineering, to combat the threat posed by SQL injection attacks. Evaluation of these different models and strategies has highlighted both the strengths and weaknesses of the individual frameworks and their design implementation. Explanations have been given as to how they can be applied in real time environment situations and what impact can be expected of them. Conclusions drawn from the research have identified that none of the systems offer guaranteed detection or elimination of SQLIA or SQLIV in their method and further research must be carried out to enhance web application security. Overall the PSR model has demonstrated to be the most effective example of the models discussed at removing vulnerabilities and has the added advantage of having the functionality to rectify source code, patching the fault. Minimal effort is needed to adopt the method into new and existing programs or applications and has the ability to be adapted to many other programming languages. Further research of the PSR model is expected to yield improved results potentially allowing it to remove 100% of all vulnerabilities. Introduction of proxy services to monitor and restrict access between an application and its database do show the potential to keep an application secure, but due to their nature and functionality incur high computational overheads which may be impractical, especially in an application such as Facebook or Twitter that conduct several million transactions an hour. Evidence does show higher success rates of an implemented model when programmers adopt secure conventional coding practices during the development cycle paying particular attention to modules of code that contain embedded SQL statements. Even when using an automated checking system such as SAFELI or PSR validation analysis still need to be performed to check the stability and security of the system. Standing alone each research method has its own benefits and limitations; combining techniques to reduce vulnerabilities in an applications source code and monitoring the application at runtime to detect a possible attack would greatly reduce the risk of data being compromised and would further maintain the integrity of the system.

References

Prithvi Bisht, P. Madhusudan, and V. N. Venkatakrishnan, 2010, "CANDID: Dynamic candidate evaluations for automatic prevention of SQL injection attacks", *ACM Trans. Inf. Syst. Secur.* 13, 2, Article 14 (March 2010)

Eugenio Capra, Chiara Francalanci, Francesco Merlo and Cristina Rossi-Lamastra, 2011 "Firms' involvement in Open Source projects: A trade-off between software structural quality and popularity", *Journal of Systems and Software*, Volume 84, Issue 1, January 2011, Pages 144-161, ISSN 0164-1212

Adrienne Porter Felt, Matthew Finifter, Joel Weinberger, and David Wagner, 2011, "Diesel: applying privilege separation to database access". In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (ASIACCS '11), pages 416-422

Impervia, 2011 "Web apps attacked every two minutes, Network Security", Volume 2011, Issue 8, August 2011, page 20, ISSN 1353-4858

Xiang Fu, Xin Lu, Boris Peltsverger, Shijun Chen, Kai Qian and Lixin Tao, 2007,
"A Static Analysis Framework for Detecting SQL Injection Vulnerabilities",

In *Proceedings of 31st Annual International Computer Software and Applications Conference* (COMPSAC 2007), pages 87 – 96

Konstantinos Kemalis and Theodores Tzouramanis. 2008, "SQL-IDS: A specification-based approach for SQL-injection detection", In *Proceedings of the 2008 ACM symposium on Applied computing* (SAC '08). pages 2153-2158

Yuji Kosuga, Miyuki Hanaoka and Kenji Kono, 2011, "Generating Effective Attacks for Efficient and Precise Penetration Testing against SQL Injection", *Information and Media Technologies*, Vol. 6, No. 2, pages 420-433

Frank S. Rietta, 2006. "Application layer intrusion detection for SQL injection", In *Proceedings of the 44th annual Southeast regional conference* (ACM-SE 44), pages 531-536

Stephen Thomas, Laurie Williams and Tao Xie, "On automated prepared statement generation to remove SQL injection vulnerabilities", *Elseveir Information and Software Technology 51* (2009) page 589–598

Fang Yu, Muath Alkhalaf, and Tevfik Bultan, 2011, "Patching vulnerabilities with sanitization synthesis", In *Proceeding of the 33rd international conference on Software engineering* (ICSE '11). ACM, New York, pages 251-260

An Evaluation of Proposals to Detect Cheating in Multiplayer Online Games

Bradley Peacock

Abstract

With the advent of broadband came the exponential explosion and popularity of online gaming, in particular Massively Multiplayer Online Games (MMOG's). This is seen as fun for most people but it has become a platform for others to develop their hacking skills. I am going to evaluate current research methods designed to detect cheating in MMOG's and determine if their proposed solutions are effective in combating or even stopping online gaming cheating.

1 Introduction

The number of people who play games online is rising year on year. Advances in graphics and faster CPU's along with fast broadband connections means that online games are more popular than ever. According to Ki and Cheon (2004), the subscription MMOG market alone was worth $1.6 billion in 2009.

The traditional network infrastructure that MMOG's are built upon is the Client/Server Model. The cost to implement such a system can be substantial as it requires a large investment in hardware resources, computing power and network bandwidth. And with the actual development of a game potentially costing up to and including $20 million, Reynolds (2010), the developers need to generate as much return revenue as possible.

With the Client/Server approach being the most widely used model, it should make it hard to cheat as the developers have sole ownership of the servers. And with the business premise of MMOG's being subscriptions the provider needs to be total control of this to allow or deny players based on who has paid their subscriptions and the Client/Server model provides this functionality.

A cheaper alternative platform is the peer-2-peer model but as the game is distributed amongst clients, security concerns are raised severely as it is harder to detect and prevent cheating although research has been done to try and improve security on the Peer-to-Peer architecture, Kabus and Buchmann (2008), Kabus *et all* (2005).

Research has also been carried out as to why people cheat, Kabus, Terpstra, Cilia and Buchmann (2005), Joshi (2008). By manipulating the source code, the ultimate aim is to gain an unfair advantage over the other players and possibly a reputation within the gaming community, whether this is achieved through a highest score, progression through a game the quickest, or buying illegally copied items from other gamers to short-cut a game. There is even a virtual market place for people to buy and trade virtual avatars and property which earns them real money, Kabus, Terpstra, Cilia and Buchmann (2005).

And so with cost involved in developing, producing, deploying and maintaining an online game, it's imperative for the developers to keep cheats out of the game because it could drive away honest players who can't compete with the cheats, thus resulting in lost revenue. However one thing that is almost inevitable is flaws at the design stage of a game and this is the source of most hacks as hackers exploit these oversights, Laurens *et all* (2007).
One aspect of current computing research is aimed at detecting whether a human being is in control of the game and inputting commands, or whether an automated player agent, commonly referred to as a 'gamebot' or 'bot', has been implemented to input commands. The research is aimed at providing the ability to find out.

The rest of this paper is organized as follows: Section 2 presents and evaluates the five technical proposals researched which aim to achieve the same goal. Section 3 is a critical evaluation of the research and the paper concludes in section 4 with synthesis of what has been learnt from sections 2 and 3.

2 Presentation and Evaluation

It would appear that most players in the gaming community disagree with the use of bots as most players will put a lot of effort into earning various achievements and also gaining rewards. Several anti-cheat software programs have been developed to combat cheating, such as Punkbuster and GameGuard but they can't prevent all bots. Ki and Cheon (2007), analyse and classify known attacks and also categorize these attacks into layers, helping to segregate the attacks which could possibly help focus

the development of an anti-cheat software program, specifically aimed at certain attacks. However this research which has been compiled aims to determine whether or not a human is in control, by using various methods, regardless of what category the attack falls under.

