The Technoarete Transactions on Recent Advances in Cyber security and Digital Forensics Journal

Volume No. 12

Issue No. 2

May - August 2023

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

The Technoarete Transactions on Recent Advances in Cyber security and Digital Forensics Journal

The Technoarete Transactions on Recent Advances in Cyber security and Digital Forensics Journal

(Volume No. 12, Issue No. 2, May - August 2023)

Contents

Cyber Security Challenges & Online Frauds On Internet

Krishan Tuli*, Dr. Neenu Juneja*
*Chandigarh Group of Colleges, Landran, Mohali

ABSTRACT

The fast evolution of on-line and mobile channels has etched out new markets and brought large opportunities for aborting and established organizations alike. However, sadly the past decade has additionally witnessed important disruption to ecommerce payment processes and systems. The interconnected, anonymous and fast nature of those channels has inevitably diode to the event of malicious threats targeting ecommerce and retail services corporations, their individuals and their customers.

These e-crime and digital fraud threats still evolve apace, with attackers utilizing progressively refined techniques to focus on vulnerabilities in individuals, processes and technologies. The e-crime threats, if with success completed, will undermine essential digital services, cause important injury to complete reputations, and end in wide money and operational pain for organizations and their customers.

Cyber crime is rising as a significant threat. Worldwide governments, police departments and intelligence units have begun to react. Initiatives to curb cross border cyber threats are taking form. Indian police has initiated special cyber cells across the country and have started educating the personnel. This text is a trial to supply a glimpse on cyber crime in Asian country. This text is predicated on numerous reports from journalism and news portal.

Key words: Cyber crime, Hacking, Phishing, Cyber squatting, e-crime and digital fraud

1. INTRODUCTION

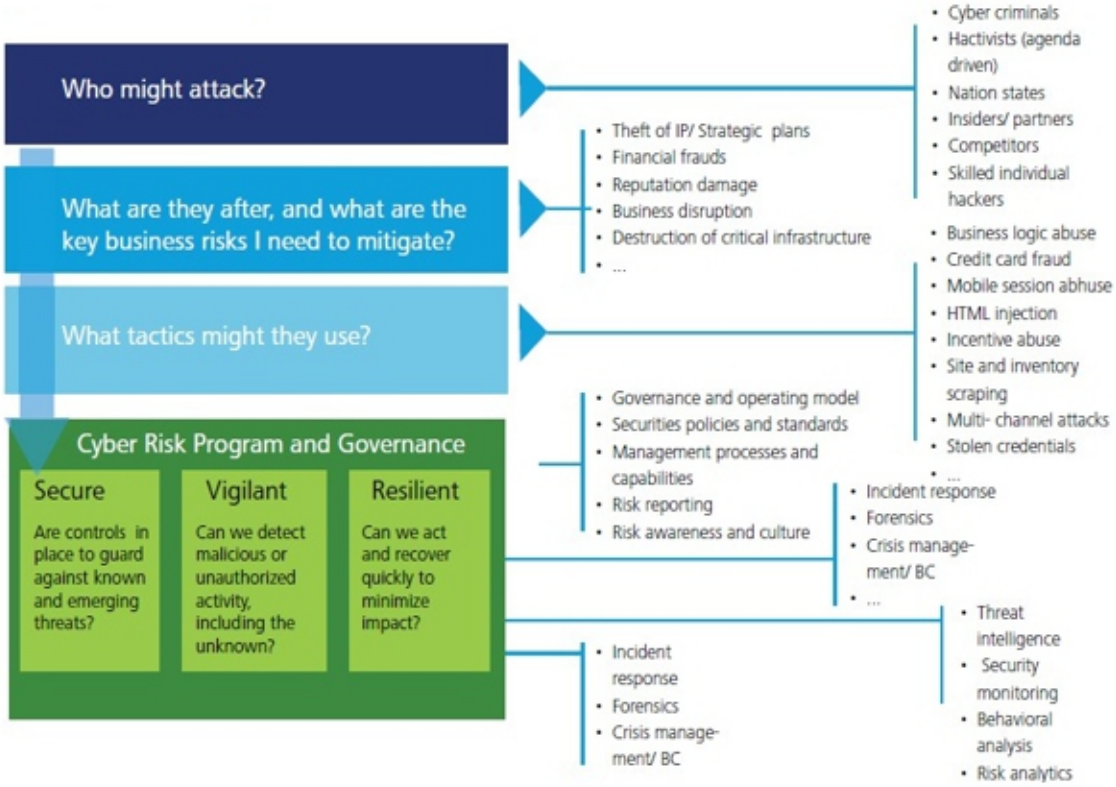
Worldwide, regulators are also turning their attention to these threats, with enhanced scrutiny of organizational resilience and the introduction of stringent compliance requirements. The challenge that ecommerce services firms are facing is to deliver richer, integrated services, through multiple remote and digital channels, under significant cost restraint, and in the face of sophisticated e-crime threats. Recent cyber-attacks highlight the urgency for retail organizations to contend with ever increasing risks to customer protection, continuity, fiduciary responsibility, and operations. In order to achieve the security objectives, it is necessary to recognize that the security of the services and the protection of the customers' data are essential. To this end, and specifically to support the current security equation, it is

necessary to have an enterprise wide target customer security model. This should be designed to deliver enhancements to both customer-facing and back office security capabilities, and in particular to improve existing security defenses for remote online, telephone and mobile banking channels.

As far back as the early 1990s, the Internet was argued to be a unique medium showing the fastest speed of diffusion in human history (Nguyen and Alexander, 1996). Today, there are very few people whose lives are not affected beneficially and/or harmfully by the technology of the Internet era. On the positive side, the ability to share and exchange information instantaneously has provided unprecedented benefits in the areas of education, commerce, entertainment and social interaction. On the negative side, it has created increasing opportunities for the commission of crimes – information technology has enabled potential offenders to commit large-scale crimes with almost no monetary cost and much lesser risk of being caught. Compared to perpetrators of traditional economic-motivated crimes (e.g., burglaries, larcenies, bank robberies), online fraudsters are relatively free of worry from directly encountering law enforcement and witnesses.

With the continuous advancement of Internet technology and personal computing devices in recent years, Internet crimes have risen to an alarming level. For instance, in the U.S., the National White Collar Crime Center reported a 33.1% increase in citizen complaints of Internet crimes between 2007 and 2008, and this figure is reflective particularly of the increased incidence of identity theft. Another source of information also indicated that the number of identity thefts increased more than tenfold within a 9-year period – growingfrom 31,140 incidents in year 2,000 to 313,982 in 2008. In addition, identity theft remained the top one complaint category filed by the victims across years. Evidence from victimization survey also pointed out that about 5% of Americans aged 16 and above was victims of successful and attempted identity theft within two years, and the direct financial damage to the victims were as high as 16 billion dollars. These statistics coincide with the notion of ―Crime of the New Millennium as the phenomenon quickly emerged in the 21st century. On the basis of this upward trend, we aim to examine identity theft from an analytic angle with a focus on the expanded versatilities of this contemporary crime. In the present article, the mechanism of identifying an individual is first discussed, followed by the definition and typology of identity theft. Elements and methods of identity theft will be deconstructed for classification, and subsequent discussions will be emphasized on recent variations in online fraud. The study will conclude with the implications of the close relations between identity theft and the fast growing Internet, and suggestions for improved means of identity protection.

2. CYBER RISK TAXONOMY



3. EVOLVING DEGREE OF THREATS

The threat landscape is ever evolving and increasingly challenging. Customer data with retailers and e-commerce firms has been increasing at a rapid pace. As per the incremental service provisioning in e-commerce, more data will be generated in the next two years than was generated ever before. Access to all this data has made the retail industry one of the primary targets for cyber-attacks. Some of the key threats today's organizations are vulnerable to include:

- User account takeover via robotic attacks, password guessing, HTML injection and Man-in the-Middle or Man-in-the-rower. Account peeking is a very common behavior by fraudsters as it allows them to validate the login credentials, identify higher value accounts and understand the controls which must be defeated to complete future unauthorized transactions.

- Business Logic Abuse or the use of portal's functionality for malicious or exploitative purposes (e.g., abuse of loyalty point programs or shopping cart functionality, fraudulent account set up, Scripted attacks to find valid coupon codes.). Impact of such abuse may include effect on the genuine customer due to unauthorized use of coupon offers, overall decrease in revenue due to offer abuse, incremental portal overhead due to scripted attacks and site scraping by resellers or coupon aggregator sites.

- Distributed-Denial-of-Service or DDOS attack on the application layer where a deluge of page requests coordinated by a bad actor overwhelms the server and brings the site down.

- Site or Architecture Probing to gather as much information about site structure and security vulnerabilities as possible to prepare for an attack on that site.

- Site & Inventory Scraping or data theft perpetrated by copying large amounts of data from a website, typically via automated scripts.

4. ISSUES

Cyber Security issues lead to brand degradation and change in consumer behavior. Attacks are exploiting weaknesses in traditional controls, some very destructive. Traditional controls around Point of Sale and other IT systems are necessary but not adequate – greater emphasis must be placed on preventative controls, rapid detection, and rapid response.Retail innovations that drive growth (e.g. Digital, Omni-channel retailing, social etc.) also create cyber risk. Cyber risk management strategy must be a component of business strategy, and can't simply be delegated to IT.

1. Lack of appropriate control and transparency add to cyber security risk. Despite growing frequency and sophistication of cyber-attacks on the ecommerce industry, payment settlement agreements between credit card networks, the banks and the merchants have remained a closely guarded secret. Neither the government nor any database shares the list of defaulters with the public. Banks and credit card companies determine fault on a case-by-case basis through private contracts with individual merchants. Fines and the reasons for them remain sealed. Due to the lack of transparency, the majority of customers is not aware of any cyber security breaches and remains vulnerable to cyber attackers.

2. E-commerce firms and retailers face heat to increase efforts to ensure greater cyber security. In the wake of recent data-security breaches at large retail corporations, retailers have been pushed to spend more to ensure tighter customer data security. While the traditional retailers have been investing millions of dollars to compete with online retailers the cyber-security threats have multiplied their operational expenditures.

3. Third-party cyber risk As firms look to exploit the competitive edge they gain from the data they capture about their customers, they are increasingly leveraging the expertise of third parties

Such as analytics specialists and social marketers. Couple this with increasingly lengthy and complex supply chains; retail organizations are increasingly becoming enmeshed in very complex, interconnected value chains where sensitive data is shared and dependencies are introduced between business critical systems. Firms are rapidly waking up to the realization that they often have very little visibility in these areas, and that they do not have a good understanding of where their customers data is travelling, and what their risks are. We should focus on to map these interconnections, develop robust risk management frameworks, and provide firms with assurance that they have understood and actively managed the risk of each partner relationship.

4. Inadequate joint efforts by banks and retailers to counter cyber security threats While collaborated efforts are expected to ensure tighter cyber-security, banks and retailers differ in terms of responsibility sharing. Banks want retailers to bear more of the costs of replacing cards after breaches occur whereas retailers say banks have been slow to adopt new, more secure debit card technology.

5. IDENTITY THEFT BREEDERS AND DAMAGES

Breeder identification can be gained by any means; its significance is in its use for obtaining additional, separate, false, or fraudulent means of identification controlled exclusively by the perpetrator without the victim's knowledge, or ability to know. An identity thief can fraudulently use obtained personal information to generate other means of identification, ranging from open new accounts, apply for loans and credit cards, to receive governmental benefits (General Accounting Office, 1998). Breeder ID means occur most often in the course of committing credit card fraud for the purpose of establishing the —authenticity required to obtain a new account, although their incidence is fairly frequent in conjunction with check fraud, document fraud/counterfeiting, signature forgery, and bank/loan fraud as well.

