IAA (Internet Access Account) Based Security Modal For Detection And Prevention Of Cyber Crime

Gaurav Singhal
M.Tech. Scholar
Department of Computer Science & Engineering
S. R. Tandan
Assistant Professor
Department of Computer Science & Engineering

Rohit Miri
Assistant Professor
Department of Computer Science & Engineering

Abstract

The current generations increasingly rely on the internet and advanced technologies to further their criminal operations. These criminals can easily leverage the internet and carry out the traditional crime such as disrupting illicit drugs and sex trafficking. Today's these concern often arise among a large discussion surrounding the Government to resolve this problem.

Conceptualizing cyber crime involve a number of key elements and questions that include where do the criminals act exist in the real and digital world and what technologies are involved in carry out the crimes. Researchers are trying to develop a system which can detect the actual criminals.

In this paper we investigate the security system using IAA(Internet Access Account) to detect access pattern of cyber criminals which act as a interface between user and internet access media to keep the actual identity of user, no matter where and what machine they are using.

1. Introduction

The rapid growth of the Internet, not just in terms of users, but also in terms of functionality has allowed entire industries to move their operations, and importantly their money, onto the Internet. This has lead naturally towards a prolific growth in criminal activity conducting solely through virtual means. Although cybercrime is not a new phenomenon, computers have always proved to be valuable targets, the essentialness of the Internet has necessitated a change in our understanding of security, risks and threats [7]. The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information [8].

Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity [5]. The distinction between cybercrime and other malicious acts in the virtual realm is the actor's motivation. Cyber criminals can exhibit a wide range of self interests, deriving profit, notoriety, and/or gratification from activities such as hacking, cyber stalking, and online child pornography. Without knowing the criminal intent or motivation, however, some activities of cyber criminals and other malicious actors may appear on the surface to be similar, causing confusion as to whether a particular action should be categorized as cybercrime or not. When referring to cybercrime incidents, terms such as cyber attack, cyber espionage, and cyber war are often loosely applied, and they may obscure the motives of the actors involved [1]. Scholars who perpetrated cybercrimes and are arrested by police told

the court that they did not know that what they did was unauthorized. Scholars not only need to learn how to use computers but also must learn the basic laws related to computer use and they should know about the ethical use of technological tools in the cyber world. There is an urgent need for data ethics and ethical education programs, and more scholars need to become involved. It is never too late to educate scholars and other internet users, regardless of their age [2].

One view of password research is that little progress has been made in the past 20 years. Despite countless attempts to dislodge them, passwords are more widely used and firmly entrenched than ever. The list of new technologies, research efforts and industry initiatives that have tried to supplant them is impressive in effort, and disappointing in outcome. We consider the possible reasons in an attempt to learn from this failure. We find that despite almost universal agreement on the desirability of finding something to replace passwords, much confusion has resulted from a failure to specify both the actual requirements needed of a replacement, and a relative ranking of such requirements. If a solution which satisfies all needs cannot be found, then "best fit" approaches should be explored. The premature conclusion that passwords are dead has generated some perverse effects. We argue that it is time to admit that passwords will be with us for some time and moreover, that in many instances they are the best-fit among currently known solutions. Two broad area of research suggested that identifies scenarios where passwords are indeed the best fit and encourages means to better support them; this could have tremendous positive impact given the scale of password deployment and systematically prioritizing competing requirements (as rarely can all requirements be met), and using this in comparing alternatives. We assert the need to better understand the loss situation (what the actual losses related to password compromises are, and what attack vectors they result from); our current data poor state means perception drives decisions more than evidence. Password research has been far from systematic [9]. Our aim is to promote a research agenda that both better supports passwords, and allows progress forward to diminish the cyber crime.

Cyber system is one of the most important resources of human to access information of whole world using internet service. Increasing use of internet makes it difficult to manage cyber system main responsibility of service provider is to avail the services that should be reliable, fast, easy to access and most important thing is legal use of internet services. One of the biggest challenges of cyber system is to detect and prevent cyber crime. Cyber crime can be any type of activities which try to harm cyber system. Table 1 show the list of cyber crime.

Increasing Public Influence

Type	Local Law Enforcement Level	National Security Level
Traffic Violations	Driving under influence (DUI), fatal/personal injury/property damage traffic accident, road rage	-
Sex Crime	Sexual offenses, sexual assaults, child molesting	Organized prostitution
Theft	Robbery, burglary, larceny, motor vehicle theft, stolen property	Theft of national secrets or weapon information
Fraud	Forgery and counterfeiting, frauds, embezzlement, identity deception	Transnational money laundering, identity fraud, transnational financial fraud
Arson	Arson on buildings, apartments	-
Gang / drug offenses	Narcotic drug offenses (sales or possession)	Transnational drug trafficking
Violent Crime	Criminal homicide, armed robbery, aggravated assault, other assaults	Terrorism (bioterrorism, bombing, hijacking, etc.)
Cyber Crime	Internet frauds, illegal trading, network intrusion/hacking, virus spreading, hate crimes, cyber-piracy, cyber-pornography, cyber-terrorism, theft of confidential information	

TABLE 1: Crime types at different levels [1].