2.1 CAPTCHA's

It may not initially sound difficult in distinguishing human players from bots as the abilities of the two are quite different, but a bot can be injected into a game controlling an avatar just like a human controlled one, only a little quicker and more responsive, predicting and reacting to a scenario quicker than any human could. And so Golle and Ducheneaut (2005), propose the use of a variety of tests, which can tell humans and computers apart, collectively known as Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA's), Von Ahn *et all* (2003).They propose to apply them in both hardware and software tests with the hardware tests being versatile enough for use in a wide variety of online games. A capture test works by presenting challenges that are simple for humans to solve but are difficult for a computer to solve, Pau *all* (2010). The most implemented CAPTCHA tests rely on humans' to ability to recognize randomly distorted text or images, Pau *et all* (2010).

The hardware proposal is to turn input devices such as a mouse or joystick into CAPTCHA devices. If the CAPTCHA device is rendered tamper proof there would be no other way for input signals to be sent to the game software other than physically interacting through the device. The signals would then be authenticated either at the game server or to the game software running on the machine. They believe a machine could physically interact with the hardware device but a human would be much faster and more reliable where reactions are critical. This could also apply to games played using a keyboard but they state to render a keyboard tamper-proof could be difficult and expensive to design, however the research does not state that they have approached any manufacturers to ascertain how much the cost would be. Perhaps if the authors had taking this into consideration then the proposal would be more substantiated as a lot of games are played using a mouse/joystick and a keyboard. They claim that CAPTCHA input devices are best suited to First Person Shooters (FPS) and claim they also guarantee that the 'aimbot' cheat, typically used in FPS, cannot be used. It could be argued that the player still has to control the avatar to some degree in order to make use of the aimbot which requires the interaction of the hardware device anyway, thus challenging this statement.

The software proposal is a CAPTCHA token whose function is testing a player is indeed human and they estimate it is a lot cheaper than the hardware counterpart. Again no research has been done to ascertain this. It would be based upon standard cryptographic techniques and come in the form of an onscreen challenge in which the player has to press a number(s) on the keypad correctly to continue playing the game. These would appear at random intervals during the game which, one would assume, would be frustrating to the game player.

"CAPTCHA tokens require an interruption on the part of the player and thus appear most suitable for slow-paced games with very specific rules and low-entropy inputs and outputs, such as card and board games (chess, poker, etc)" Golle and Ducheneaut (2005).

They do compare their implementations to others used in other two-factor authentication and so it would appear they have taken an idea and tried to improve upon it. They state they propose two broad approaches to help combat bots, but the term 'broad' implies it will not work on all systems. They also state that they can distinguish bots from human players which is commendable, but they do not propose any solution as to what they will or can do once the bots are identified.

2.2 Human Input Device's

While Golle and Ducheneaut (2005) believe CAPTCHAs do provide a sound solution, Schluessler *et all* (2007), contradict their proposal, finding through research that CAPTCHAs are limited to non-real time applications, Pao *et all* (2010). What Schluessler *et all* (2007) propose is a method which ensures data input actually enters a system through a physically present human input device (HID). The HID will detect whether data has been modified prior to its use with the aid of an input monitoring system. It works on the premise that the input data generated by the HID has to be the same as the input data used by the game software. If they differ, then some form of illicit modification, insertion, or deletion occurred. The input monitoring system will compare the two data streams and if they differ in any way then a notification is sent to a remote service provider (RSP). The prototype proposed can be implemented on any standard personal computer (PC) and the system architecture will change only slightly as the input monitoring system will come in the form of a firmware update but additional hardware must be purchased in the form of hardware duplication filters. The authors alluded to the cost of these only stating it was moderate, a more specific figure would be beneficial to any persons con-

templating this system. It has been designed initially to work with Intel® chipsets and so it is assumed the authors have not experimented with other chipsets.

When a software application is started and elects to have the inputted data protected, a RSP is contacted and the application sends its inputconfiguration as well input devices allowed to connect,to the input verification service (IVS) within the firmware and the IVS then links up to the RSP. Each key press, mouse movement etc is passed through hardware input duplication filters and one data stream is sent to the game software and one to the IVS. The IVS then compares the two and if an attack is detected, determined by two different data streams, the IVS sends notification the RSP. This is sent over a secure connection to prevent any sort of tampering, and so the connection has to provide message integrity, authenticity, confidentiality and message duplication detection. Once an attack is detected, all connected clients are notified of who is cheating and an on screen message is displayed stating who the cheater is. It is also possible to kick cheaters from game and ban them completely.

The prototype which was built deviated from the initial design architecture to keep hardware costs down and because of this Schluessler *et all* (2007) could not implement such a system which was not vulnerable to circumvention, and this was one of the prerequisites for the system to be successful. As such the initial design cannot be verified. However the system they did test was successful in detecting input injection attacks. They decided to test it against the online game *Quake 3* which is a FPS, using an Intel® x86 platform. The prototype detected the use of an aimbot which automatically aims a user's weapon at the enemy.

Although providing an initial successful implementation of their system, the authors do conclude that the answer to their papers title "Is a bot at the controls" remains unanswered. This is because there are many questions which remain as the prototype was only tested on one specific machine against one specific game and the architecture deviated against the initial proposal.

2.3 Human Observational Proofs

A very similar scheme is one proposed by Gianvecchio *et all* (2009). They base their system of bot detection on Human Observational Proofs (HOPs) which is a form of an Intrusion Detection System (IDS). According to their research it is difficult for a bot to perform certain actions in a human-like manner. The HOPs passively monitor input actions and compare them against a series of human user input traces already collected. In direct contrast to the HID system designed by Schluessler *et all* (2007), the proposed system actually lets a data stream pass through to the game server.Two components are required: a client-side exporter and a server-side analyser. The exporter sends the users data stream for the exporter to analyse to decide if a bot is operating the client or not. A cascade neural network is at the core of the analyser, which 'learns' the behaviours of human players. They have used a neural network as research shows that they perform well with user input data, Webb and Soh (2007). What the authors do not state is whether the neural network needs to be installed on each game server and then subsequently 'learns' human behaviour or whether or not it can 'learn' one persons behaviour which can then be transferred to other servers and used as a basis for every player. They have not stated if it is the same for the bot behaviours.

The authors devised a series of experiments under different configurations to gather information about different game bots and used different human players to give them enough scope to make a successful system within the parameters they propose, and were thorough in which user-input actions to record. Unlike the previous research, Schluessler *et all* (2007); they also used their system on two games, *World of Warcraft* and *Diablo 2*, and so could confidently state they had enough information to reach a definite conclusion. There research shows quite clearly in the form of charts how the input actions of a human and a bot differ and could be used as a visual referenceas proof of this as it is very precise. Unlike Schluessler *et all* (2007), and Golle and Ducheneaut (2005), what they do not state is what they would do once a cheat is detected.

2.4 Player Behaviour Analysis

A similar concept is proposed by Laurens *et all* (2007). They have designed a proof-of–concept system that detects cheats by monitoring player behaviour although the authors do state from the outset that that their evidence shows that their system can only correctly distinguish most cheating from non-cheating players, not all, but it is a proof-of-concept.

