Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 12 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cyber Police: An Idea for Securing Cyber Space with Unique Identification

By Ziaur Rahman, Md. Baharul Islam & A. H. M. Saiful Islam
Daffodil International University, Bangladesh

Abstract - The advancement of cyber technology completely depends on how conveniently we use it. Many people deceived in different ways in our current cyber system. We can prosper ourselves through the utilization of this internet technology. However any country can improve their online security through improving cyber system. On the other hand it may cause precarious outcome if it is incorrectly handled by any unplanned administration. An appropriate mechanism can move forward our cyber world with a safer e-biosphere. The purpose of this paper is to propose an idea that will ensure security and justice in cyber world. This idea proposes to diminish all types of anarchy from the cyber space by ensuring authentic identification to every internet user; securing website browsing; preventing any kind of fraud as well as guarantee truth and justice in the online world.

Keywords : *cyber world, wo rld wide web, virtual justification, cyber security, sensor technology.*

GJCST-E Classification : *K.4.4*

Strictly as per the compliance and regulations of:

Cyber Police: An Idea for Securing Cyber Space with Unique Identification

Ziaur Rahman [α], Md. Baharul Islam [σ] & A. H. M. Saiful Islam [ρ]

Abstract - The advancement of cyber technology completely depends on how conveniently we use it. Many people deceived in different ways in our current cyber system. We can prosper ourselves through the utilization of this internet technology. However any country can improve their online security through improving cyber system. On the other hand it may cause precarious outcome if it is incorrectly handled by any unplanned administration. An appropriate mechanism can move forward our cyber world with a safer e-biosphere. The purpose of this paper is to propose an idea that will ensure security and justice in cyber world. This idea proposes to diminish all types of anarchy from the cyber space by ensuring authentic identification to every internet user; securing website browsing; preventing any kind of fraud as well as guarantee truth and justice in the online world.

Keywords : cyber world, world wide web, virtual justification, cyber security, sensor technology.

I. Introduction

Initially we have tried to identify the reasons behind the existing cyber world have been working for long time since it was born. And finally we have found that the today's cyber space is unplanned, unmanaged, inconsistently distributed, commercialized, and immorally active. The relationship between the various attack methods and their corresponding solution are described (Adeyinka, 2008). Really there is no master plan under the huge cyber world. Managing a simple house is almost impossible without at least a minimum plan whereas this cyber world is running without of any reliable control.

For example, if a new application is developed, it is added to internet world spontaneously through enormous advertisement typically without any minimum certification or any valid justification as prerequisite. Consider an application for measuring the amount of love between two persons in percentage if just two names are given to it. A vast number of Apps and mini tools like this are unnecessarily available in different social network sites today. We have been using these or we have to insensibly click on it before we go on for further browsing without any evaluation even in some cases entirely unknowing what it is. We never consider how much time it wastes and how many problems it creates. Not only apps, we're unintentionally offered different irrelevant virus, worms etc through firing unwanted script when we download software or anything from different websites. Some websites and even many ads are always misusing our cookies and session to sneak our data irrespective of minimum privacy policy. We're technically deprived of doing anything against this type of deceptions we often face everywhere online as there is no exact authority to take care our allegations and to dispute it into a solution as well. However, up to now no endeavor we have towards establishing any regulatory body to step up against this kind of frauds. Internet Technology is now a matured youth after its disorderly long-teenage stage. But the bitter truth is that the amount of high speed internet users is not as enough as we ever hope. Whenever, this rate is quite alarming in developing countries around the globe. Unlimited commercialization of this very technology is not a new feature at all, but it has intractably increased in an intolerable extend from the last decades of the previous century. And the ultimate situation is getting worse than before day by day. Direct and indirect advertisements are now a critical hindrance while we surf internet. Immoral activities in cyber space are another very frequent issue from its birth to at present has noticeably caused hundreds of thousands of sufferers here and there across the world. It is said that cyber space is as a negative stuff as even several educated parents are totally unlikely to let their children to use internet at their early age. United Nations International Children's Emergency Fund (UNICEF) has recently funded a campaign through their website to save the Children abuse online. Certainly, it's not acceptable in any manner in this modern on-screen date. So far, now is the time even though it's quite late to rethink about our cyber space to advance it towards a wonderful virtual world that we all once dreamed of. To successfully encounter this challenge, we propose an awesome solution. Let's see what exactly Cyber Police wants to do. (Langner, 2013) finds out why cyber security risk cannot simply be "Managed" away. Towards measure internet security strategy for small medium enterprise is finding (Fortinet, 2013)] with better definition (Aspnes, 2003). (Library, 2009) worked with an annotated bibliography of select foreign-language academic literature. There were a lot of research on cyber crime study and their cost (Anderson, 2012).