Thus, as long as the identity thieves have knowledge of or keep a record of the stolen identities, deeper and long-term damage to the victims can explode or surprise the victims at any time after the initial damage. For that reason, in addition to financial and credit damages, some victims of identity theft may suffer from varied psychological, social, and/or legal disturbances. These hidden costs are considerable but usually are not addressed. The recent supplement of the National Crime Victimization Survey shed some light in this regard – the emotional distress experienced by some types of identity theft victims (e.g., open new account, stolen personal information) were comparable to an average violent crime victim.

6. THE ELEMENTS AND OFFENDING METHODS OF IDENTITY THEFT

An identity thief may reach others identifying information through various means. The examples of identity theft are, probably, limited by each individual's imagination but expandable by the escalation of technology advancement. Here, we employ two dimensions to deconstruct the seemingly complicated incidents of identity theft.

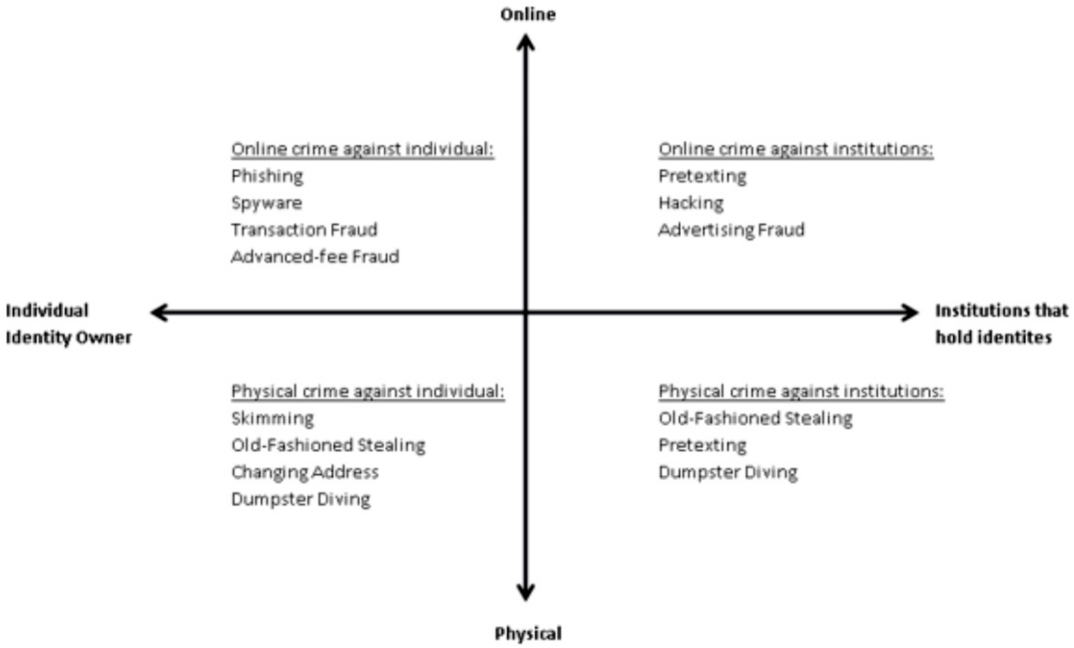


Figure 1: Deconstructing Types of Identity Theft

The horizontal dimension is the source from which identity thieves obtain the identifying information. On one end of this dimension is the individual victim; on the other end are institutions that legitimately store client personal information. Stealing each individual's personal information generally is easier than penetrating institutions security protocols. However, once identity thieves penetrate layers of protection employed by those institutions, the loss of identity information is often massive and the damages are much more substantial.

The vertical dimension is the place where the identity-stealing conduct occurs. Identity thieves either violate social rules implemented in the physical world (e.g., steal individual victim's mails like bill statements containing personal information; bribe or coerce institutions employees who have access to clients personal information) or deceive Internet users of different services. Sometimes, the financial damage of identity theft does not begin until fraudsters purchase identity information that was collected illegitimately in the first place. The underground data warehouses that sell identity information online can contribute greatly to financial disaster for individuals.

The purpose of recognizing these two dimensions is threefold. First of all, these two dimensions help identify major dimension of paths that those identities are or can be stolen (cyberspace vs. physical space; individuals vs. institutions). The classification also lays out aframework for detailed examinations of each type of identity theft. Without this foundation, further elaboration and analysis are limited.

Dumpster Diving/Trashing

Identity thieves can rummage through trash of residences or businesses looking for bills, paper documents, storage devices, and even discarded credit cards containing personal information. This way of stealing identifying information is fairly labor-intensive and is restricted to limited geographic areas. Consequently, suspects are relatively easy to locate by law enforcement agencies.

Old-Fashioned Stealing

Via traditional stealing methods, identity thieves either target goods that include personal information or obtain victims personal identification as a byproduct of pickpockets. The targets are those usually containing personal identifying information, such as wallets and purses, mail, especially bank and credit card statements, pre-approved credit offers, new checks, and tax information. Old-fashioned stealing can also occur when offenders steal personnel records from institutions or bribe/coerce /deceive employees who have the access.

Changing Address

Identity thieves divert victim's mail, particularly billing statements, to another physical location by completing a change of address form. This type of identity theft is usually conducted by filing the change-of-address form with the U.S. Post Office. Thus, the U.S. Postal Inspection Service is intuitively the corresponding law enforcement agency accountable for preventive/deterring actions.

Skimming

Skimming occurs when legitimate transactions are processed by swiping credit/debit cards in retail stores or any other type of institutions where swiping cards is required. Generally, the credit/debit card numbers are stolen by a special storage device built in or attached to the swipe machines. The card information is stolen simultaneously when a legitimate business transaction occurs. The thief can be

anyone who has access to the swipe machine, including, but not limited to, technicians of swipe machine vendors, and retail stores' staffs/owners. Skimming sometimes can be completed by perpetrators who attach a slim seem-like-real cover on a given ATM machine.

Pretexting

Pretexting involves a series of deceptive actions that obtain victim's personal information from the owner of the information, institutions that hold the information, and/or other individuals who may have knowledge of the information. Pretexters may pretend to have different roles (e.g., customer service representatives, survey researchers, the victims or the victim's authorized representatives) in order to collect pieces of victim's personal information. In sum, as a technique of social engineering, pretexting is a cluster of pretenses with the ultimate intention of taking financial advantage of the victims.

Hacking

Hacking was perceived as a creative activity that helped overcome the limitations of computers about a half century ago when such machines were not common, but the image of hacking changed, largely influenced by the media, to a threatening force in 1980s (Britz, 2009). The developed categories of hackers (e.g., white hat, black hat, and gray hat) are usually not mutually exclusive (McQuade, 2006; Parker, 1998) because whether their intention is malicious is uncertain from discovered evidence. Even though contemporary hacking is usually associated with stealing valuable information other than personal information (e.g., business secrets, confidential documents) and properties (e.g., copyrighted artifacts, billing) in cyberspace, it can be used as a means to obtain identifying information. Stolen identity information sometimes can be a —by-product of hacking for other purposes. Hacking is attractive for the reason that offenders do not have to physically appear at the —crime scene to —rob or —steal from institutions. Instead, exploiting online financial and billing systems is enough to illegitimately gain privileged information. Especially after database technology is widely utilized by varied institutions to store and manage huge amounts of data, a copy of the database itself is very valuable in the black market. As more money, transactions, and even resources are moved to and managed in the virtual space for the sake of efficiency and convenience, it is likely hacking will remain a seductive means of identity stealing.

Phishing

Phishing is the pursuit of personal financial information with the intent to commit fraud by relying upon the recipient's inability to distinguish bogus emails, messages, web sites, and other online content, from legitimate ones – they all designed to appear with legitimacy.Phishers can use a combination of tricks involving web sites, emails, and malicious software to deceive potential victims for the purpose of stealing their personal identity information and financial account credentials. The significance of phishing is that it enables remote identity theft. Precisely, phishing significantly reduces the risk and the costs to identity thieves because no physical contact, such as dumpster diving or old-fashioned stealing, is needed to complete the crime. Consequently, the chance of being caught at the crime scene is virtually eliminated. Another significance of phishing is its popularity in the U.S. where the largest proportion (25%) of phishing sites are hosted, compared to other countries in the world.

A typical phishing attack begins when phishers (offenders) send out massive amounts of email (spam) or messages with bait, which is intended to trigger the targeted victim's intuitive interests. Usually, the unsolicited emails ask recipients, with a sense of urgency often exaggerated by an alleged security breach, to log onto the provided URL and confirm their personal information details, particularly their password of access. Typically these fraudulent emails are designed to look like they are from large and well-known financial institutions, such as Bank of America, Citigroup, or PayPal. In the past several years, however, observers have witnessed that phisher's Spyware (Malicious Software).

7. ONLINE FRAUDS

In general, fraud refers to the act of taking advantage of others, largely motivated by economic reasons, via varied deceptive means. Online fraud intuitively refers to those conducted and/or facilitated by the Internet. As discussed earlier, identity theft is the inception of many fraudulent and criminal activities, but it does not necessary means that identity theft is the start of all online frauds.

Business Transaction Frauds

The network of computer networks creates a cyberspace where business transaction platforms, such as stores, can be operated virtually. In some cases, the same products demonstrated in a company's physical stores or printed catalogues can be found in their corresponding online stores. The most significant difference between buying from a physical or virtual store is the method of business transactions, including both the payment and the delivery of products or services, and this joint venue is where online frauds usually emerge.

Online Advertising Frauds/Advertisement Click Frauds

Cyberspace has created new business models, as well as new ways to advertise. One of the most common, and probably the least intrusive forms of advertising online is a banner on Web sites that invites interested customers to click on it and view the details. Once an Internet user clicks on the banner, s/he is linked to another site of products/services and the information system automatically records the click for later cumulative counts. The corresponding business model for charging the advertising fee is typically based on how many times the banner was clicked. Consequently, a particular fraudulent behavior online is to defraud Internet advertising billing systems by employing individuals or software to massively click on the advertisements. Outsourcing the task of fraudulent massive clicks to countries with cheap human labor becomes a rational choice to offenders.

Advanced-Fee Frauds

Advanced-fee frauds, again, is not something new in civilized human history, but this type of fraud has regained attention for its rapid increase use of email. The latest version of this fraudulent form is frequently referred as Nigerian 419 scam, named after the Nigerian criminal code section (Edelson, 2003). Online advanced-fee frauds generally begin with the receipt of a fake formal letter claiming a large amount of money needs to be transferred through a third-party bank account.

8. CONCLUSION

The rapid pace at which technology is changing has provided large opportunities for organizations to develop new business models, services, and products. While the digital revolution has transformed the way we do business, it has also created complex and sophisticated security issues. Assets and Information that were once protected within the organization are now accessible online; customer channels are vulnerable to disruption; criminals have new opportunities for theft and fraud. With organizations growing organically and inorganically, complexity of managing businesses & security operations are also becoming complex.

Identity theft and online frauds are contemporary crimes for profit. As the world market continues to progress toward transferring and managing money conveniently on the Internet, online frauds and scams are inescapable. As long as identity theft and online frauds are relatively easy paths to financial gain, the use of these fraudulent means will increase with the growth of the Internet. With the movement of processing transactions totally online, online fraud has gradually transformed from a hybrid

cybercrime to a true cybercrime. Collectively, cyberspace has become such an attractive place where suitable targets like personal information increase in value while effective guardians typically fall behind. Anti-fraud efforts must be accelerated and orchestrated proficiently to make online scams difficult for offenders.