They based their system on *CounterStrike: Source* and specifically targeted wall-hacking. Again like Gianvecchio *et all* (2009), the authors state that players using cheats exhibit in-game behaviour which is very distinguishable from players who are not.

"A system based on behavioural analysis to detect cheating play promises significant advantages over current anti-cheat mechanisms"
(Laurens *et all,* 2007)

This could be true and only if it works, again their system is a proof-of-concept but any good idea needs a starting point. However Gianvecchio *et all* (2009) have proven results based on two games, but unlike Gianvecchio *et all* (2009), the authors of this system devised their own algorithm based on results from game play to detect cheating play. To achieve the results they performed thorough experiments similar to Gianvecchio *et all* (2009), using players very experienced in gaming to eliminate the learning curve as to achieve a more accurate set of behavioural results. Yet the authors do not relate to any other research on behavioural analysis and actually state that there appears to be very little academic research done in the field of online gaming security. This can be contested as scores of papers were found on this subject suggesting more could have been made of their idea if similar work was taking into consideration.

Their concept is very similar to Schluessler *et all* (2007), the difference being the cheat detection system resides on the game server as a plug-in where it monitors the player's actions from within the game world. Communication takes place via an interaction layer with players' data being pulled in and traces performed upon the state of the game to determine the information required. The data is then formatted and then passed to the analysis engine and then passed back to the game server to be acted upon. Again, unlike Schluessler *et all* (2007) and Golle and Duchneaut (2005), the authors do not state what happens if a cheating player is detected but do state in their 'Future Work' segment that the scope of their work was to be limited and was designed to demonstrate the feasibility of behavioural analysis to be implemented to gaming security.

2.5 Trajectory-Based Player Behaviour Analysis

Chen *et all* (2008) take the concept of behavioural analysis and propose a trajectory-based approach, which they believe can be applied to any game in which a player directly controls an avatar. Their theory is sound but they do not qualify this statement with results from research. They used the game *Quake 2*,a FPS, which has a built-in gameplay recording function which can be used to reconstruct the game and review each player's actions and movementsfrom any position and angle.. To represent diversity the authors only used traces that actual players contributed voluntarily. Using one map of *Quake 2,* they were able to plot the aggregated navigation of each player. The same was done using three different bots in the game and the results were compared. The authors found that the pattern of the human players varied greatly to that of the bots, with the behavioural analysis, for example, being that humans tended to keep next to walls when moving around the map so as not to expose themselves in open areas where they would most likely be shot by an enemy, unlike a bot who's reaction times would be quicker and would be able expose themselves in open ground for that exact reason. Also human players adjust their movements more continuously and slightly as they constantly move and spin round, side-to-side *etc* to detect enemies that happen upon them. This work appears to derive some good and valuable information.

Using this the authors then used a framework to train a classifier which is then able to determine whether any given segment of an avatars trajectory is the result of a human player or a bot. The detection accuracy achieved results of 95% with traces longer than 200 seconds.With the type of bot used also being detected this is very commendable work and appears more accurate than the previous proposals.

3 Critical Evaluation

All of the systems evaluated achieved varied results based around the same concept. The authors have proposed solutions but due to various reasons including budget and time, could not fully test their systems on more than two games at any one time.
What is interesting is the how similar the systems are, excluding Golle and Ducheneaut (2005), which would not work in real-time gaming. And it seems apparent that the potential flaws in one system could be overcome by using another. It could be possible to combine Schluessler *et all* (2007) with Gianvecchio *et all* (2009) as the user data carried by the client-side exporter in Gianvecchio *et alls* (2009) proposal could be tampered with prior to it being sent to the server-side analyser. Implementing Schluessler *et all* (2007) idea would ensure that the data was indeed inputted by a human. If Chen *et alls (2008)* proposal could also be implemented then there would be indeed three layers of protection, but the burden on hardware resources could be considerable. Chen et all (2008), Gianvechhio et all (2009), Laurens et all (2007), Schluessler *et all* (2007) and Golle and Duchneaut (2005) have all stated the cost for their systems is minimal but only for their very specific scenarios, the actual cost to design such systems which would work across all platforms could be more.

4 Lessons to be Learnt

The most obvious question arising from the research is whether the proposed solutions would work on any other system and game aside from the actual ones used. Until, or indeed if further research is done using these methods the question will remain but progress has been made. With hacks deriving from security flaws at the design stage all of the proposed solutions merit further investigation by developers as the cost incurred in the research could be a lot less in comparison to revenue lost due to players abandoning games because of cheats.

References

Ki, J., & Cheon, J. h. (2004). Taxonomy of online game security. *The Electronic Library Vol. 22 Iss: 1* , 65 - 73.

Kabus, P., & Buchmann, A. P. (2008). Design of a cheat-resistant P2P online gaming system. *DIMEA '07: Proceedings of the 2nd international conference on Digital interactive media in entertainment and arts*, (pp. 299-306). Athens.

Kabus, P., Terpstra, W. W., Cilia, M., & Buchmann, A. P. (2005). Addressing cheating in distributed MMOGs. *NetGames '05: Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games.* New York.

Yan, J. J., & Choi, H.-J. (2002). Security issues in online games. *The Electronic Library Volume 20 Number 2* , 125-133.

Chen, K.-T., Liao, A., Pao, H.-K. k., & Chu, H.-H. (2008). Game Bot Detection Based on Avatar Trajectory. *Entertainment Computing - 7th International Conference*, (pp. 94-105). Pittsburgh.

Gianvecchio, S., Wu, Z., Xie, M., & Wang, H. (2009). Battle of Botcraft: fighting bots in online games with human observational proofs. *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security.* Chicago.

Laurens, P., Paige, R. F., Brooke, P. J., & Chivers, H. (2007). A novel approach to the detection of cheating in multiplayer online games. *2007 IEEE International Conference on Engineering of Complex Computer Systems* ,(pp. 86-95).Auckland.

Schluessler, T., Goglin, S., & Johnson, E. (2007). Is a bot at the controls?: Detecting input data attacks. *NetGames '07: Proceedings of the 6th ACM SIGCOMM workshop on Network and system support for games.* Melbourne.

Golle, P., & Ducheneaut, N. (2005). Keeping bots out of online games. *ACE '05: Proceedings of the 2005 ACM SIGCHI International Conference on Advances in computer entertainment technology.* Valencia.

Yan, J., & Randell, B. (2005). *Security in computer games : from pong to online poker* . Newcastle-Upon-Tyne.

Harding-Rolls, P. (2010, September 19). *Subscription MMOGs - Mixed Fortunes in High Risk Game.* Retrieved October 17, 2011, from www.screendigest.com http://www.screendigest.com/reports/2010822a/10_09_subscription_mmogs_mixed_fortunes_in_high_risk_game/view.html

Reynolds, D. (2010, June 22). *The Cost to Make a Quality MMORPG.* Retrieved October 17, 2011, from www.WHAT MMORG?com: http://www.whatmmorpg.com/cost-to-make-a-quality-mmorpg.php

Joshi, R. (2008). *Cheating and Virtual Crimes in Massively.* London.

von Ahn, L., Blum, M., Hopper, N., & Langford, J. (2003). CAPTCHA:Telling humans and computers apart. *Advances in Cryptology, Eurocrypt '03*, (pp. 294-311). Warsaw.