Author α : Lecturer, Department of ICT, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh.
E-mail : zia@iut-dhaka.edu
Author σ : Senior Lecturer, Department of Multimedia Technology and Creative Arts, Daffodil International University, Dhaka, Bangladesh.
E-mail : baharul@daffidilvarsity.edu.bd
Author ρ : Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh.
E-mail : saifcse@daffodilvarsity.edu.bd

Cyber-crime is the big challenges for coming of age (David, 2012). Policy for cyber security is increasing via internet governance, reporting and awareness reforms (Amor, 2012).

II. Methodology

Diminishing the distance between virtual and the real world will be the preliminary task of Cyber Police. For this, first of all, we'll have to ensure a genuine online identity or the Cyber ID (CD) in short. It is really inevitable to have a unique online address as we usually have in our physical world. To guarantee this desired CD we can apply different modern way but now we want to begin with ratifying our email addresses. The email profile of a user exclusively has a duty to match his national citizen profile. To make it easy, we can regard national ID as our email address. Suppose, National id of a Bangladeshi traffic is 8217318598379 (as shown in the Figure 1) should be his distinctive CD. One of the prominent advantages of this system is that an infant will naturally be a member of this huge Cyber family immediate after its birth. However, almost half of the total idea will be impulsively implemented itself if we can make certain an authentic, credible and reliable CD.

Figure 1 : Sample National ID card of a Bangladeshi Citizen

Then the next steps will be easier to initiate as it requires not moving away much from the existing system structure currently we have. In our real life we habitually see, who you are entering into my house you must inform me before you go in. Same as, a user will have to substantiate his CD before logon into any web server or website. The server/site authority will let the specific traffic to sign in if no prior allegation is found alongside him. At the same time, it will also authenticate whether it's he or not exactly who is requesting for to login besides reporting his mental health as well. Question is how we can prove that the id and the user on behalf of it are uniquely resembles. The answer is so easy as we need not to be worried any kind. Modern finger print sensor technology is that what we can easily apply to solve this. In a broad sense if we consider it then we can think about DNA code encryption matching through a biometric encoding method. For these we only need an extra key on the keyboard or totally sensing input device. To check user's healthiness we'll just append a bio-informatics technology inside the additional desired button. For more reliability in future we can re-deign our system through making it artificially intelligent or through enabling its total object detection capability. Nonetheless, what about resource and time? Yes, No need to be nervous about it because we could save our valuable time and resource if the idea here is put into service completely. An activity history profile will simultaneously monitor and store user's event information of every second at server memory when he sends http request to the server. If he attempts to do anything out of security policy automatically will be logged out after informing the reason behind it. And it will also send a report (diary) to ICCJ accusing of the suspected user. International Cyber Court of Justice (ICCJ) is a proposed sovereign council to ensure cyber law and justice worldwide. ICCJ will receive and verify the diary immediate after submitting it and will go forward for further investigation to finally Figure out whether the suspect is guilty or not. If the acquisition is proved then the authority will take necessary step against the alleged user. As a penalty the accused id could be sent to the custody cell enlisting it as an illicit id for a certain period of time or a fixed balance could be cut down from his bank account as charge according to the intensity of the crimes. If ICCJ finds any severe crimes, it will redirect the case to the proper authority of the user's Country to warrant physical punishment for what he has ever done. Meanwhile a user will be privileged to appeal to ICCJ showing documents in favor of it to be acquitted himself. One may have a question how an unschooled inexpert user will do that. Yes, we can imagine e-lawyer to resolve this type of situation if it arises. The lawyer or anybody experienced will show the necessary browser record on behalf of the supposed user. If any traffic wants to convict against a website or server he could apply the same process above.