REFERENCES

1. *Crume, J. (2000). Inside Internet Security: What Hackers Don't Want You to Know. Harlow: Addison-Wesley.*
2. *Cukier, W. and A. Levin. (2009). Internet fraud and cyber crime. In Frank Schmalleger and Michael Pittaro (ed.) Crimes of the Internet. Upper Saddle River, NJ: Pearson Education Inc.*
3. *Economic Crimes Policy Team (1999). Identity Theft: Final Report. United States Sentencing Commission.*
4. *Albert, M. R. (2002). E-buyer beware: Why online auction fraud should be regulated. American Business Law Journal, 39(4): 575.*
5. *Britz, M. (2009). Computer Forensics and Cyber Crimes: An Introduction. Upper Saddle River, NJ: Pearson Education Inc.*
6. *Federal Trade Commission. (2003). Overview of the Identity Theft Program: October 1998 – September 2003. [online]. Available from: http://www.ftc.gov/os/ 2003/09/timelinereport.pdf [Accessed 28/08/2010].*
7. *Federal Trade Commission. (2009). Consumer Fraud and Identity Theft Complaint Data: January – December, 2008. [online]. Available from: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/ sentinel-cy2008.pdf [Accessed 20/08/2011].*
8. *Federal Trade Commission. (2010). Consumer Fraud and Identity Theft Complaint Data: January – December, 2009. [online]. Available from: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/ sentinel-cy2009.pdf [Accessed 20/08/2011].*
9. *Huang, W. & Wang, S. K. (2009). Emerging Cybercrime Variants in the Socio Technical Space. In B. Whitworth & A. de Moor (ed.) Handbook of Research on Socio-Technical Design and Social Networking Systems. Hershey, PA: Information Science Reference, IGI Global.*
10. *Jasper, M. C. (2002). Identity Theft and How to Protect Yourself. Dobbs Ferry, NY: Oceana Publications.*

Open Source Rules For Real-time Protection Of Web Server

Ekaterina Dudin, Anna Otsetova
Asstt. Prof., PhD, University of Telecommunications and Post, Sofia, Bulgaria
Asstt. Prof., PhD, University of Telecommunications and Post, Sofia, Bulgaria

ABSTRACT

Modern web-based applications often remain open for hacker attacks and vulnerabilities of the server operating system. This fact requires the additional protection of the web server and the software it uses. This paper presents the main types of hacker attacks and the ability to prevent them using ModSecurity-based protection rules provided by Open Web Application Security Project. The ModSecurity modul, applying a set of rules for protection by inspecting incoming traffic and the response to these requests by the server was discussed. Practical results of their impact on various attacks - HTTP (fingerprinting), DoS (Denial of Service), DDoS (Distributed Denial of Service), SQL injections, etc. were presented.

Keywords: ModSecurity, Rules, HTTP fingerprinting, DoS, DDoS, SQL injections

1. INTRODUCTION

Attacks to modern web applications are characterized by a different approach, scope and purpose [3]. To achieve information security of modern web applications, the following options are use:

- Firewalls;
- Administrative accounts for access to databases;
- Terminate access by using the Internet Protocol Message Protocol (ICMP) and Simple Network Management Protocol (SNMP);
- Providing protection for both the operating system and the used applications;
- Regular updates and patches on servers,
- Checking and validating the input data in order to verify code.

In order to ensure stable protection of a web server, it is necessary to periodically assess the known vulnerabilities, in parallel with the updating of the software used and the regular updating of the used technologies [6].

This paper proposes the use of open source real-time server protection policies provided by the Open Web Application Security Project (OWASP).

The purpose of the report is to offer practical solutions for developing real and complexrules for the protection of a real-time web server.

2. BASIC WEB SERVER ATTACKS

The most common hacker attacks on modern web servers are [10]:

1. HTTP fingerprinting attacks.
   Each server is characterized by its unique profiling. This circumstance enables the identification of both the type and the version of the software that is used [7]. HTTP fingerprinting attacks are uniquely identifiable (on the fingerprint principle). To scan for HTTP attacks, programs such as Httprint (operating under Windows, Linux, and Mac OSX Httprecon) are used [2].

2. DoS (Denial of Services).
   The purpose of a DoS attack is to block the server by filling its operating memory and fully occupying its resources. The sender sends a large number of immediate requests, thus making it difficult to service the real users [3, 9]. The fact that attacks on the server are multiple queries from one user makes it easier to protect.

3. DDoS (Distributed Denial of Service).
   DDoS attacks aim to make the server resources inaccessible for a certain period of time or permanently. In these cases, the server does not distinguish the malicious from the legitimate request, since both types of requests use the same protocols and ports [2]. The main steps to prevent their action are:

- Ensuring bandwidth surplus for incoming traffic - this is one of the easiest ways to protect a server from lower-level DDoS attacks, but this approach is costly;

- Using an Intrusion Detection System (IDS);

- Using a product to protect against DDoS attacks. Several manufacturers offer devices designed specifically to detect and provide DDoS protection and prevention that are specifically designed to detect and frustrate the DDoS attacks;

- Back up Internet connection with a separate base with Internet addresses for critical users. This alternative is used in case the primary chain is overloaded with malicious queries.

Unlike DoS attacks, DDoS are sent from hundreds of sources simultaneously, this circumstance make protection complex and even in some cases impossible [7]. This paper does not offer comprehensive DDoS attack protection rules, as DDoS attacks are filtered at the internet provider level.

4. SQL injections - a code injection technique used to attack a web application without filtration or other protection methods [8]. This type of attack allows the use of the database information on the server [2].

5. Shell command execution - a combined technique for achieving maximum effect. The effects of these attacks consist of three basic steps [7, 12]:

First step:
Select applications vulnerable to SQL injection, and then create a .php extension file that records the desired content of the attacker.

Step Two:
Create a file containing the System command ($ _ REQUEST ['cmd']).

Step Three:
Deleting server content - www.site.com/exec.php?cmd=rm-rf/.

6. Attack Brute force attacks - used to break passwords by using all possible combinations of letters, numbers and characters set in the attack algorithm. An effective protection measure for this type of attack is to limit the number of attempts from one source to identify a user [5].

3. OPEN SECURITY POLICIES USAGE

ModSecurity is a web-based firewall application [9]. It controls inbound and outbound data streams by applying a set of real-time protection rules. The principle of this module is presented in Figure 1 [1].

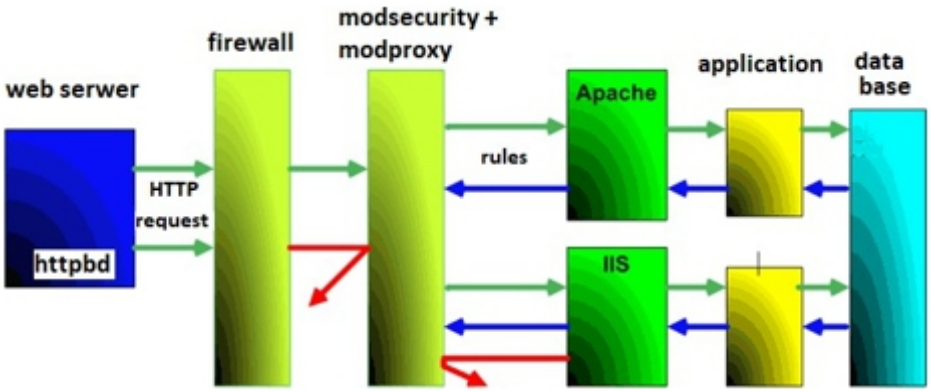


Fig. 1. ModSecurity

When detecting suspicious traffic or abnormal behavior on the part of the user, ModSecurity acts as a borderline that verifies malicious content by skipping or blocking requests received according to the result of the previous step. ModSecurity activates procedures and offers a number of options, including some injecting content into communication, as well as a full.

HTTP transaction entry [1, 2].
The structure of the archive and the access to these rules are presented on the OWASP Foundation's official website: https://github.com/SpiderLabs/owaspmodsecurity-crs [11].

The main benefits of using these policies are:
Flexibility when creating and editing security rules - using text editors such as notepad, vi, nano, emacs, etc. [4, 6].

- Possibility to create own rules,
- An opportunity to develop comprehensive and strong protection rules.

When an attack is detected, the ModSecurity module provides the option of selecting a user action option [11]:

- recording the information in a log,
- blocking incoming traffic,
- sending an e-mail to the site administrator,
- sending commands to the server operating system,
- running a certain external script file.

4. PRACTICAL IMPLEMENTATION OF COMPLEX RULES FOR PROTECTION

ModSecurity is compatible with Apache Foundation, Nginx, and Microsoft Internet Information Services (IIS).

This paper proposes the use of a virtual container installed with OS Ubunto 14.04.3, Apache 2.4.27, PHP, MySQL and OWASP ModSecurity Core Rule Set (CRS) Version 3. In addition, a WordPress system is installed to provide additional protection from common attacks and specific vulnerabilities.

For the purpose of our paper, the following ModSecurity configuration was used:
root@example:/etc/modsecurity# tree
modsecurity_crs_10_setup.conf
modsecurity_crs_11_dos_protection.conf
server-baner-protection.conf
shell-exec-block.conf
sql-injection-block.conf
wp-brute-force-block.conf

1. Brute Force Attack Protection
   The following logic is suggested - when entering a user and password, the server responseshave the following statuses:

- 200 for wrong password and return page to login,
- 302 Redirect - redirecting to the administrative part when correctly identified to the system,
- 401 - deny access and log into the log file of an "ip address blocked" message.

Applying this mechanism we check the status of the response to the client and provide the opportunity to count wrong attempts. Upon reaching a certain limit, the host is blocked for a certain time (for example, for 5 minutes - 10 attempts). When sending 10 POST queries to /wp-login.php, the server responds to status 401, blocking the attacker and writing the log file data to the server.

==> /var/log/apache2/wp-access.log <==

192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601

```
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 200 3601
192.168.254.6 - - [12/Une/2017:09:14:16 +0200] "POST /wp-login.php HTTP/1.1" 200 3601

==> /var/log/apache2/modsec_audit.log <==

blog.example.dev 192.168.254.6 - - [12/ Une/2017:09:14:15 +0200] "POST /wp-login.php HTTP/1.1" 401 458 "-" "-" VsAkrH8AAQEAABF@0vUAAAAB "-" /20160214/20160214-0854/20160214-085436-VsAkrH8AAQEAABF@0vUAAAAB 0 1110

md5:0e2b472e2caf97d6a685435ef42b058e

==> /var/log/apache2/wp-access.log <==

192.168.254.6 - - [12/Une/2017:09:14:16 +0200] "POST /wp-login.php HTTP/1.1" 401 458
```

2. Protection from SQL ingection code is expressed in the use of a set of OWASP rules. A content file was used to demonstrate the effectiveness of the rules:

```
#OR 1
# DROP sampletable
# DROP/*comment*/sampletable
# DR/**/OP/*bypass blacklisting*/sampletable
# SELECT/*avoid-spaces*/password/**/FROM/**/Members # SELECT /*!32302 1/0, */ 1 FROM tablename
#' or 1=1# #' or 1=1-- -
#' or 1=1/*
#' or 1=1;\x00
```

When attempting to deliver a malicious code, the server response is instantaneous, with the first request:

==> /var/log/apache2/wp-error.log <==

[Wen Une 12 09:16:21.680851 2017] [:error] [pid 4477] [client 192.168.254.6] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(/*!?|*/|[';]--|-- [\\\\s\\\\r\\\\n\\\\v\\\\f]|(?:--[^-]*?-)|([^\\\\-&])#.*?[\\\\s\\\\r\\\\n\\\\v\\\\f]|;?\\\\x00)" at ARGS:test. [file "/etc/modsecurity/sql-injection-block.conf"] [line "18"] [id "981231"] [rev "2"] [msg "SQL Comment Sequence Detected."] [data "Matched Data: /* found within ARGS:test: DROP/*comment*/sampletable"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "8"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "blog.example.dev"] [uri "/"] [unique_id "VsAnhX8AAQEAABF9zVgAAAAA"]

==> /var/log/apache2/modsec_audit.log <==

blog.example.dev 192.168.254.6 – [12/Une/2017:09:16:21+0200] "GET /?test=DROP/*comment*/sampletable HTTP/1.1" 403 279 "-" "-" VsAnhX8AAQEAABF9zVgAAAAA "-" /20160214/20160214-0906/20160214-090645- VsAnhX8AAQEAABF9zVgAAAAA 0 1708 md5:e04d1076a86e8d56b7cd506d2581f14d

==> /var/log/apache2/wp-access.log <==

192.168.254.6 – [12/Une/2017:09:16:21+0200] "GET /?test=DROP/*comment*/sampletable HTTP/1.1" 403 279

3. Shell command execution protection

To prevent this type of attack, a "drop" method is used instead of "deny," as a result of the applied rules, the attacker receives a blank response from the server [7]. In this way, no resources are assigned to respond to the interrogated request, but the attacker is deluded (Figure 2).