Pao, H-K; Lin, H-Y; Chen, K-T; Fadlil, Junaidillah. (2010). Trajectory Based Behaviour Analysis for User Verification. *11th International Conference on Intelligent Data Engineering and Automated Learning* pp. 316-323). Paisley: Computer Science

Webb, S. D., & Soh, S. (2007). Cheating in networked computer games: a review. *DIMEA '07: Proceedings of the 2nd international conference on Digital interactive media in entertainment and arts*, (pp. 49-53). Perth.

Duh, H. B., & Chen, V. H. (2009). Cheating behaviors in online gaming. *Online Communities and Social Computing. Proceedings Third International Conference, OCSC*, (pp. 567-573). California.

Chow, Y.-W., Susilo, W., & Zhou, H.-Y. (2010). CAPTCHA Challenges for Massively Multiplayer Online Games Mini-game CAPTCHAs. *2010 INTERNATIONAL CONFERENCE ON*

CYBERWORLDS (CW 2010), (pp. 254-261). Singapore.

An Empirical Study of Security Techniques Used In Online Banking

Rajinder D G Singh

Abstract

The objective of this paper is to examine encryption methods used to achieving a secure environment in the banking sector. This paper discusses the encryption techniques of online security comprising the factors that compromise online banking security comprising key points that cause the vulnerability of users to phishing and malware threats in section 2, followed by the common security threats in e-banking in section 3. The evolution of encryption methods will be covered in section 4 which discuss the efforts taken by banks to improvise the online banking systems with the implementation of new technologies. Section 5 touches on some experimental work carried out by researchers in order to examine the strengths and weaknesses of authentication methods that have been executed by banks followed by section 6 that summarizes a comparative study to the encryption techniques being experimented on. Finally I conclude the usage of encryption techniques and some recommendations for banks and users towards achieving a better future in online banking in section 7.

1 Introduction

Online transactions have been taking place since the early 19th century. Over time, the usage of internet for banking matters has grown amongst users that they find it efficient and a hassle free way to conduct their daily banking needs may it be purchasing goods from virtual stores, fund transfers or paying bills. The popularity and usage of online banking has increased tremendously in the past few years thus marking the importance of security standards over the internet. Various encryption methods and technologies have been implemented since the start of online banking, however, comparably it has increased an alarming threat of fraud and identity theft amongst users. As early as 1984, there has been a surge of interest amongst active e-banking users about a number of computer break-ins [Haskett, 1984] thus jeopardizing the trust of users in performing transactions online.

2 Factors That Contribute To E-Banking Security Threats

Banking activities over the internet platform are sensitive therefore higher security standards have become a necessity to curb the growing

menace in the industry. Constant use of greater security technologies improves the level of secure banking contradictorily affecting the usability of the product and services (Holbl, 2008). According to Haskett (1984), break-ins were caused by novel users using dial-up facilities to hack into computers by guessing combinations of user id and password on a repeated basis (Haskett, 1984).

> "While the battle between those who would have tight security and those who want simpler (user-friendly) log-ins continues, some of us find ourselves needing an immediately implementable system..." (Haskett, 1984).

It was studied that one of the reasons hackers were on the large at that point in time was caused by customer mentality of wanting a system that can simply be accessed without having to remember long combinations of passwords. Commonly, most users prefer having short passwords than long nonsense alphanumeric characters to enable them to remember passwords easily rather than walking around with a notebook full of passwords to various secured sites.

Besides choosing short and easy manageable password, users tend to reuse their passwords across various platforms. "...people accumulated more accounts but did not create more passwords" (Gaw et al. 2006).

The number of passwords people use is not at par with the number of online bank accounts that they have which makes it easier for attackers to crack the code and have access to not only one account but to all accounts associated with that particular password. In addition to that, Gaw et al (2006) also claimed that reuse of passwords was a major

problem amongst users where they used a single password for multiple bank accounts.

3 Common Security Threats in Online Banking

The most known attacks in the online banking industry are the Trojan attacks, phishing attacks and the MitM (Man-in-the-Middle) attacks. In the Trojan attack scenario, the attacker sends out emails to user accounts convincing them to open a specific site. When the site is visited, the website automatically installs the virus on the user's computer. The Trojan then sits in the system and observes the computer activities and gets into action as soon as the user begins an online banking session. When a transaction is made, the virus invisibly changes the amount and destination of the transaction not known to the user (AlZomai et al. 2008).

Phishing attacks are done by tricking users into revealing their banking account details (Peng et al. 2010). For instance, an email from L1odys is impersonated to convince a user that it actually sent from a genuine server. The change of 'l' to '1' is hardly visible at one glance, making it difficult for the user to notice the attack. The user therefore opens the email which leads him to a dummy Lloyds bank web page. As soon as the user inputs his username and password, the attacker is able to record the details and the account is hacked in no time.

In the man-in-middle scenario, the attacker potentially tends to sit between the bank server and the user and impersonate them both. This kind of activity is known as pharming (Berghel, 2006). The man-in-middle can act as both the bank and the user therefore making it next to impossible to detect any faults by both parties where the bank thinks it's a genuine user and the user thinks it's a legitimate bank website.

4 The Evolution of Encryption Techniques of Online Banking

The password technique is a greenhorn method used more than twenty years ago where a user is required to enter passwords with combinations of alphabets and numbers to access a secure banking site. The loop holes in this method were soon noticed by the intruders where they only had to guess a combination of usernames and passwords randomly till they found a matching pair. Keeping that into consideration, this technique only allowed three attempts of inserting a correct combination of username and passwords. If an account is indeed accessed by an intruder, on the fourth attempt he is automatically redirected to a dummy webpage that appears to be a genuine one. The intruder therefore thinks he's successful in cracking the code but where in actual sense, he isn't. The motive of this technique was to create confusion amongst hackers where they believe they were on the right track but they were not. Failure to login on several counts on a frequent basis can lead to hacker trap, if desirable (Botting, 1986).

In order to overcome the problem of having users to remember long passwords a technique known as secondary passwords was introduced (also known as supersets of Pass-algorithms). This technique is used by providing passwords along with the one provided by the vendor of a particular operating software of a system. Pass-algorithms are affordable, easy to install and maintain. Moreover it requires no alterations to the operating system therefore it makes it a hassle free process for both the provider and the users. According to Haskett (1984), this scheme allows enforces and system administrator to collect site dependant information about any attempted break-ins.

According to Holbl (2008), most banks have adopted the two-factor authentication approach that is basically gets information from what the users know (passwords) and what they have (security device). Though the actual implementation of this method may vary among banks worldwide, but the basic idea of this authentication technique is the same. Along with the static password that users use to access their online accounts, all transactions performed will require the second part of the authentication which may be a PIN/code on their security device or cell phones that were registered during the opening of the account. This code is known as the one-time-password approach. This approach is currently used by the Barclays Bank in the UK and also some banks in Malaysia, German and the Scandinavian countries (Holbl, 2008).