III. Experimental Result

To Login into the ICCJ email system we need to enter valid Cyber Id and password. If the username and password is correct then the traffic can sign in. Otherwise if the traffic enters wrong password or Cyber Id that doesn't match with the Cyber Id and Password exist in database he will be the shown the same interface again as we can see in Figure 2.

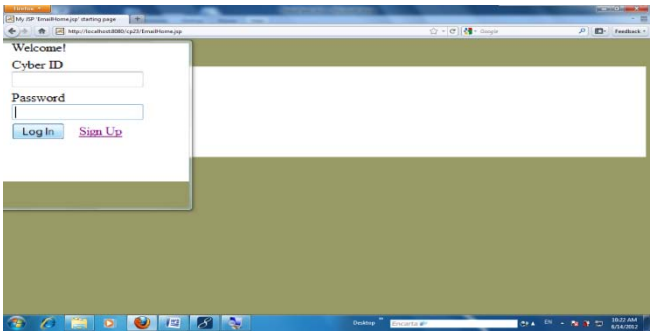

Figure 2 : Webmail login interface

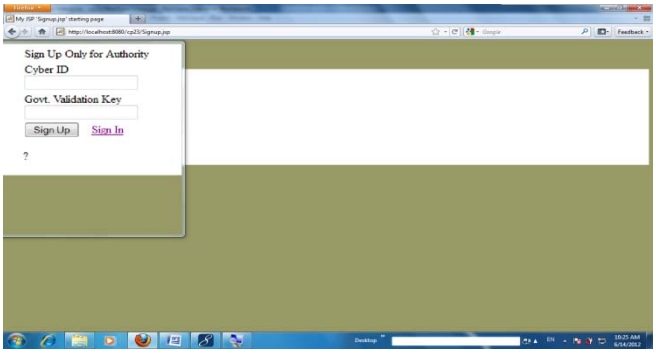

Figure 3 : Signup Interface System

In login page there is another option called signup out there for new entry beside form submit button. This idea demands a much authenticated type of login. As we said our national id will be our email id. And an email id will be generated by the government authority instead of individual initiation. But as here it's not very easy to implement this plan so we've considered a government validation key for temporarily entry to check up. For the real case or for professional use of this idea certainly we need our sophisticated cyber id (CD). To register a new account we need to click on Signup button. After clicking on it we see the windows as shown in Figure 3.

a) Sample Page Login Interface

After using his email a user can easily log out from the system. Now we will see how our ICCJ would be monitoring our internet surfing. And how will it control itself. First of all if we want to browse a website, as early as I enter the desired web address on our address bar; it will automatically redirect server login page as shown in the Figure 3 in the right interface. After login we will see our desired website in the left interface of the Figure 3 available below.

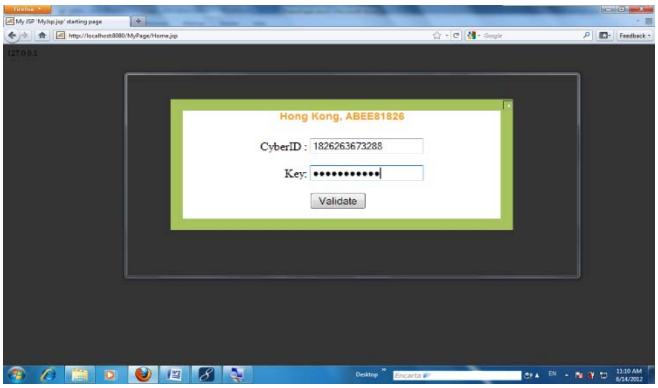

Figure 4 : Login window to access any website

Figure 5 : Ministry of Education in Bangladesh Website

After successfully checking up the validation, the user will see the page he looks for. Here as a sample we show our page. The page is official website of Ministry of Education, Bangladesh in Figure 5. In this page a webmail service is available for office use only. The webmail system is not public as it demands user authentication. If anybody unauthorized wants to use this webmail system and s/he enters wrong password and username more than three times then s/he will be logged out from that site or server. At the same time ICCJ will send an email to his email profile as an accused allegation.

b) Alleged User Email Interface

Once allegedly logging out from the server the user can't login into the same page again because of acquisition. He is supposed to open his ICCJ email inbox to check the allegation against him. Here in Figure 6 shows a sample message from ICCJ while a user is acquitted of. After reading the mail thrown by the ICCJ automated system if the user want to appeal in favor of his own side he can do it before the deadline. For the successful implementation of this proposed idea we certainly need an active browser what can provide us necessary history on browsing period. The message will

show an attachment containing the activities details what he did online that is shown in Figure 7.