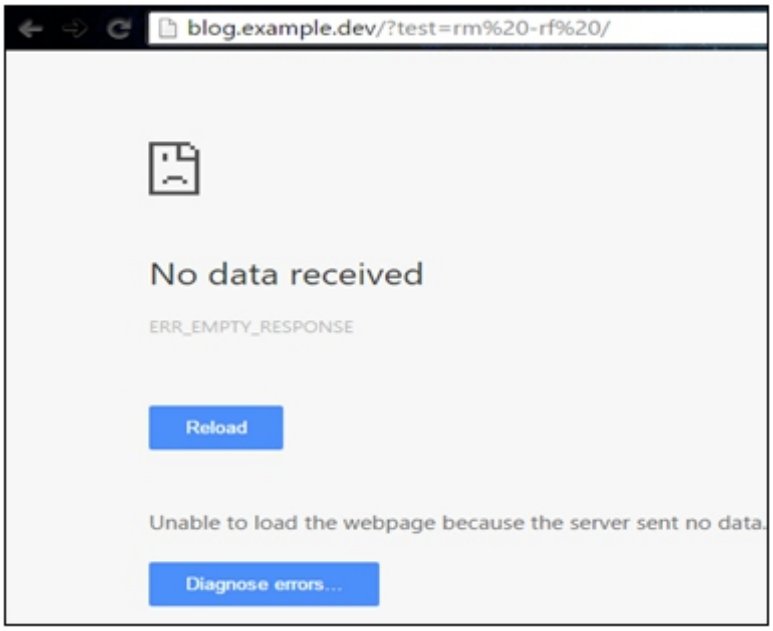


Fig. 2. Shell command execution protection

4. DoS attack protection is provided by experimental rules by setting the following configuration parameters for the system: 60 sec time interval, 100 requests in the activation time interval and 5 min blocking time.

The server response after application of those protection rules is presented in Figure 3.

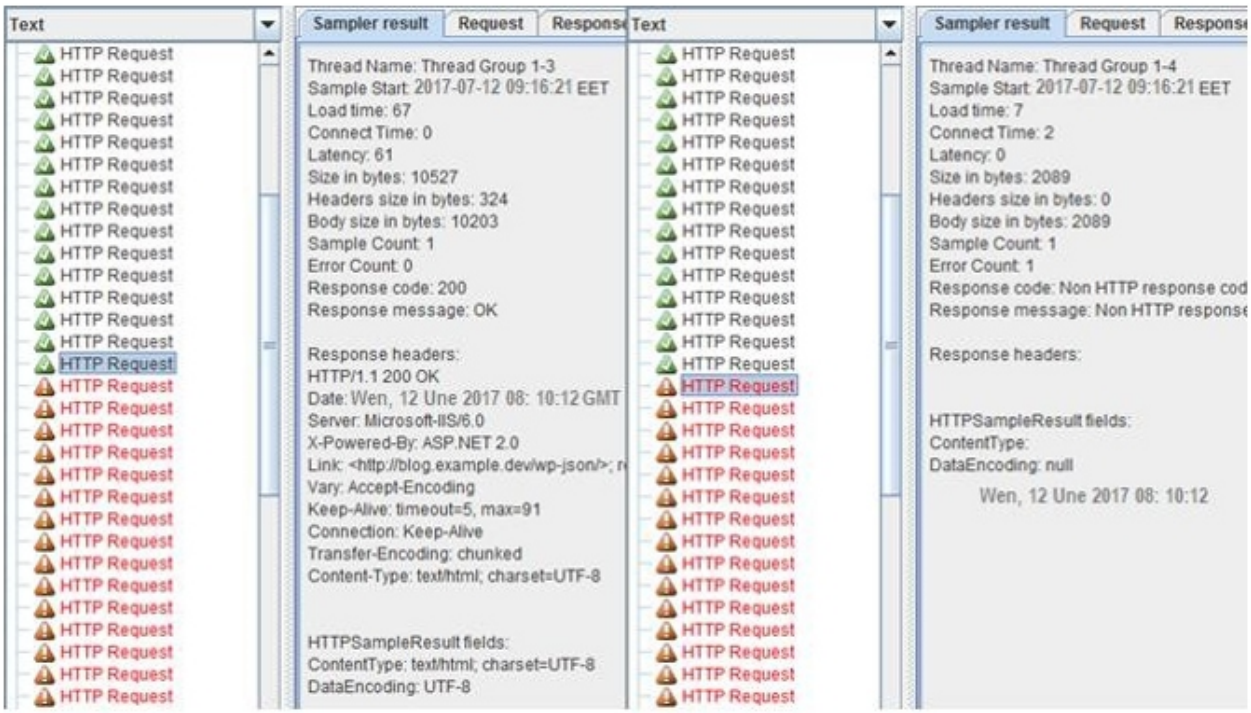


Fig. 3. DoS attack protection

5. HTTP fingerprinting protection with a rule:

SecServerSignature "Microsoft-IIS/6.0"

SecRule &REQUEST_HEADERS:Host "@eq 0" "id:1001,phase:1,deny"

SecRule &REQUEST_HEADERS:Accept "@eq 0" "id:1002,phase:1,deny"

SecRule REQUEST_METHOD !^(get|head|post)$ "id:1003,phase:1,t:lowerCase,deny"

SecRule REQUEST_PROTOCOL !^http/1\.(0|1)$ "id:1004,phase:1,t:lowercase,deny"

Header set X-Powered-By "ASP.NET 2.0"

Header unset Etag

The practical results of applying HTTP fingerprinting protection rules are presented in Figure 4.

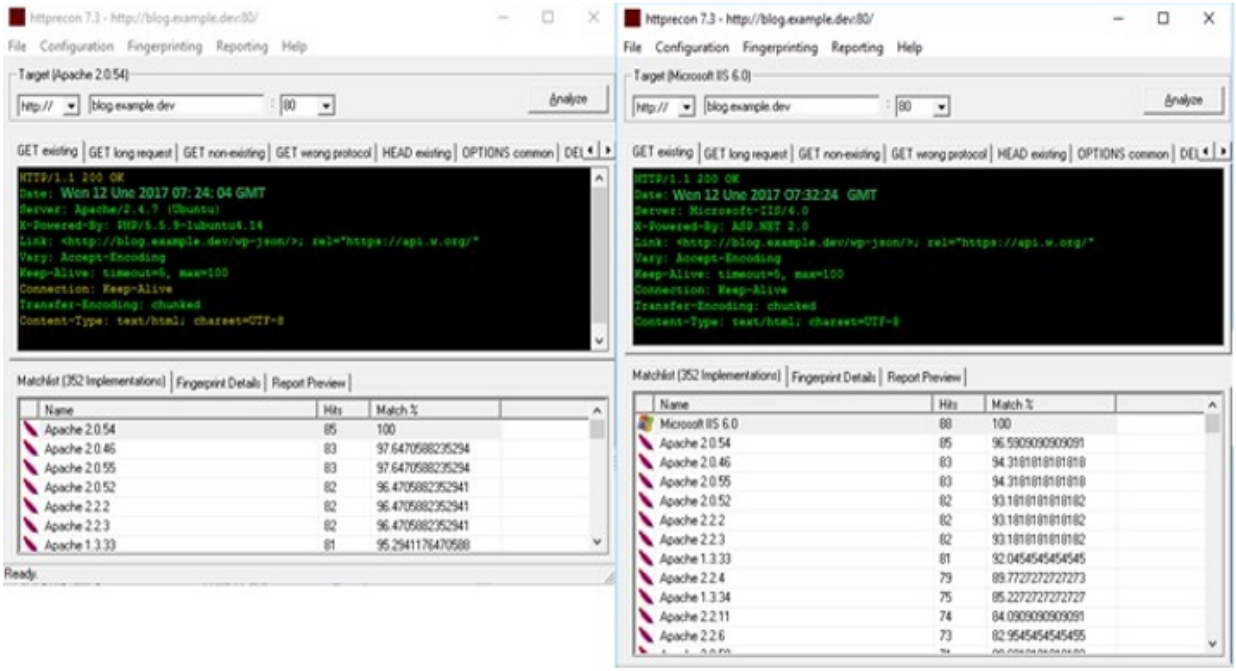


Fig. 4. HTTP fingerprinting protection

5. CONCLUSION

The paper proposes the use of open source security rules provided by the OWASP Foundation based on the ModSecurity module. Advantages of this system include: easy installation, compatibility with the most common web servers - Apache, Nginx and Microsoft IIS and numerous user-friendly rules. Based on the ModSecurity module, real, complex real-time web server protection rules are presented against breakthrough techniques and commonly used vulnerabilities in OS Linux. Practical results show that the selected security module provides Successful and secure server protection by neutralizing high- and medium-level threat attacks such as HTTP fingerprinting, Shell command, DoSattack, SQL injection and Brute Force.

REFERENCES

1. *Lochart, A., (2005), Network Security Hacks,O'Reilly,https://books.google.bg/books?id= 5AiAVtIAKsC& printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false*
2. *Scambray, J., Kurtz, G., (2012), Hacking Exposed 7, Network Security Secrets and Solutions by Mcclure, Mc Graw Hill*
3. *McClure, St., Scambray, J., Kurtz, G., (2011), Hacking Exposed, Network Security Secrets and Solutions, Sixth Edition 6th Edition, Mc Graw Hill*
4. *Barnett, R., Grossman, J., (2001), Web Application Defender's Cookbook, Battling Hackers and Protecting Users*
5. *Magnus, M., (2009), ModSecurity 2.5, Rasct*
6. *Ristic, I., (2012), ModSecurity Handbook, Feisty Duck*
7. *Dudin, E., (2017), Web server protection by ModSecurity rules, (in Bulgarian)*
8. *Folini, Ch., Ristic, I., Modsecurity handbook, Fiesty Dusc, 2017*
9. *Mod Security 2.9, https://www.modsecurity.org/, 2017*
10. *Httprint, http://www.net-square.com/httprint.html, 2016*
11. *https://www.owasp.org/, 2001-2017*
12. *https://malware.expert/signatures/, 2017*

Improved Framework For DDOS Attack Prevention In Clustered Environment

Rshma Chawla, Gurpreet Kaur
Assistant Professor, MMICT & BM, MMU, Mullana (Ambala)
Assistant Professor, MMICT & BM, MMU, Mullana (Ambala)

ABSTRACT

Distributed Denial of Service (DDoS) attack is large scale coordinated attack on the availability of services of a victim system or network resources. We proposed the problem of existing paper is high speed traffic measuring in DDoS attack. This problem is solved by transparency protocol. In existing paper it is just mentioned that it is measured through clustering, but we proposed that when it is divided into clustered traffic it is sent to transparent protocol. Transparent protocol works on the originality of data. In this source & destination address could be used as unique labels for the end system.