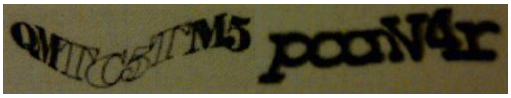
The two-factor authentication method was backed up by Nilsson (2005), when she talked about: 1) Security Box, which works with a dynamic password and 2) Fixed Passwords which means having one constant or static password (Nilsson et al. 2005). The security box method simply means that users are provided by dynamic passwords on a device (e.g. cell phones or smartcard readers) that users receive a unique transaction code on. This code coupled with the user's password is used to login and perform transaction over the internet. Where else in the fixed passwords method, a user is provided with a code upon registering at the bank for the first time. This code is static and users use the same code together with their passwords to perform online transactions overtime which is used

by Lloyds TSB, UK. The security box type of authentication is known to be safer than the fixed passwords method because a unique password is generated each time users try to login their online bank accounts. The unique code is dynamic and different each time it's sent out from the server. The 'fixed password' method is used by some financial institutions in the United Kingdom where else most Sweden banks use the 'security box' method.

Another form of classification in the two-factor approach is the certificate-based-approach, where a license is used as a second validation factor. This certificate requires PKIs (Public Key Infrastructures) which can be stored in any physical storage device (e.g. USB stick or smart card) (Holbl, 2008). This method is known to be cheap and easy to use. This approach can be classified as a timer-based-password approach where it's used by the banks to providers of services like Paypal and eBay (Holbl, 2008). This method is used using hardware generators where the password generated for a particular transaction lasts for a certain time only (e.g. 60 seconds) thus limiting intruder activities. The final classification of the two-factor authentication approach is the certificate-smartcard based approach. This approach requires a specific card reader that can be used to store certificates or to generate one time passwords. All transactions are recorded on the smart card therefore chances of identity stealing in the Trojan attacks are equal to zero. Although this method has its benefits and is safe to use, it is rarely used by banks around the world due to its expensive cost. *"There is not a single bank that makes such an approach mandatory"* (Holbl, 2008).

Where some researchers talked about secure login and transactions, Alzomai et al. (2008) expressed that data security is also an essential key point to online banking. The team claimed that there are two types of authentication that are important in online banking. They are: 1) user authentication and 2) data origin authentication. He stressed that data authentication is as equally as important as user authentication. It is important to be within genuine web pages throughout the transaction process right from the user login until the transactions are completed. It is important to generate data from a genuine provider and that the data is not tampered with to ensure data integrity. It is of no use if a user logs in safely and protects his data but the site that he is accessing is not a genuine one. The impact is of no less than a stolen user identity. Therefore, a typical method for data origin discussed was the OTP (one-time-password) for every transaction. This method is similar to the one discussed previously where the transaction not only requires the normal user passwords but also requires a hardware token that can generate one-time-authorization code with limited validity time. The OTP implementation can be of different ways (e.g. security boxes, hardware tokens or SMS messages through mobile devices).

Li et al. (2010) studied another method known as CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart). A text CAPTCHA is shown below:



CAPTCHA (Image: Courtesy of Li et al. 2010)

This method is deployed at the login level and the transactions level. CAPTCHAs are mainly used to prevent automated MitM (Man-in-the-Middle) attackers (Li et al. 2010). Many banks around the world have deployed this technique alongside their existing security methods to make it harder for malicious programs to manipulate transactions. Unlike the OTP, this solution does not base on any physical device thus making it cost effective to maintain and implement for both banks and its users. The principle of CAPTCHA is that pattern recognition tasks are tremendously tricky for computers but simple for humans (Li et al. 2010).

Some of the methods mentioned above are further discussed in the following sections based on experiments conducted by different researchers.

5 Experimental Research and Results

The first two experiments discussions are done on the bank's end and the third experiment is done based on a user's viewpoint towards secure online banking.

As mentioned earlier, to achieve a certain standard of online security, greater technologies have been implemented which affects the usability of an online banking. AlZomai et al. (2008) conducted an experiment on the two-factor authentication approach focusing on the one-time-password (OTP) method using email instead of SMSs that required cell phones. The study was carried out on a group of students from Queensland University of Technology (QUT), Australia which consist of undergraduate students, master students and PhD research students including staff on campus and non QUT participants. The experiment was to examine the usability of the SMS authentication scheme (AlZomai et al. 2008). The participants varied from different faculties (law, education and IT) within the university and aged between 20 and 40. A

dummy online bank simulator was created and participants were asked to perform transactions on the simulator. While the participants were doing their transactions, two simulated attacks were carried out namely the Trojan attack and the man-in-the-middle attack. The results showed that out of 53 attacks sent out, 42 were discovered by participants and the transactions were therefore cancelled. This means that 79% of possible obvious attacks were successfully avoided. In a separate method of sending out attacks, only 39% of stealthy attacks were managed to be blocked. The OTP codes were sent via email rather than the SMS system where in real world banking; mostly all banks use the SMS systems or a security device alternatively. Although the avoided attacks success rates were high, the accuracy of results cannot be relied on 100 percent as emails are more likely to spread viruses and phishing activities compared to SMS systems. This experiment therefore concludes that the one-time-passwords sent via emails are not the best solution to online banking security.

Apart from that, Li et al. (2010) carried out an experiment to test the strengths of CAPTCHA solutions by deploying practical real time attacks on various CAPTCHA schemes used by banks in Germany and China using image processing and pattern recognition tools. These CAPTCHA breaking tools are technically run on specific mathematical formulas. The results showed that automated programs could recognize each and every character even better than humans when the distorted text was well segmented (Chellipah et al. 2005). The results returned an alarming success rate of 100% of breaking CAPTHCAs. Therefore it can be concluded that CAPTCHA solutions do not meet the expected security requirements in real world banking.

Nilsson et al. (2005) however took a different approach in examining encryption techniques from a user's perspective. The team conducted a survey on 40 participants in Sweden to test the 'security box' method and 40 participants in UK on 'fixed password' systems. The questionnaire comprised of questions encompassing four major aspects; trust, authentication, location and control (Nilsson et al. 2005). The findings showed that the first three factors significantly influenced online banking users with an average of more than 3.7 points for 'location' on a likert scale of 1 till 5 for both the methods used. This concludes that trust and authentication of users in a particular online webpage depends on the location of where they are accessing the webpage from. A user accessing his online account from a cyber cafe is more likely to be exposed to virtual threats than a user accessing his account from a home PC.

6 Comparative Conclusion on Experimental Study

The experiment done by AlZomai et al. (2008) on One-Tine-Password methods returned high results of users being able to avoid security attacks. This study was narrowed down on a specific number of participants within an organization. Users performing transactions from dummy accounts on simulated WebPages were not sensitive to the nature of real world banking that involves actual personal funds. Therefore I conclude that this study did not return reliable results based on the scope of the experiment and the platform used to deliver OTPs which in this case is through emails. Moreover, CAPTCHAs on the other hand were proven to be weak and could be broken into using carefully designed mathematical formulas by Li et al. (2010). Neither methods proved to solve e-banking issues efficiently thus increasing the necessity of a thorough study to reveal best methods possible to achieve safe and secure online banking. Although the OTP encryption method is most commonly used by banks around the world, it has not been proven that the security attacks via this method is zero. Besides, user experience and knowledge on security issues also plays a major role in the banking industry.