2. Related Work

Existing Approach of cyber crime pattern detection was based on IP Address Tracking of Devices to prevent cyber crime. But now a day's most of the system user's using internet through different Cyber Offices, Internet Café, etc. and Owner of the service providers keep their identity manually (Register Entry). This technique is not accurate and safe to trace the actual culprit who has committed crime. This will lead failure of Cyber Crime Tracking System, and create problem of Owner. Cyber Crime detection system mainly works on [4]

(a) *Entity Extraction:* Entity extraction identifies particular patterns from data such as text, images, or audio materials. It has been used to automatically identify persons, addresses, vehicles, and personal characteristics from police narrative reports [4]

(b) *IP Identification:* Speaking at the opening of the East Africa Cyber Security Convention

2012 at the Laico Regency in Nairobi, permanent secretary at the Ministry of Information and Communications Dr. Bitange Ndemo said the Communication Commission of Kenya (CCK) will ensure every mobile operator will give each device a unique IP address that will make it possible to identify each individual gadget [4].

(c) Criminal Network Analysis: Criminal often develop networks n which they form groups or teams to carry out various illegal activities. Data mining task consisted of identifying subgroups and key members in such networks and then studying in interaction patterns to develop effective strategies for disrupting the networks [10].

3. Proposed Work

We proposed detect and prevent cyber crime

1. Integration of internet service providers (ISP) to generate unique ID and PWS for each user of internet.

2. Periodically Tracking system of user access pattern in devices.

In case of 1 User of internet need to enter his/her information for creating accounts that will be known as INTERNET ACCESS ACCOUNT (IAA), that account will remain alive according to the users choice he/she may create another one by deleting previously created one. There will be facility of password recovery with other security features for actual user identification. There should be strong interfacing between Web Browser developing organization and Internet Service Provider.

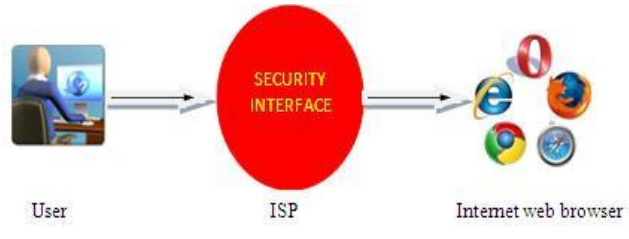

FIGURE 1: Security interface for internet access account

APPROACHE FOR USER DATA ACCESS PATTERN

Data Access Pattern, This strategy is based on detection of pattern according to user past data access pattern, we can identify the user past data easily and immediately interpret that What and How user had access data set.

Our proposed model periodically monitors the IAA of individual user and send the access records to the cyber crime department for targeting of culprit.

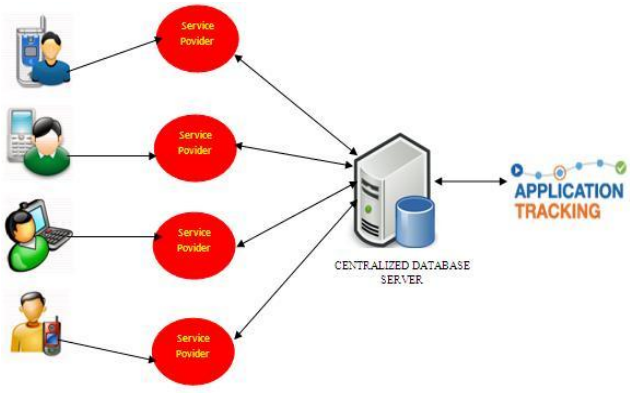

Figure 2: Periodically scanning of user access data

PROPOSED WORKING MODEL OF USER ACCESS PATTERN

- ✓ Connect with Internet Service Provider
- ✓ Open Internet Web Browser
- ✓ Create Login Account (IAA)
- ✓ Information of ISP and User will be saved in Centralized Database Server for future use
- ✓ Application tracking system will periodically check the IAA of individual active user to identify their data access pattern for cyber crime.
- ✓ Application Tracking System send data access pattern of the IAA user to Cyber Crime Detection and Prevention Organization.