Keyword: DDoS, Transparent protocol, clustering, flooding.

1. INTRODUCTION

Denial of service attack programs have been around for many years with growth of internet they have increased. A DDoS streams do not have common characteristics as the currently available intrusion detection system (IDS). The aim of DDoS attacks is to make internet based services unavaible to its legitimate users. DDoS attacks is challenging for two reasons. First, the number of attacks involved in DDoS attacks is very large. If the volume of traffic sent by single attacker is small then the victim host is overwhelming. Second, attacker usually spoofs IP address, which is difficult to trace. Three types of flooding attacks are accessed in it TCP/SYN, UDP & ICMP. TCP SYN flood is a most dangerous of the DDoS attack .UDP flood attacks is to exploit the UDP services. UDP packets to different port of a target in random way. ICMP is a smurf attack which is used to put the target resources out of service that results in making the resource stagnate. DDoS attacks network follows two types of architecture. The agent handler architecture and internal relay chat. The agent–handler architecture for DDoS attack is comprised of clients, handler and agents. The attacker communicates with DDoS client system. The handlers are often software packages located through the internet that are used by client to communicate with the agent. The agent software is placed in the compromised system that finally

carries out the attack. IRC communication channel is used to connect the client to agent. IRC ports can be used for sending commands to the agents. IRC channel as such channels tend to have large volume of traffic. DDoS defense mechanism approaches are three types of deployment source end, victim end and intermediate end.

2. RELATED WORK

A.Saidi [1] describes the conception of a multi-agent based intrusion prevention system that can apprehend these flooding attempts in distributed way. Three types of flooding DDoS attack SYN; UDP & ICMP are explained in it. The main features of DIDS are communication between its components and a fast analysis to assure a global view of the whole network and an efficient analyzer locally by distributing IDS tasks.

K Govinda [4] proposes a secure data transfer over cluster environment ensures composition of different traffic to handle DDoS attacks in cluster environment. This issue generally is in need of processing huge amount of data. The cloud computing is an extremely success full paradigm of service oriented and has revolutionized by the way computing infrastructure is abstracted and used.

Shahaboddin shamshiraband [2] proposes an IDS calling fuzzy and learning algorithm to protect wireless nodes within network and target nodes from DDoS attack to identify the attack patterned and take appropriate countermeasures .The FQL algorithm was trained and tested to establish its performance by generating attacks from the NSL-KDD. This paper discussed how DDoS attacks are launched in wireless network can be modeled through fuzzy Q-learning algorithm. The purposes of developing such models are included to evaluate whether resources of given system are vulnerable to certain types of attacks. The WSN model is represented in it. The aim of the proposed FQL is to obtain high detection accuracy with a low false alarm rate.

Saman taghavi zarger [6] presents that DDoS flooding attacks are one of the biggest concern of security. In this paper, it describes the DDoS flooding attack problem and attempts to combat it. They categorize the DDoS flooding attack & classify existing countermeasures based on where and when they prevent, detect and respond to flooding attack. An ideal comprehensive DDoS defense mechanism must take specific features to combat DDoS flooding attack both in real time and as close as possible to the attack sources some features are included in it.

Yuri demchenko [12] explains how the proposed model and SDLM SDI can be naturally implemented using modern cloud based infrastructures. The paper refers to different scientific communities to define requirement on data management access control and security. It analyzes the new challenges imposed in modern Q-science infrastructures by the emerging big data technologies. The main goal of the scientific infrastructure is to support the enterprise and operational procedure related to process monitoring and data processing. Cloud technology simplifies building of such infrastructure and provisions it on demand.

Guang Yao [3] proposes a lightweight and efficient framework for router based IP –spoofing filtering named SEFA. IP spoofing is well known security threat on the internet though there have been number of spoofing prevention mechanism due to the diversity of network. If taking into account the evolution of network. Even for a single network there is not always a solution applicable in practice. Operators may want to choose the solution exactly suitable for the network and demand a novel architecture to support spoofing filtering named SEFA (software defined filtering architecture). In route based IP spoofing filtering, SEFA should keep the router mostly unchanged. Operators do not want to offload all the functioning on router to SEFA. It should provide the minimal function set. They do not want to manage a full stack SDN controller.

Herodotus Herodotou [11] introduced starfish a self tuning system for big data analysis. Starfish builds on Hadoop well adapting to user needs and system workload to provide good performance automatically, without any need for users to understand and manipulate the many tuning krobs in Hadoop. Well Starfish is system architecture is guided by work on self tuning database system. Hadoop is a MAD system that is becoming popular for big data analytics. An entire eco system of tools is being developed around Hadoop. A combination of factors contributes to Hadoop's Madness. First, copying files into the distributed file system is all it takes to get data into Hadoop. Then the Map reduce methodology is to interpret data at processing time not loading time. A system like Starfish is essential as Hadoop users continues to grow beyond companies like Face book, Yahoo etc. Hadoop now is a viable competitor to existing systems for Big data analytics.

Dilip Kumar G [7] surveys of DDoS detection methods are published .it highlights the open issues research challenges and possible solutions. The purpose of this paper is usually to put some order into existing defense methods to ensure that a greater perception of DDoS attack methods maybe accomplished and subsequent better efficient and effective algorithm techniques and procedures to combat these attacks could also be developed. The defense mechanisms like statistical, knowledge, soft computing are deeply explained in it. Defense architectures are divided into three classes: Source End, Victim End & Intermediate defense mechanisms are described in this paper.

T.Poonachandar [9] proposed DOS based adaptive & selective verification mechanisms are effective and efficient compared with the existing methods. Cloud clients can adapt efficiently to an attack by growing the request rate based on timeout windows to calculate attack rates. They conclude ASV advances the state of the art in bandwidth based DOS defense mechanisms by introducing cloud computing technology by using distributed adaptive solutions based on selective verification. It is shown that the effect of ASV on internet cross traffic is minimal and comparable to that of its native non-adaptive counterpart which represents no defense attack scenarios.

Manisha Sharma [13] describes cloud computing has generated a lot of interest and competition in the industry. It is an internet based service delivery model which provides internet based services, computing and storage for users in all market including financial, health care etc. In this paper we did systematic review on different types of clouds and security challenges that should be solved. Cloud security is becoming a key differentiator and competitive edge between cloud providers. This paper discusses the security issues arising in different types of clouds.

Monowar H.Bhuyan [10] presented an overview of DDoS attacks, detection schemes, research issues and challenges .The comparison of the existing detection mechanisms shows that most schemes are not capable of fulfilling all the requirements for real time network defense. Different performance parameters meet be balanced against each other dedicatedly and appropriately performance evaluation using DDoS tools data sets are fully elaborated in it. DDoS attack detection methods which are based on the architecture victim end & source end in network are discussed. The classify methods into major classes are also presented different strategies to evaluate performance of DDoS attack detection methods are described.

Abdullah H.alqahtani [8] concludes the design flaws of TCP/IP suite of protocol have been responsible for most of the attacks on the internet. It always requires security to be applied as an external layer to the TCP/IP suite and this approach causes various problems itself. It presents various attacks directed as TCP/IP and focused on the tools and defense mechanisms to identify the vulnerability that causes these attacks and ways to plug them. Networks sniffers and network analyzers are tools software/hardware used to sniff data flow through a connection .They work in passive mode and only tap into the connection to listen into the packet exchanged without alerting or redirecting some malicious packets. Wire shark, TCP/dump, Kismet, Ettercap are explained in it. IP spoofing & connection hijacking are described in it. IP spoofing involves maliciously creating TCP /IP packets using other IP addresses as source address with the aim to either conceal own identity. Routers use the IP address of destination and forward the packets to it.

3. PROPOSED FRAMEWORK

This section proposes high speed traffic analysis for measuring in DDOS attack. The aim is to detect the DDOS attack at network site. It uses three basic components of IDS controller, analyzer, and response module.

Packets: It can be placed on a segment of a network. Any data like graphics, videos, audios etc that is shared over the network is sent in the form of segments is called packets.

Clustering traffic: According to nature of data stored in packets, these packets are categorized in different types of traffic that is busty traffic(BT),iterative traffic(IT),latency sensitive traffic(lST) and non real-time traffic(NRT).Very large files with huge transfer time is in busty traffic that consumes higher bandwidth and resources. Data that is essential and requires secure transfer is known as iterative traffic, e.g online banking transaction and real time chat messages. These files are smaller in size but require highly secured transfer protocols. Latency sensitive traffic attracts more flooding attacks due to its nature of high bandwidth consumption. Non real time traffic like emails that can be sent with delay categorized in non real time traffic.

Transparent protocol: The entire packet goes to transparent protocol that will check the flow of data. Transparency means originality. It cannot allow slowing down of the processing of normal packets. It could flow essentially unaltered throughout the network and their sources and destination addresses could be used as unique labels for the end system. It is the ability of a network to transport application information while altering or manipulating.e.g.Ipv6 packets cannot transport a payload of a maximum allowable size depending on the maximum transmission unit (MTU) of the relaying telecommunication infrastructure. If the application data generated is bigger than maximum transmission unit (MTU), it is fragmented at the sender side by the network layer process and transmitted in more IP packets delivered completely independently.

Event monitor: It is responsible of counter measure to an intrusion. The event monitor is responsible for all events. Event monitor detects such types or an event like message, alarm, and traffic regulations etc. If events have passive reaction, the system is called intrusion detection system. It audit the intrusion and others extrusion forwards to risk assessment. It warns to all extrusion data and tells about intrusion. It also tells that do not do any significant work because you are in risk. The Risk assessment sends the notifications to all extrusions through e mail or message queue. The audit data sends to server execution agents. The server execution agents have free senseless resource allocation. Other extrusions are in risk assessment that is defined by enabled IDS policies.

Using social networking media new attacks are generating day by day which are no one know about that so it difficult to attempt this framework. Another disadvantage is that it is time consuming. It takes lots of time to transfer the data.

Fig1 shows the said architecture

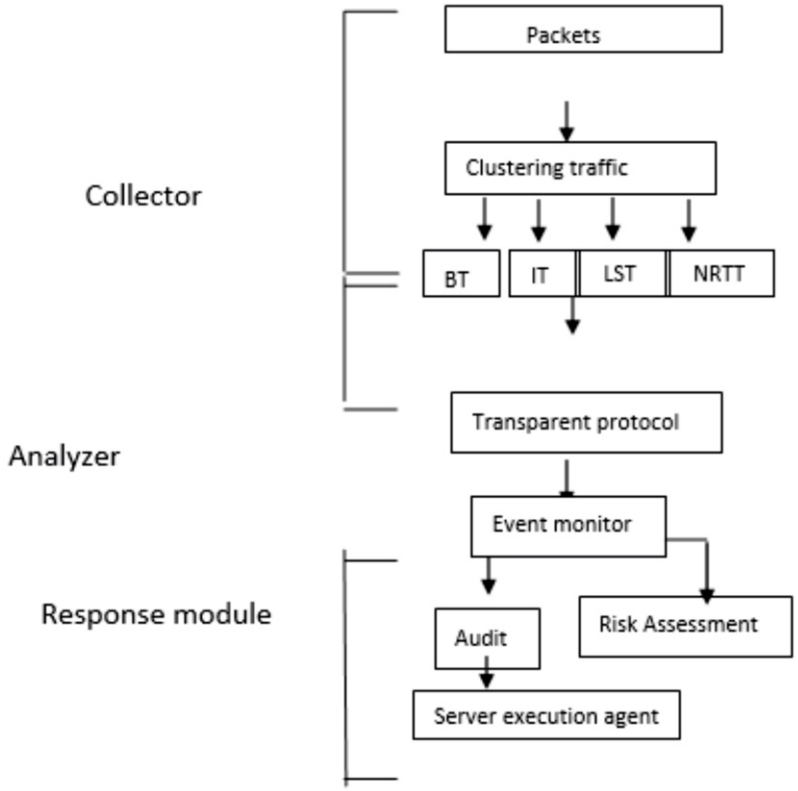


Fig1. Proposed framework of high speed traffic analysis of DDoS Attack

The proposed framework consists of three major modules that are collector, analyzer & response. The collector module is receiving node that collects incoming packets and then these packets are further classified based on the cluster traffic types that are busty traffic (BT), IT (), LST (), & NRTT (). Then these categorized packets are sent to Transparent Protocol in analyzer module in which data in these packets is treated on the basis of category, packets that contains bulk of data are treated with flow control protocols that ensures that packet is given high bandwidth to be transferred over the network. Packets that contain very essential data are treated with highest security protocols. Transparent protocol makes certain that every packet that passes through is clean and contains no malicious data. If any packet seems to be containing any harmful data or is not one of the selected categories, it stops the transfer of that packet and diverts it to event monitor. Event monitor further explores the content of packet received and send it for audit and risk assessment. If no policy against the packet is defined already, server execution agent creates a new security policy for the kind of packet received.