7 Conclusions

The nature of online banking security is sensitive as this type of transaction over the internet is always susceptible to security threats. Various methods were studied and examined by different researchers on various aspects of e-banking security around the world. The results however were not as promising considering the platforms on which e-banking operates. The e-banking security has to be meticulously evaluated in order to achieve the high level security standards of banking online. E-banking security is yet to be improved to overcome malicious programs and curb other invisible attacks.

The usability factor should also be kept into consideration while upgrading and implementing safer security technologies in order to ease online transaction amongst users.

Apart from the banks assessing new technologies to withstand particular attacks, users equally hold importance in enhancing online banking security and keeping their accounts as safe as possible. Users should take measure to educate themselves

about possible attacks and how attackers operate on their paroles.

References

AlZomai M, AlFayyadh B, Josang A and McCullagh A, 2008, 'An Experimental Investigation Of The Usability Of Transaction Authorization In Online Bank Security Systems', *AISC '08 Proceedings Of The Sixth Australasian Conference On Information Security*, Volume 81, Australian Computer Society, Inc. Darlinghurst, Australia, Australia ©2008

Berghel H, 2006, 'Phishing Mongers and Posers', *Communications of the ACM – Suporting Exploratory Search*, Volume 49 Issue 4, April 2006, ACM New York, NY, USA

Botting R, 1986, 'Novel Security Techniques For Online Systems', *Magazine: Communications of the ACM*, Volume 29 Issue 5, May 1986 ACM New York, NY, USA

Chellipah K., Larson K., Simard P, and Czerwinski M, 2005, 'Computer Beat Humans At Single Character Recognition In Reading Based Human Interaction Proofs (HIPs)', *CEAS* 2005.

Gaw S. and Felten E W, 2006, 'Password Management Strategies For Online Accounts', *Proceeding SOUPS '06 Proceedings Of The Second Symposium On Usable Privacy And Security*, ACM New York, NY, USA ©2006

Haskett A. J, 1984, 'Pass-Algorithms: A User Validation Scheme Based On Knowledge Of Secret Algorithms', *Magazine: Communications of the ACM*, Volume 27 Issue 8, Aug 1984, ACM New York, NY, USA

Holbl M, 2008, 'Authentication Approaches For Online-Banking', *CEPIS*, ACM Digital Library ©2008

Li Shujun, S.A. Shah H, Khan Usman, Syed Ali Khayam, Sadeghi A and Schmitz R, 2010, 'Breaking E-Banking CAPTCHAs', *Proceeding ACSAC '10 Proceedings of the 26th Annual Computer Security Applications Conference*, ACM New York, NY, USA ©2010

Nilsson M and Adams A, 2005, 'Building Security And Trust In Online Banking', *Proceeding CHI EA '05* CHI *'05 Extended Abstracts On Human Factors In Computing Systems*, ACM New York, NY, USA ©2005

Peng Y, Chen W, Chang M and Guan Y, 2010, 'Secure Online Banking on Untrusted Computers', *Proceeding CCS '10 Proceedings Of The 17th ACM Conference On Computer And Communications Security*, ACM New York, NY, USA ©2010

A Critical Study on Proposed Firewall Implementation Methods in Modern Networks

Loghin Tivig

Abstract

The world's economy faces a high dependency of Internet and computer systems. The need for data protection solutions has increased along with the development of internet based systems. The firewall is one of the most important tools created to protect a system or a computer network from outside attacks. The aim of this paper is to analyse and critical evaluate some of the existing and some of the proposed firewall implementation techniques that apply to various types of networks. The paper also suggests several practical approaches to efficient implementation and structuring of firewalls for companies in order to reduce time, expenditure and in the same time to increase the standard of security in their networks, based on the testing proofs presented in the research papers studied. The conclusion sustains that researchers have managed to find effective solutions of firewall implementation that can be applied by companies in order to benefit of high standard security at reduced costs.

1 Introduction

In order to benefit of protection, confidentiality, integrity and availability, networks can be protected by firewall applications. The firewall represents the barrier between a trusted network/system and an untrusted one. Due to increasing network speed and traffic, the firewall software needs to evolve in order to be able to confer a good quality of service. The transfer of data packages between networks/systems is analysed following sets of rules and if the package complies with the rules the transfer is allowed. Modern firewalls must perform more than applying these rules; they also need to act as protection against viruses, different types of attack and to monitor all the data traffic. Basically the good functionality of the firewall is set by how good the rules policy is: if it's too permissive the network is unsecure and if it's too restrictive, traffic that should have access is denied. Having a good policy is not enough. Too much data can produce a huge queue and data packages are permitted without a valid inspection giving the possibility of an outside attack. The modern mobile applications that use the Internet can become gateways into the network and increase the risks of attack. The development of e-commerce has led to a necessity for having security rules that every company using this type of commerce needs to comply with. This is in order to protect financial information used in these transactions (e.g. credit cards details, bank accounts), typically targeted by hackers. These companies must respect security standards like Payment Card Industry Data Security Standard (PCI DSS) or Sarbanes Oxley (Garlick 2009). Developers have tried to change the common way of thinking in creating firewalls, some of them getting ideas from nature like "Ant Colony Optimization based approach" (Sreelaja and Vijayalakshmi Pai 2010) or "Modeling firewalls by (Tissue-like) P Systems" (Leporati and Ferretti 2010). A different approach was to verify packets transfers by using multiple firewalls at the same time either in parallel or in series (Khalil et al. 2010). The latest software product in security matters is the Intrusion Prevention System (IPS) or Intrusion Detection and Prevention System (IDPS). This type of software monitors the traffic and activities within the network or system in order to prevent an attack using signature-based detection methods, statistical anomaly-base detection and also stateful protocol analysis detection. Later in this paper it will be discussed the idea of

creating a firewall's simple structure to match the Network Intrusion Detection System capabilities.

2 Background

The problems related to protection through using firewalls emerge from continuous evolution of computer networks. The amount of data transferred inside a network along with new versions of harmful software and changing strategies used by hackers ask for a constant need of regular updates.
Many companies consider that having an older version of firewalls will protect them against threats but the reality is different: hackers are most of the time one step ahead the current protection software, so developers also must to keep up with them by creating new products or updating old versions (Garlick 2009). The appearance of Wi-Fi networks and Smart phones has created the need of a new firewall strategy to be implemented in this type of networks.

As state by Strohmeyer (2009) in PC World magazine that some people use to believe there is no need to install firewall software on their devices because the Wi-Fi router already has a built-in firewall. The article clarifies that in fact, the router has a built-in firewall but it protects only against port scanners, and the main risk of getting your device infected with malicious software is the downloading of information. This is where the need of protection software like firewalls should be installed on a device.

According to Chris King (2011), from Palo Alto Networks, using the IP port 80 associated with HTTP transfer gives the possibility of dangerous packages to go through because the traffic is always allowed by the firewall's rules. The solution he proposes is to analyse the applications and also the port used and the packet to be allowed only if the user has the right credentials. The same problem applies to HTTPS networking protocol.