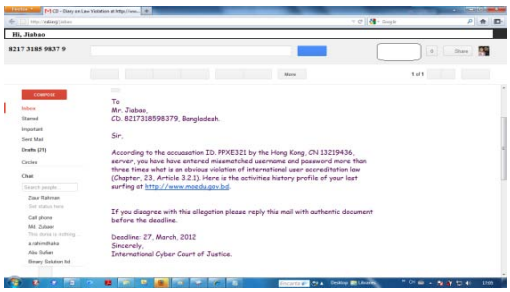

Figure 6 : Email from ICCJ immediate after allegation

Activities History Profile

CD. 8217318598379

Server : Hong Kong, CN13219436

No	Even ID	Time	Purpose	Remark
1	AB9871	16:34:26	Redirecting Server Validation	√
2	EE2144	16:34:26	Pressing Sensor Device	√
3	BE2513	16:34:27	Clicking on Validation Button	√
4	AE7632	16:34:28	Redirecting www.moedu.gov.bd	√
5	CF2653	16:34:30	Clicking on Webmail Button	√
6	EC6533	16:34:33	Submitting username and password	x
7	DE1231	16:34:35	Submitting username and password	x
8	EE6723	16:34:36	Submitting username and password	x
9	DD5421	16:34:36	Logging out by server	√

Figure 7 : Active history profile

c) Suspending (Punishment) Message from ICCJ

Finally if the allegation is proved the ICCJ authority will suspend his Cyber ID for a certain period of time as shown in Figure 8.

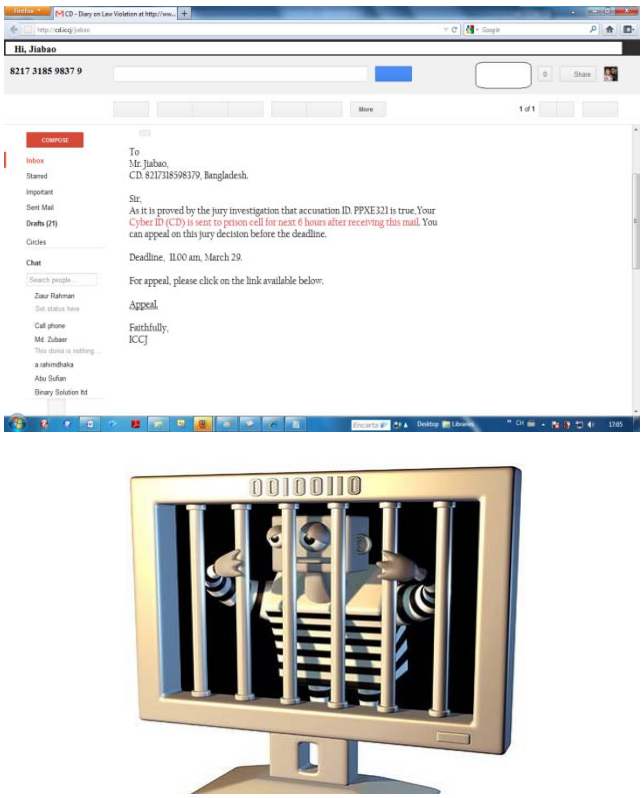

Figure 8 : Message from ICCJ containing suspension report and cyber ID in the prison

Within this time period the user will not be able to surf internet. If he tries to do the same he will be given this message as shown in Figure 9.

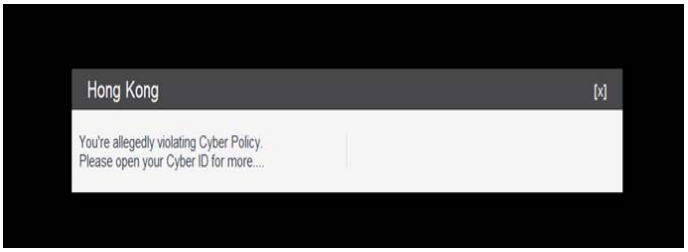

Figure 9 : User Window While CD is allegedly accused of

After the deadline the cyber id will be freed (as it was in the prison database Figure 9 specified right) and it will work again as it did before.