4. OPEN ISSUES AND CHALLENGES

The challenges impact the effectiveness of product and feasibility of their wide adoption.

1) During the rise of mobile device use, cloud computing is used &shared everything in social networking are being used.

2) The high volume & variety of data make it difficult to determine what is important, what should be collected, where it should be stored .some possible data sources include proxy logs, email Meta data, firewall logs, Ids logs, IPS logs.

3) The most notable assumption is that attack behavior is some, how different from normal traffic but attackers might hide their activities in normal traffic.

4) The high diversity of traffic on today's networks increases the challenge. There is an increasing amount of variability in network traffic that operators need to manage.

5) It is becoming more difficult to understand normal traffic and detect the important signal in the noise.

6) Lack of defense system benchmark. Researchers cannot compare actual performance of their solutions to exiting defenses.

7) Difficulty to large scale testing .This is currently impossible due to the large scale test beds, detailed and realistic tools that can support several thousand nodes.

8) Cross layer protocol which used in layers of network, it knows all the information about entire layers simultaneously.

5. REFERENCES

*1+ A. Saidi, A.Kartik, " A Multi-agent based Distributed Intrusion Prevention system against DDoS flooding attacks," Journal of Theoretical and Applied Information Technology, ISSN:1992-8645, Vol 59, No. 2, 20th Jan, 2014.

[2] Shahaboddin Shamshiraband, Nor Badrul Anwar, "Anomaly detection using Fuzzy Q-learning Algorithm," Acta Polytechnica Hungarica, Vol.11, No. 8, 2014.

[3] Guang Yao, Jun Bi, "Performing Software defined Route Based IP Spoofing Filtering with SEFA", 978- 1-4799-3572-7/14©2014, IEEE.

[4] K. Govindra, E-Sathtyamoorthy, "Secure traffic management in Cluster environment to handle DDoS attack," World Application Sciences Journal 32(9): 1828-1834, 2014.

*5+ lovepreet kaur, abhinav bhandari,"DDoS attacks and various detection mechanisms", international journal for technology research I engineering vol 1, issue 9, May 2014.

*6+ Saman Tagghavi Zarger, James Joshi and David Tipper, "A survey of Defense Mechanisms against distributed Denial of service (DDoS) flooding attacks, IEEE Communications Surveys and Tutorials, 15(4): 2046-2069, 2013.

*7+ Dileep Kumar G, Dr C V Guru Rao,"A survey on defense mechaniary counting DDoS attack in the networking."International Journal of Advanced Research in Computer and Communication Engineering Vol 2, issue 07 July, 2013.

*8+ Abdullah H. Algahtani, "TCP/IP attack, Defenses and Security Tools," International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Volume-1 issue 10 Sep, 2013.

*9+ T.Poonachandar, D.jaya prakash,"Denial of service (dos) attacks detection in cloud computing "Indian journal of research, volume: 2, issue 11, Nov 2013.

[10] Monowar H. Bhuyan, H.J.Kashyap, "Detecting Distributed Denial of service attacks methods, tools and future directions." Springs, (080933-7150, U.S.A. December 2012.

*11+ Herodotus Herodotou, Harold Lim, "Starfish: A self-tuning system for Big Data Analysis."5th Biennial conference on innovative Data systems research (CIDR'II).Asilonar, California, U.S.A January 09-12-2011.

[12] Yuri G. Dantas, Vivek Nogam, "A selective Defense for Application Layer DDoS attacks," Federal University of Paraiba, Joao Pessoa, Brazil,2011

*13+ Tripathi, Manisha Sharma, A mishra,"cloud computing security consideration "signal processing communication and computing (IPSCC), IEEE international conference 2011.

Data Mining And Privacy Issues

Dr. Jatinder Kumar
Assistant Prof., A.S. College, Khanna

ABSTRACT

The era of IT and IT enabled services has brought a revolution in the present day life which revolves around the data, its use and the interpretation as per the need of the users. Apart from focusing on issues related to efficient and secure data storage, effective and secure data retrieval is the key area now a days. Privacy is the buzzword these days in all the companies handling and providing data to one and all. The customers have now noticed that it is their right to determine which personal information about him or the organization is to be made available to others. The customers want to be secure from unauthorized disclosure of information about oneself or the organization. This paper is emphasizing on hammering on the question that ***Can data privacy and data mining coexist?*** *The aim is to explore how exactly data mining can be a threat to privacy, and what type of legislative and technical steps should be taken to make sure that data mining and data privacy go together a long way.*

Keywords: Data Security, Data Privacy, Authentication, Cryptography.

1. INTRODUCTION

One's life consists of a variety of data. Without any technical devices, we may get much information or data from others. For example, how they look, what language they speak, and what they eat. Although what we could get from others is a continuous stream data format, those data, roughly collected, can tell us many things about them, for instance, their age, race, nationality, food tastes, etc. Today we consciously or unconsciously diffuse our data somewhere. Whenever we shop, use credit card, rent a movie, withdraw money from ATM, write a check and log on the Internet, our data go somewhere. Virtually, every aspect of our life discloses information about us. With the development of computing and communication technology, now data can be captured, recorded, exchanged, and manipulated easier than before. Recently, issues about information privacy have emerged with the dramatic growth of data storage, computer processing power, and networks. Especially, data mining becomes a hot issues related to data privacy of individuals in the context of the Internet, e-commerce, direct marketing, and interactive advertising raises potential problems of data mining. “Data mining represents a major challenge to privacy because the companies who practice data mining cannot predict what uses the resulting information will have,”

What is Data Mining?

It is basically the definition of policies stating which information is collected, how it is used and how customers are informed and involved in this process.

Data mining technology has been developed with the goal of providing tools for automatically & intelligently transforming large amount of data in knowledge relevant to users.

It's the science of extracting useful information from large data sets of databases.

Data mining is the process of analyzing data from different perspectives and summarizing it into useful information - information that can be used to increase revenue, to cut costs, or both.

Data mining is the process of finding correlations or patterns among dozens of fields in large relational databases.

Data mining is a set of automated techniques used to extract or previously unknown pieces of information from large databases. Data mining is not a business solution but simply the underlying technology. In technical terms, data mining is described as the application of artificial intelligence (AI) and other intelligent techniques such as neural networks, fuzzy logic, genetic algorithms, decision trees, nearest neighbor method, rule induction, and data visualization, to large quantities of data to discover hidden trends, patterns, and relationships.

Although data mining is a relatively new term, the technology is not. Figure I shows the process of data mining.

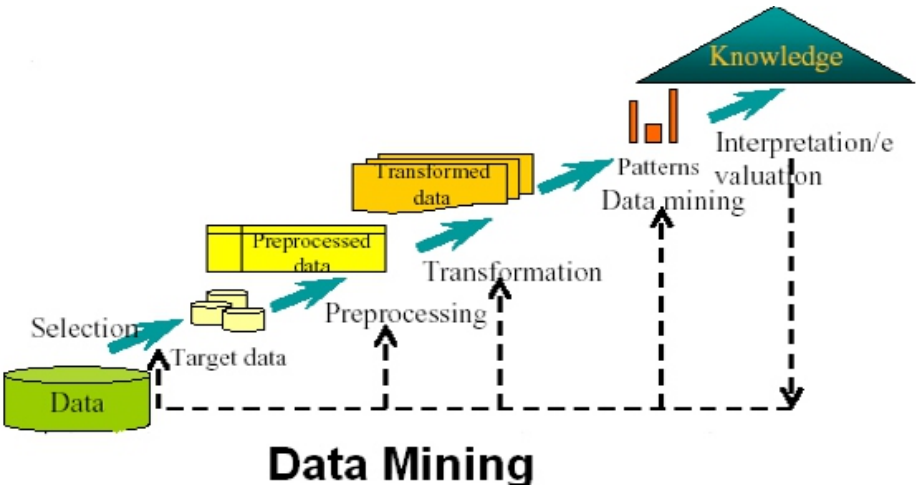


Figure I: Process of Data Mining

Applications of Data Mining

With data mining, a retailer could use point-of-sale records of customer purchases to send targeted promotions based on an individual's purchase history. By mining demographic data from comment or warranty cards, the retailer could develop products and promotions to appeal to specific customer segments WalMart is pioneering massive data mining to transform its supplier relationships. WalMart captures point-of-sale transactions from over 2,900 stores in 6 countries and continuously transmits this data to its massive 7.5 terabyte data warehouse. WalMart allows more than 3,500 suppliers, to access data on their products and perform data analysis. stored data is used to locate data in predetermined groups. For example, a restaurant chain could mine customer purchase data to determine when customers visit and what they typically order. This information could be used to increase traffic by having daily specials.

Likewise, data mining now is considered as basis for new products and for enhancing existing offerings, and sometimes as a tool for R&D and solution to business problems.

Taking another example, not only as a marketing tool, large data mining companies such as HNC Software and IBM, have used data mining techniques to detect credit card fraud and to evaluate real estate.

Data mining is primarily used today by companies with a strong consumer focus - retail, financial, communication, and marketing organizations. It enables these companies to determine relationships among "internal" factors such as price, product positioning, or staff skills, and "external" factors such as economic indicators, competition, and customer demographics.

Data mining is usually used for four main purposes:

(1) To improve customer acquisition and retention;

(2) To reduce fraud;

(3) To identify internal inefficiencies and then revamp operations, and

(4) To map the unexplored terrain of the Internet.

Data Mining and Privacy:

Privacy is a loaded issue. In recent years privacy concerns have taken on a more significant role in our society as merchants, insurance companies, and government agencies amass warehouses containing

personal data. The concerns that people have over the collection of this data will naturally extend to any analytic capabilities applied to the data. Users of data mining should start thinking about how their use of this technology will be impacted by legal issues related to privacy. Data mining is the driving force for lots of businesses. However, these days, privacy concerns of data collection and manipulation are getting bigger than ever before.

The process of mining the data can also return sensitive information about individuals and organizations, posing a threat to the individual's right to privacy. It can also reveal critical information about business transactions, causing a free competition in a business setting. Therefore a strong need is being felt to prevent disclosure not only of confidential personal information but also knowledge which is considered sensitive in a given context. It leads to the need of various privacy preserving algorithms. **The aim of these algorithms is the extraction of relevant information or knowledge from large amount of data while protecting at the same time the sensitive information.** These algorithms allow one to hide sensitive item sets or patterns before the data mining process is executed.