The problems identified can be classified in three categories: costs, performances and type of network. The small to medium size businesses cannot afford the high prices for the latest products' releases on the market. More costly effective solutions of firewall systems must be developed and in the same time, these products must offer a level of protection comparative with other more expensive products existing on the market. In the aspect of performance there is a need of techniques that can deal with high volume of data transfer for large companies' use. The different architecture of Wi-Fi networks also requires new firewall systems that can adapt to their demands.

3 Literature Review

For the problems listed above, many solutions have been proposed in the literature and some of them will be analyzed in the following paragraphs of this paper.

3.1 MANET Networks

"A mobile ad hoc network (MANET) is a self-organizing network of mobile routers and associated hosts connected by wireless links" (Suman et al. 2010).
The increasing number of devices Wi-Fi compatible like Smart phones, computers, printers etc. creates large networks, especially in public places, and a growing demand of security solutions for this type of networks. One of the primary protections is the existence of built-in firewall software in network routers but these firewalls only prevent port scanner attacks and cannot protect against malicious software (Strohmeyer 2008).

Research has been carried out in this domain to solve security problems and a proposed technique for MANET networks is to randomly change the firewall router after a fixed amount of time in order to make more complicate finding an entry in the network in a case of outside attack (Suman et al. 2010). The authors claim that their technique will increase the security in MANET networks. A graphical representation of the method's functionality is presented in figure 1. In this case every device within the network must be able and willing to act as a firewall. The authors claim that this method will confer a much better security for these types of networks.

Although this concept is a revolutionary one and might help increasing the security for MANET,

functionality has been demonstrated using a series of mathematical calculation. For specific values and in a certain situation the authors make obvious the efficiency of their theory. The mathematical demonstrations sustain their claims in a "perfect" network. In the real world there is no such a thing as perfect network, because devices can develop a multitude of problems, so to demonstrate the efficiency and advantages that this implementation might bring, a series of tests must be performed. The networks to be used in these experiments must contain a large variety of devices in order to analyze how each one of them will act. A problem that could be encountered is to create the firewall software in such a way to be compatible with all the wireless platforms and operating systems currently existing. The devices' battery power is also an important factor that should be considered.

Therefore, as the authors admit in their conclusion, more research is needed for this technique to become usable (Suman et al. 2010).

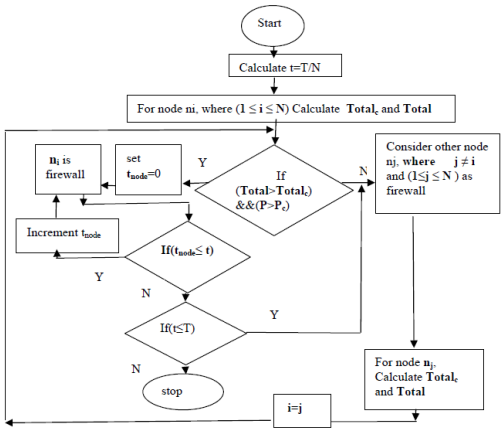


Figure 1 Flowchart of random selection of firewall (Suman et al., 2010)

3.2 Parallel Firewalls

A proposed solution that claims to reduce time and speed up the data packages verifications is the use of multiple parallel firewalls. According to Khalil et al. (2010), this technique has proved to be extremely efficient. The claims have been confirmed by testing different implementations of firewall protection and comparing the results. In order to test their experiment the following hardware and software resources have been used: Microsoft parallel firewalls (ISA) with a constant number of 3000 rules policy, Virtual Personal Network (VPN) and also Cisco 6500 switches with Network Load Balancing (NLB). Tests have been performed for the following cases:

- No firewall.
- Standalone firewall without VPN.
- Standalone firewall with VPN.
- Enterprise edition ISA integrated with NLB for only internal without VPN.
- Enterprise edition ISA integrated with NLB for only internal with VPN.
- Enterprise edition ISA integrated with NLB for only internal & external without VPN.
- Enterprise edition ISA integrated with NLB for only internal & external with VPN.
- Two standalone firewalls with two Cisco 6500 switch with HSRP enabled without VPN.
- Two standalone firewalls with two Cisco 6500 switch with HSRP enabled with VPN.

For each one of the above cases it has been recorded and compared the following results: processor usage, the amount of data transferred, time and bandwidth usage. The conclusion of all these experiments is that using their proposed technique (two standalone firewalls with two Cisco 6500 switch with HSRP enabled) the best results can be achieved for any of both cases, with or without VPN.

The experiment is descriptive giving the possibility to be easily repeated by anyone interested in this aspect. Considering the wide range of tests performed, there is enough evidence to accept the claims made for the specific case presented. A concerning fact in this approach is the cost of its implementation. Having parallel firewalls could be an improvement in speed and quality but because of high cost it might not be applicable to companies with small budget. Further tests of this concept can be performed using different firewall products and implementing this technique in a real world company network to see what level of improvement and service

quality can be gained in comparison with the existing system.

3.3 Filter and Firewall Automatic Cooperation

One of the latest network protection techniques is the use of IPS (Intrusion Prevention Systems). These systems incorporate existing technologies like firewall, antivirus and intrusion detection software. The problem of IPS is the cost of implementation because they require expensive hardware. For medium to large size companies this might not be an issue, but for small companies this solution can be unaffordable.
In their research Shirazi and Salehi (2009), demonstrate that the same standards of security can be achieved using a much more cost effective solution. The proposed technique is the use of NIDS (Network Based IDS) integrated with Packet filtering. The experiment was performed using Snort NIDS and a simple firewall created in IPTABLES. The results obtained after running intrusion attacks against the experimental protection demonstrate the effectiveness of the method. Although the experiment has been performed on a Linux platform, using XML for communication between NIDS and firewall means that this type of implementation can be extended on other platforms.

The schema and all the necessary details are well explained in the paper leading to an easy remake of the experiment. Their theory is more interesting because for the test performed, it has been used common applications and the whole implementation doesn't necessary need expensive hardware and software resources. The fact that Snort is an open source detection system and IPTABLES a common Linux tool makes this research a practical solution for low budget companies due to the reduced costs of its implementation. The experiment had good results in the case presented and sustain the claims made by the authors. Further tests should be performed in the matter of attack diversity. Also a comparison between IPS and this type of implementation could reveal some useful information about the level of security each of the methods provides. Considering the variety of operating system used, a continuation of this research would be the development of software compatible with all major operating systems.

3.4 Network Processor Solution

A method proposed to speed up the filtering process is network processor solution. This method targets the data transfers between two of the most used types of network: WAN and LAN. It can be defined as a "hybrid firewall architecture that independently leverages the control and data path capabilities available in the network processors" (Seong-Hwan Kim et al. 2010).
The technical details of functionality are presented in figure 2.