IV. Discussion

Our idea is successfully tested with the help of certain necessary tools. Before testing there were some faults and bugs inside it but now it is totally bug free. The schedule of test is given in table 1.

Table 1 : Test Schedule

Test Start Date	Test Complete Date	What was Tested	What was not Tested
June 1, 2013	June 12, 2012	• Login Security • Hosting • Deployment • Filtering • Session • Cookie	• Finger Print Validation • National ID Matching

V. Conclusion

We know what is happening in online world. Online technology is a wonderful invention for the humankind but we're not able to get maximum number of throughput from it because of uncontrolled and so called regulation system. Now it is the time for change. Only a convenient change can be a solution for the problems we have ever encountered. So far, though it's quite late to rethink about our cyber space to advance it towards a wonderful virtual world as once our anterior generation dreamed of. To successfully encounter this challenge "Cyber Police: An Idea" we propose may be an awesome solution. It is true that founding and activating an international council like ICCJ is the foremost important task before apply this initiative titling "Cyber Police: An Idea" and it's not as easy as we're talking about. But to save our cyber space for a better, safer virtual world the United Nations or the leading IT Giants today can play a vital role to implement this dream towards true. We keep our hope alive.

References Références Referencias

1. Adeyinka, O. (2008) 'Internet Attack Methods and Internet Security Technology', *Second Asia International Conference on Modelling & Simulation,* 77-82.
2. Amor, F.E.B. (2012), 'Policy Memorandum: Increase Cyber-Security via Internet Governance, Reporting and Awareness Reforms, The Journal of Science Policy and Governance, 2(1).
3. Anderson, et al. (2012), 'Measuring the Cost of Cyber crime, 1-31.
4. Aseef, N. et al (2005), 'Cyber-Criminal Activity and Analysis', White Paper, Center for Security & Privacy Solutions.
5. Aspnes, J., Feigenbaum, J., Mitzenmacher, M., Parkes, D., (2003) 'Towards Better Definitions and Measures of Internet Security', Position Paper.
6. Cleveland, F.M. 2008, Cyber Security Issues for Advanced Metering Infrastructure (AMI), IEEE.
7. Comprehensive Study on Cybercrime, UN Office on Drugs and Crime, February 2013.
8. David H. (2010), 'Cybercrime Coming of Age', White paper.
9. Doyle, C., (2013), 'Cyber-security: Cyber Crime Protection Security Act (S. 2111, 112th Congress)-A Legal Analysis, CRS Report for Congress Research Service.
10. Ericsson, G.N., 2010, 'Cyber security and power system communication-Essential parts of smart grid infrastructure', IEEE Transactions on Power Delivery, 25 (3).
11. François P. (2010) Cybercrime and Hacktivism, White Paper, McAfee Labs.
12. Fortinet, (2013) 'Cyber criminals Today Mirror Legitimate Business Processes', Cyber crime Report.
13. Grzybowski, K. M., (2012), 'An Examination of Cyber-crime and Cyber-crime Research: Self-control and Routine Activity Theory, Arizona State University.
14. Guerra, P., (2009) How Economics and Information Security Affects Cyber Crime and What It Means in the Context of a Global Recession, White paper.
15. Langner, R., Pederson, P., (2013) 'Bound to Fail: Why Cyber Security Risk Cannot Simply Be "Managed" Away', Cyber Security series, Foreign Policy at Brookings.
16. Library, C. (2009), 'Cyber-crime: An annotated bibliography of select foreign-language academic literature', Federal Research Division, Library of Congress.
17. Library, P. (2011), 'Cyber crime: Issues (Background Paper), Library of Parliament, Ottawa, Canada, Publication No. 2011-36-E.
18. Ponemon, I., (2011), Second Annual Cost of Cyber Crime Study, Benchmark Study of U.S. Companies, Research Report.
19. Software, G.F.I. (2011) 'Towards a comprehensive Internet security strategy for SMEs', GFI White Paper, 1-6.
20. Schaeffer, B.S., Chan, H., Ogulnick, S., (2009), 'Cyber Crime and Cyber Security', White paper.