Privacy of data while extracting information from the data bases is of paramount importance. Privacy involves a definition of policies among which information is collected, how its used & how customers are informed & involved in this process. It is the right of a person to determine which personal information about him or organization may be communicated to others. Privacy is the right of an individual to be secure from unauthorized disclosure of information about one self that is contained in an electronic repository.

The information which can be mined from a database by using various data mining algorithms also poses a threat to the privacy of the individual. The thrust area now is to data and private knowledge remain private even after the mining process.

As various Privacy Preserving Data Mining Algorithms (PPDM) are available, the crucial issue is to determine which one among these techniques is better to protect sensitive information and is to find out a set of criteria's with respect to which these algorithms can be evaluated and ultimately we may lead to the standardization in this area. However, apart from protection of sensitive information, it is also very important to assess the quality of data resulting from the modifications applied by each algorithm as well as the performance of each algorithm. The need is to find out a comprehensive set of criteria's (or a framework) for estimating & comparing Privacy Preserving Data Mining Algorithms and ultimately to find out whether the algorithm meets the specific requirements. Some of the techniques/ Dimensions which are considered are:-

1. Efficiency-: Ability of privacy preserving algorithm to execute with good performance in terms of all resources implied by algorithm. Performance is accessed in terms of time & space and in case of distribution algorithm, in terms of communication costs incurred during information exchange.

2. Scalability: - It is described as the efficiency trends for increasing values in data sizes. It concerns with increase of both performance & storage requirements together with the cost of communication required by distributed technology. The less rapid is the decrease in efficiency of Privacy Preserving Data Mining algorithms for increased data dimensions, better is its scalability.

3. Data Quality: - Quality of data after application of a privacy preserving technique is again a major area of concern. Because if the quality of data transmitted or shared is not good then it will be of no use. Quality of data is being checked by comparing it before and after the application of Privacy Preserving Data Mining Algorithms. It is quite a relative criterion which varies from context to context. The major parameters which are considered most relevant are: accuracy, completeness and consistency. The accuracy is closely related to the information loss resulting from the hiding strategy.

4. Hiding failure: - It is the portion of sensitive information that is not hidden by the application of a privacy preserving technique. Target of Privacy Preserving Data Mining algorithm is to achieve a zero hiding failure.

5. Privacy level: It estimates the degree of uncertainty according to which sensitive information that has been hidden can still be predicted. We need to define a unique parameter quantifying privacy level ensured by these algorithms.

Data Mining and the customer issues:

In order to determine whether personal data currently available to data mining should be restricted, however, two points should be considered; one is fairness and the other is openness in consent. First, because data subjects are often "not informed" during the data collection or data mining, sometimes it is impossible for them to set up a new normatively private situation regarding the data. Secondly, because the personal data that data subjects may have willingly granted for use in one context is often subsequently mined for another context different from the original situation. This brings about issues related to unauthorized consent.

Around the world, virtually all privacy legislation, policies or guidelines have been derived from the set of principles established in 1980 by the Organization for Economic Co-operation and Development (OECD) (Cavoukian, 1988). These principles are often called **"fair information practices,"** and cover eight specific areas of data protection.

They are:

1) Collection Limitation;
2) Data Quality;
3) Purpose Specification;
4) Use Limitation;
5) Security Safeguards;
6) Openness;
7) Individual Participation; and,
8) Accountability.

While many European countries have already adopted their own data privacy policy, we are left behind in policy making for privacy issues. Government should pass laws on how personal information is collected "What's going on today is exponentially more threatening to those who want to protect privacy," People can't make informed decisions on the Net because they do not have enough information. With government's regime, IBM, along with many other industry leaders, has adopted its own guidelines, called "Code of Conduct (1997)" for handling personal data and claims that most other substantial organizations that collect, use, or process data, understands the stake they have in consumer confidence. Some other trade associations also have privacy principles and guidelines which govern how their members do business.

In short, self-regulation is a sham. The policies that companies have posted under the pressure from the government are as vague and confusing as anything … Most sites don't limit how they or their partners use consumer information. And Web sites can transfer information to partners without telling their own customers. Many sites also change their practices at will and without warning. **The work is rather going on to tighten such measures to ensure the right use of the customer data. Indian Government has taken many serious steps to design and implement cyber laws to protect the data from unauthorised access.** The Department of Information Technology has been directed to hasten the process of amending the Indian IT Act to ensure that any breach of secrecy and any illegal transfer of commercial or privileged information is made a punishable offense.

On the technically side, What is needed? … is a machine-to-machine protocol for negotiating privacy protection. The user sets the preferences once – specifies how they would negotiate privacy and what she is willing to give up – and from that moment on, when she enters a site, the site and her machine negotiate. Only if the machines can agree the site will be able to obtain her personal data.

CONCLUSION:

The need of the hour is that privacy policy should be open and fair, but there exists various privacy-related conflicts between different groups, **i.e., consumers vs. businesses, data subjects vs. data miner**, etc. These conflicts should be negotiated in the open and fair environments and the efficient privacy preserving algorithms should be made available. For this, this paper presents that users/data subjects should have "informed choices" for collection, mining and exchange of data about themselves. Despite the rapid growth of privacy concerns, there are no current laws and business guidelines to sufficiently protect privacy violation in data mining. The need is to design and operate such an environment and platform which can have all these three areas of legislative, economic, and technological aspects under one roof. Though all of these approaches are contributable to expand user's informed choices for their privacy, each approach is not mutually exclusive but interleaved. A narrow approach to push only one-sided solution might intensify the tension between data privacy and data mining. So we believe that the tension can be minimized if and only if privacy policy is built on multiple approaches because data mining seems a survival strategy for companies in these days and to survive the organizations have to use data mining in an authenticated way.

References:

Vassilios S. Verykios1, Elisa Bertino2, Igor Nai Fovino2, "State-of-the-art in Privacy Preserving Data Mining" Elisa Bertino Igor Nai Fovino Loredana Parasiliti Provenza "A Framework for Evaluating Privacy Preserving Data Mining Algorithms"

"Data Mining" Next Generation Challenges and Future Directions, Hillol Kargupta, Anupam Joshi, Krishnamoorthy Siva Kumar, Yelena Yesha.

Agarwal.R and Srikant ,R.2000,Privacy preserving Data Mining. In Proceedings of the ACM SIGMOND International Conference on Management of Data.

H. R. Nemati and C. D. Barko(2003)"Key Factors for Achieving Organizational Data Mining Success". Industrial Management and Data Systems, vol. 103, no. 4, pp. 282–292.

Hillol Kargupta, Anupam Joshi, Krishnamoorthy Siva Kumar and Yelena Yesha, Data Mining: Next Generation Challenges and Future Directions,Publishers: Prentice-Hall of India, Private Limited, 2005.

Evaluating Security Awareness Impact On Perceived Risk And Trust: The Case Of Social Networks

Zakaria I. Saleh, Ahmad Mashhour
American Intercontinental University
University of Bahrain

ABSTRACT

The social media networks offer individuals and communities opportunities to communicate with broad global reach. This paper studies the social media users' awareness of the security and the personal privacy issues, and investigates perceived risk and trust on information disclosure behavior in Social Network sites (SNSs). In addition, to further extend the benefits of this study, we have collected and analyzed data to evaluate the participants' perceived benefits and drawbacks of the social media networks, where mixed results were found. This is due to the unique characteristics of social media: openness, participation, and sharing. However, despite rapid adoption, we find that a growing concern and skepticism regarding the use of social media exists among the social network users. There is nothing in paper about benefits and draw backs.

Key words: Privacy, Risks, Social Network Sites (SNS), Security, Trust

INTRODUCTION

Social networks are an inherent part of today's Internet and used by more than a billion people worldwide [www.facebook.com]. A growing number of SNS users over time indicate that people are gaining many benefits from using SNS services. Apart of the advantages that can be obtained by the SNS, users sharing personal information, SNS may become potentially vulnerable to privacy violation as it does not tenet the use of one's information (e.g. name, picture, etc.) by others It also paves a ground for new attack by malware authors where they can spread malicious code by taking advantage of the users' inherent trust in their relationship network.

Social network such as Facebook, Twitter, etc. have become an unprecedented phenomenon which has fundamentally changing the way people communicate, collaborate, and increasingly, they play a significant role in how they interact, but they're also have high risk. The Facebook statistics at the end of March 2016 show that there are, over 1.65 billion monthly active Facebook users which is a 15 percent increase year over year accessed the site (www.facebook.com). With hundreds of millions of users,

these tools have attracted attackers more than any other target in recent years. Social media are getting attractive and are increasingly used by individuals worldwide. However, since their emergence, the social networks are considerably changing the relationships of individuals to society. In addition, of being involved in conversations and interactions with each other, the individuals are getting involved in more sophisticated usages (publishing, sharing, playing, networking, buying, etc.) And while there are various articles, books, and training program to help individuals become fully aware of the benefits and consequences, there still many users who are not aware of the existence of such resources. In addition, most of the research on social networks security has so far dealt with the information assurance aspects, which is primarily about protecting the data using techniques such as authentication and encryption, where information assurance assumes that the devices responsible for encrypting, forwarding and sending are trustworthy. However, they're high risk associated with accessing the social media websites. With hundreds of millions of users, the social networks have attracted attackers more than any other target in recent years. This research is trying to determine whether or not the social network users are aware of the risk associated with accessing the websites as well as find out if awareness of the risk associated with using social network would impact users' trust.

LITERATURE REVIEW

Web 2.0 covers a wide range of technologies. The most widely used are blogs, wikis, social networks, podcasts, and information tagging. The Web 2.0 introduces the idea of a Web as a platform. Web 2.0 applications changed the way we interact with the online world and the other users we connect with through it. Web 2.0 applications have made the Internet more interactive. The shift to Web 2.0 however, was not necessarily the result of a substantive change in technology, but rather in ideology (Kaplan & Haenlein, 2010). Social Networking Websites are defined in terms of its core functions as an online platform that enables individuals to create a public or semi-public profile, articulate a list of other users with whom they share a connection (so-called "friend list"), and browse their list of connections and those made by others (Boyd and Ellison, 2007). And the social media are Web 2.0 internet-based applications, and the user-generated content of the social media network (Obar and Wildman, 2015; Kaplan and Haenlein 2010). However, this research considers the terms "social media," "social networks," "social networking websites," "social networking sites," and "online communities," as synonyms, and refer to the same kinds of websites. Social networks can be formalized by a generative process in which interactions between actors are generated based on some assumptions, i.e., a model with some parameters (Hafez et al. 2015). Social Networking Websites provide tools for users send instant messages, find friends, join online groups, photo sharing, video sharing, social bookmarking, social gaming, and virtual world (Schejter and Tirosh, 2015). Social networks, such as Facebook, were created for the sole purpose of helping individuals communicate and exchange information, photos,

etc.. There are many other reasons that these technologies are used, but communication is still the number one. Many people use these networks to talk to their friends in other cities, states, or even other countries. Social networks are a rapidly growing research area for information system scholars (Oinas-Kukkonen et al. 2010). Over the past few years, almost all of the major social media platforms have seen a significant increase in the proportion of U.S. adults who use them. Some have witnessed more rapid growth than others (Duggan, 2015). A related, important outcome of the scale of social networks is the explosion of user-generated content (Agarwal et al. 2008). When technology mediates social relationships, it creates new interaction dynamics, necessitating novel mechanisms for communicating about oneself and learning about others (Ma and Agarwal, 2007).