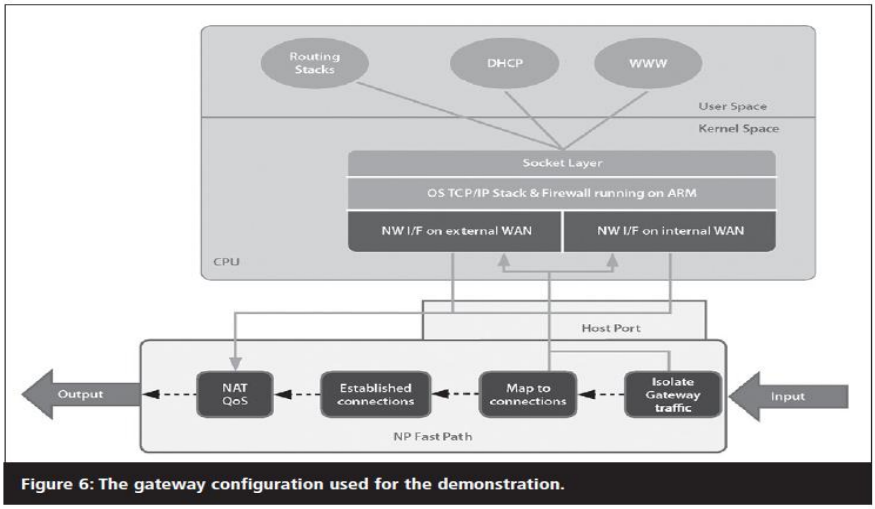


Figure 2 Network processor implementation (Seong-Hwan Kim, et al., 2010)

For this experiment it has been used the APP2200 device. The results of the performed comparison between this kind of implementation and the traditional firewall implementation demonstrate that the proposed solution, in the specific scenario presented, provides better results. The details of the test presented has a lack of information regarding the conditions and equipment used making the results open to questions regarding the connection between hardware / software capacities of the system and the results. Based on the evidences provided, it only can be assumed that this implementation targets complex networks and it requires powerful hardware resources.

The output of the test makes known that using the proposed method the transfer between WAN and LAN is much faster in any of the cases: with firewall enabled or disabled. Based on these results the authors concluded that "This model provides consistent and predictable high throughput performance for the traffic while retaining the flexibility offered by a general-purpose CPU architecture". (Seong-Hwan Kim et al. 2010)

3.5 Ant Colony Optimization

In their research N. K. Sreelaja et al. (2010) present a new bio-mimetic technique inspired from the ant colony architecture which helps filtering in the firewall rule set. The proposed solution targets general implementation of firewalls rules. Efficiency of this approach has been demonstrated by performing a diversity of case studies. The authors have developed an algorithm that has been presented in pseudo-code format and they have used that algorithm for a variety of situations. The functionality is well explained including complete mathematical calculations for every case considered. The research contains also results of comparison between this type of method and the major existing methods in targeted area.

In terms of mathematical demonstration, the overall research is descriptive and well performed but there is a lack of information about a real experiment. The theoretical advantages sustain the authors' claims, but in order to demonstrate the effectiveness of this solution, practical tests must be performed. Also, there is no specification about the type and performances of the hardware and software resources that must be used and also the cost of implementation and maintenance. A further study must be performed in these fields in order to convince companies to adopt this approach.

3.6 Tissue-like Model

Based on the similarity between P system rules and firewall rules a research has been carried out by Leporati and Ferretti. (2010) in finding a solution to use the tissue-like P system as an instrument to create and examine security properties of firewall. The aim of this technique is to help network administrators to test the filtering rules before implementation, in a faster way. The practical outcome targeted, is a reduced cost and fewer problems in system's implementation. The authors claim that this approach of using P system has never been studied in the literature and what seems to be a huge problem in the existing firewalls' rules creation methods can be easily fixed using the proposed tissue-like model. Functionality has been proved using a complex mathematical demonstration which brings enough evidence to sustain the authors' claims. The lack of information about a practical implementation and testing makes the method just a possible solution for the problems intended to solve.

3.7 Firewall Strategies for Businesses

For current companies it is critical to implement a firewall security. Their management must find a balance between performance, security and administration for a successful implementation of firewall to protect the networks and system they use and also to keep the software up to date. The rules applied should be optimized and the firewall must not be loaded with extra-services. In the event of replacing the firewall product, the use of special packages for analyzing the base rule is critical. Firewall platforms that allow this type of technology, can use a connection acceleration to speed up the traffic. In order to increase the network speed sometimes the administrators tend to use dangerous modification like reducing the level of encryption, disabling the logging for all services or switching off the TCP stateful inspection. Allowing third-party connectivity without authentication and encryption is also a common practice. All these things can put the network at a high risk, therefore must be avoided. (Garlic 2009).

Maskey et al. (2007) present a template firewall configuration that can be used as a starting point by companies or institutions as a low budget solution. Because the mentioned paper presents a basic firewall configuration for teaching and learning purposes a complete analysis of the method has not been performed.

4 Conclusions

The firewall has become a primary tool in the fight against viruses and hackers attacks. Due to the high levels of security it provides, the majority of Internet users, including companies and institutions have chosen to use a firewall product. Looking at the examples presented in this paper it is obvious the continuity of new firewall methods research as response to progress of network technologies, diversity of harmful software, hackers' attacks and the huge amount of data transfer. Based on the problems identified, this paper has analysed and presented existing solutions that can be adopted by companies. The methods studied above solve problems like costs of implementation, data transfer and methods for Wi-Fi networks. In some of the cases more research is needed for the proposed methods to become feasible solutions ready to be used.

References

Garlick N. (2009) 'The hidden benefits of optimising your firewall.' *Network Security*, 9:6--9, September.

Gold S. (2011) 'The future of the firewall.' *Network Security*, 2:13--15, February.

Khalil R. K., Zaki F. W., Ashour M. M. and Mohamed A. M. (2010) 'A Study of Network Security Systems.' *International Journal of Computer Science and Network Security*, 10(6), June.

Kim S.-H., Vedantham S. and Pathak P. (2010) 'SMB gateway firewall implementation using a network processor.' *Network Security*, 8:10--15, August.

Leporati A. and Ferretti C. (2010) 'Modeling and Analysis of Firewalls by (Tissue-like) P Systems.' *Eighth Brainstorming Week on Membrane Computing*. Sevilla.

Maskey S., Jansen B., Guster D. and Hall C. (2007) 'A Basic Firewall Configuration Strategy for the Protection of Development-related Computer Networks and Subnetworks.' *Information Systems Security*, 16(5):281--290.

Rowan T. (2007) 'Application firewalls: filling the void.' *Network Security*, 4:4-7, April.

Shirazi H. M. and Salehi H. (2009) 'Automatic Cooperation between Filter and Firewall for Improving Network Security.' *Journal of Information and Communication Technology*, 2(2):107-113.

Sreelaja N. K. and Vijayalakshmi Pai, G. A. (2010) 'Ant Colony Optimization based approach for efficient packet filtering in firewall.' *Applied Soft Computing*, 10:1222-1236.

Strohmeyer R. (2008) 'True or False: Wi-Fi Users Don't Need a Software Firewall.' *PC World*, October.

Suman, Patel R. B. and Singh P. (2010) 'Random Time Identity Based Firewall In Mobile Ad hoc Networks.' *International Conference on Methods and Models in Science and Technology*. Chandigarh, India.