4. Conclusion

The concept of this paper focuses on the security issue to protect our social system from unauthorized data access pattern by keeping the entire record of the individual user in centralized database and also maintaining the information users in different internet service providers. Approach (a) Keeping ID and PWD of Service Provider and (2) Keeping IP Address of System are not well suited to current criminal activities but our approach suggest to keep the record of user before accessing any information through internet.

Acknowledgment

We would like to thank Mrs Ranjeeta Tandan for her valuable support during the research work.

References

[1]. Kristin M. Finklea Specialist in Domestic Security Catherine A. Theohary Analyst in National Security Policy and Information Operations "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement" CRS Report for Congress *Prepared for Members and Committees of Congress.* January 9, 2013

[2]. Sattar J. Aboud Iraqi Council of Representatives Department of Information Technology Baghdad-Iraq sattar_aboud@yahoo.com "An Overview of Cybercrime in Iraq" The Research Bulletin of Jordan ACM, Volume II (II)

[3]. Y. Zhang, F. Monrose, M.K. Reiter. "The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis". ACM CCS 2010.

[4]. Zhong Xiu-yu School of Computer Science liaying University Meizhou, Guangdong, China e-mail: wch@jyu.edu.cn "A Model of Online Attack Detection for Computer Forensics 2010 International Conference on Computer Application and System Modeling (ICCASM 2010).

[5]. Dr.B.Muthukumaran, Chief Consultant, Gemini Communication Ltd., "cyber crime scenario in India" criminal investigation department review- January, 2008

[6]. S. Kaza, D. Hu, and H. Chen, "Dynamic Social Network Analysis of a Dark Network: Identifying Significant Facilitators," in Proc. IEEE Intelligence and Security Informatics, New Brunswick, NJ, USA, 2007, pp. 40-46

[7]. Hemavathy Alaganandam – The Evolution of Cybercrime, Pravin Mittal – Cybercrime Case Study: Internet Bots, Avichal Singh – Cyberforensics, Chris Fleizach – Legal Policies and The Future of Cybercrime "Cybercriminal Activity". December 6th, 2005

[8]. Mc. Connell A report on "Cyber Crime . . . and Punishment?" Archaic Laws Threaten Global Information www.mcconnellinternational.com with support from www.witsa.org, December 2000.

[9]. Cormac Herley Microsoft Research, Redmond, USA, Paul C. van Oorschot Carleton University, Ottawa, Canada "A Research Agenda Acknowledging the Persistence of Passwords"

[10]. Hsinchun Chen, Wingyan Chung, Jennifer Jie Xu, Gang Wang, Yi Qin, University of Arizona , Michael Chau, University of Hong Kong "Crime Data Mining: A General Framework and Some Examples" Published by the IEEE Computer Society, 0018-9162/04/$20.00 © 2004 IEEE

[11]. Hsinchun Chen, Wingyan Chung, Yi Qin, Michael Chau, Jennifer Jie Xu, Gang Wang, Rong Zheng, Homa Atabakhsh "Crime Data Mining: An Overview and Case Studies"{hchen, wchung, yiqin, mchau, jxu, gang, rong, homa}@bpa.arizona.edu Artificial Intelligence Lab, Department of Management Information Systems, University of Arizona, Tucson, AZ 85721, USA http://ai.bpa.arizona.edu/

[12]. Shyam Varan Nath "Crime Pattern Detection Using Data Mining" Florida Atlantic University/ Oracle Corporation SNath1@FAU.edu / Shyam.Nath@Oracle.com +1(954) 609 2402

[13]. Li Ding, Dana Steil, Matthew Hudnall, Brandon Dixon, Randy Smith, David Brown, Allen Parrish "PerpSearch: An Integrated Crime Detection System" Computer Science Department, University of Alabama Tuscaloosa, AL 35487

Gaurav Singhal is pursuing M.Tech(CSE) in the department of CSE from Dr. C.V. Raman University, Bilaspur. He received his B.E.(IT) from Gurughasidas Central University, Bilaspur, Chhattisgarh, India. He is certified in Cyber crime and law from Indian Law Institute New Delhi. His interest area includes Cyber Crime, Cyber security, Web design and development and System Administration.

S.R. Tandan is Currently Assistant Professor in the department of CSE, and Pursuing Ph.D from Dr. C.V. Raman University, Bilaspur, Chhattisgarh, India. He received his M.Tech.(CS) form BITs Mesra and BE(CSE) from NIT, Raipur, His interest area includes Soft Computing, Information Retrieval System and Mobile Robot Navigation, and Cyber Crime.

Rohit Miri is Currently Assistant Professor in the department of CSE, and Pursuing Ph.D from Dr. C.V. Raman University, Bilaspur, Chhattisgarh, India. He received his M.Tech(CSE) form GEC Pune and BE(CSE) from GEC, Raipur, His interest area includes Application of Soft Computing.