Social network websites are easy to access, and in most cases are free of charges. Using social networking site has advantages and disadvantage, and despite all the important contribution of social networking sites, there is a legitimate concern of its scandals. It is the best interest of the user to know which site to use, when and how to use them. In order to use social networking, users must provide personal information first before they are allowed accessing the sites. Users provide an astonishing amount of personal information voluntarily, and Social Network service providers store this information, and this information can be breached by the Service Providers, Other Users, and Third-Party Applications, and thus sharing the information presents risks (Gao et al. 2011). This could lead to a Public disclosure of private information where one person may reveal information which is not of public concern and the release of which would offend a reasonable person. Therefore, privacy concerns on social networks have been proposed to understand how it can influence the relationship between satisfactions sought from social networks and issues caused by social networks (Chen and Kim 2013). In addition, personal identity theft is the main concern. Sharon (2014) indicates that the private companies are using information from users' profiles to find out about them, how they interact with each other, and these private companies can even tell when women are at risk of postpartum depression from monitoring their profile information. Lawyers and policy analysts have begun to examine a wide-ranging array of earlier legal and regulatory frameworks and scenarios with potential applicability to social media (Taylor, 2014; Semitsu, 2011).

RESEARCH OBJECTIVES

The social knowledge sharing would revolve around social relations among people who have an emotional connection and shared characters. The objective of this study is to evaluate the impact of security awareness on users' perceived risk when using the social network sites (SNS).

It will also look into the factors that influence awareness of the risks, specifically the peers' world of mouth and the perceived reputation of the social network site. The primary research question in this study is trying to determine whether or not the social network users are aware of the risks associated with accessing their websites and related perceived privacy concern, and trust on information disclosure behavior in SNS.

RESEARCH QUESTIONS

Q1: Are users aware of the risk related to the social network websites?

Q2: Does awareness of the social network security threats impact users' perceived risk?

Q3: Does peers' world of mouth among users help develop awareness of the risk associated with social network?

Q4: Does awareness of the social network security threats impact users' trust and perceived privacy?

SURVEY DESIGN

The goal of surveying is to find out the perceptions of social network users about social websites security, and to find out whether or not these perceptions have any effect on their perception of the risks related to accessing the social media websites and whether or not it effect their trust. To achieve this goal, and to avoided biased on “none users”, the research used an online hosted survey, and invited social network user to participate in completing the survey. Table 2 summarizes the Instrument's Items.

Table 2 Instrument Items.

1. Social media makes it easier to keep in touch with family and friends who live far away
2. I can make new friends by connecting with friends of friends that I don’t know.
3. There are negative effects of social media
4. Not setting the privacy settings properly can result in invasion of privacy
5. Liking someone's photo can have negative results.
6. I may get jealous if my companion (husband, wife, boyfriend or girlfriend) is interacting with opposite sex.
7. Social networks can ruin companions relationships
8. Sometimes I spend more time on my social media account than I have anticipated.
9. I believe that it can be a waste of time if I stay long on my social media account
10. I could use some of the time spent on my social media account doing useful thing.
11. Using social media enables me to communicate with friends and family more quickly.
12. Using social media is compatible with all aspects of my life.
13. I think that using social media fits well with the way I like to do things.
14. Using social media fits into my life style.

15. My interaction with social media is clear and understandable.
16. I believe I could communicate to others the consequences of using a social media.
17. I hear much about the user-friendliness of my social network website
18. I hear much about the security level of my social network website.
19. I read much information about the risks associated with using social network
20. My friends and family recommend the social network site I use over any other social network.
21. I only access the social media websites that my friends recommend.
22. The consequences of using social media are apparent to me.
23. Social media is widely used.
24. Social media gives me complete control over my account.
25. Social media implement security measures to protect social network users.
26. Social media usually ensure that posted information is protected.
27. My privacy is fully protected when using the social media.
28. Social media cannot be trusted; there are just too many uncertainties.
29. In general, I cannot rely on Social media websites to keep the promises that they make.
30. Social media is risky.
31. Social media entails uncertainty or vulnerability.

HYPOTHESES

The Internet has provided the individuals with a new medium of communicating and transacting with each other and the world at large. This new channel of communication has opened up a world of opportunities to enhance interactions, improve communication, and improve information delivery. While social media has blurred the distance between people, it has also entailed the communication of a significant proportion of sensitive information over unsecured open networks. Information exchanged over open networks is vulnerable to being accessed and viewed by unauthorized users.

H01: Social network users do not have a negative attitude towards the social media.

Word of mouth may influence the conduct of individuals. Peer effects have been found in a wide range of settings. Individuals may be affected by the actions of their peers through a variety of practices including participating in social networks. The fact is, social networks are all about sharing, which could result in a costly learning curve for many users. Unfortunately, some users share too much sensitive information and a few shares too many details related to their personal lives.

H02: Perceived reputation of social media is positively associated with awareness of the risks associated with social network.

Word of mouth is an oral or written recommendation by a satisfied customer to the prospective customers of a good or service. In this context, this research considers it to be an effective form of

spreading information, and allows people to talk about a subject like services provided by a social media website. Word of mouth can be both positive and negative. Nowadays, social media sites can be a place to spread the word of mouth and talk about many issues including issues related to social media website.

H03: Peers word of mouth positively associated with the perceived security threats associated with social network.

Social networking sites allow someone to post information that thousands of other users can read. The web sites allow hundreds of thousands of people to post content: on-line profiles, videos, and/or commentary. The volume of users and the information that gets posted on social media sites create plenty of opportunity for an attacker to use social engineering or other methods to gain access to the accounts of individuals and organizations. The more information a user post, the more his/her security and privacy will be exposed to attacks.

H04: Awareness of the security threats is positively associated with the perceived privacy of the social networking sites.

Many people click on nearly any link that they see posted and may add anyone to their private network that asks for without knowing who really is behind it. Trust has a huge impact on decisions whether to believe or disbelieve information stated by other peers, but the most common threat is the tremendous amount of trust users have in the social applications. For example when an e-mail hits the mainstream, or when instant messaging becomes ubiquitous. In addition, people trust links, pictures, videos and executables when they come from "friends.

This inherent trust, especially in messages coming from peers that have had their account compromised makes it easy for attacks to succeed again.

H05: Awareness of the security threats is positively associated with the trusting social media.

Important considerations were made in the development of a research question and hypothesis and in defining objectives for research. The five hypotheses were suggested in order to provide answers to the research questions. The research questions to hypotheses mapping is illustrated in table 1.

Table 1: Research Questions to Hypotheses mapping

Research Question	Hypothesis Number
Q1	H01
Q2	H02
Q3	H03
Q4	H04, H05

HYPOTHESES TESTING

The First Hypothesis (H01)

Our first hypothesis is that Social network users do not have a negative attitude towards the social media. Testing this hypothesis, the mean attitude score is 4.21 in the scale of 1 to 7 where "1" stands for "extremely disagree" and "7" stands for "extremely agree". The standard deviation of the attitude score is 1.24. The median of the attitude score is 4.00. The distribution is fairly symmetric about the mean (see figure 1). The first and third quartiles are 3.30 and 5.10, respectively. The number of observations is 357 (see Table 3).

Table 3: Statistics of attitude score

Number of Observations	First quartile	Third quartile	Median	Mean	St.Dev.
357	3.3	5.1	4	4.21	1.24

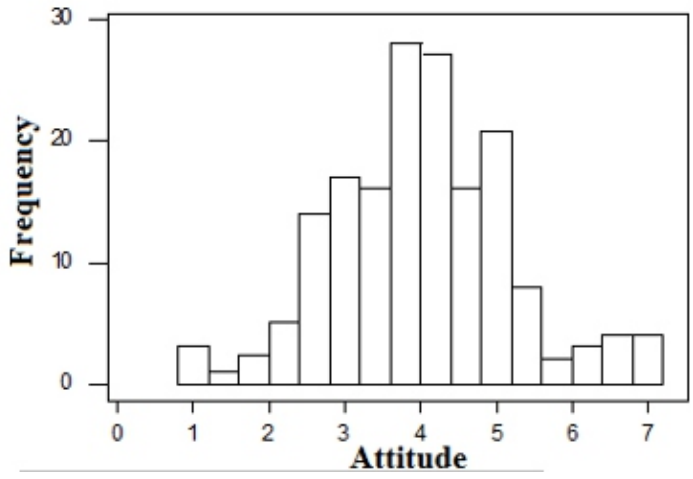


Figure 1. Histogram of Attitude Score

The independent variables were scaled between 1, indicating respondents strongly disagreed, and 7, indicating respondents strongly agreed. A score of 3.5 on this scale indicated a neutral value. Since 3.5

correspond to the neutral point, we formulate the following statistical hypothesis in order to test our first hypothesis:

Null hypothesis: The average attitude score is equal to 3.5.

Alternative hypothesis: The average attitude score is greater than 3.5.

Using a one-way sample t-test, we find an extremely small P-value, less than 0.1% (t-value is 6.74), which means that we can reject the null hypothesis at 0.1%, a very significant level. So, the social network users do not have a negative attitude towards the social media.

The Second Hypothesis (H02)

In our second hypothesis we stated that perceived reputation of social media is positively associated with awareness of the risks associated with social network. Testing this hypothesis, the mean score for perceived reputation is 4.40 and the mean score for risk awareness is 4.86 in the scale of 1 to 7. The standard deviation of the perceived reputation score is 1.05 and the standard deviation of the risk awareness score is 0.87 (see Table 4). In addition, and at 95% confidence interval, we find that the correlation coefficient (R) = 0.437, and the R squared = 0.187. We also tested to see if the slope is significantly different from zero, and found that the P value is <0.0001, which is considered highly significant. Therefore the hypothesis is accepted.

Table 4: Data of the Perceived Reputation and Risk Awareness

	Observation number	First quartile	Third quartile	Median	Mean	St.Dev
Perceived Reputation	357	3.6	5.1	4.5	4.4	1.05
Risk Awareness	357	4.7	5.3	5.2	4.86	0.87

The Third Hypothesis (H03)

In our third hypothesis we stated that peers word of mouth positively associated with the perceived security threats associated with social network. Testing this hypothesis, the mean score for word of mouth is 4.25 and the mean score for perceived security threats is 4.55 in the scale of 1 to 7. The standard deviation of the word of mouth score is 0.95 and the standard deviation of the perceived security threats score is 1.10 (see Table 5). We also tested to see if the slope significantly different from

zero, and found that the P value is 0.039, which is considered statistically significant as $P < 0.05$. Therefore, hypothesis is not rejected.

Table 5: Data of the Word of Mouth and Perceived Security

	Observation number	First quartile	Third quartile	Median	Mean	St.Dev
Word of Mouth	357	3.55	5	4.5	4.25	0.95
Perceived Security	357	4.6	5.4	5.2	4.55	1.1

The Fourth Hypothesis (H04)

Our fourth hypothesis states that awareness of the security threats is positively associated with the perceived privacy of the social networking sites. Testing this hypothesis, the mean score for security threats awareness is 4.33 and the mean score for perceived privacy is 5.17 in the scale of 1 to 7. The standard deviation of the security threats awareness score is 1.15 and the standard deviation of the r perceived privacy score is 0.75 (see Table 6). We tested to see if the slope significantly different from zero, and found that the P value is 0.149, which is considered significant. Therefore, hypothesis is not rejected.

Table 6: Data of the Security Awareness and Perceived Privacy

	Observation number	First quartile	Third quartile	Median	Mean	St.Dev
Security Awareness	357	3.5	5	4.5	4.33	1.15
Perceived Privacy	357	4.8	5.5	5.2	5.17	0.75

The Fifth Hypothesis (H5)

Our last hypothesis states that awareness of the security threats is positively associated with the trusting social media. Testing this hypothesis, the mean score for security awareness is 4.82 and the mean score for user's trust is 4.15 in the scale of 1 to 7. The standard deviation of the security awareness score is 1.46 and the standard deviation of the user's trust score is 1.01 (see Table 7). Both score distributions are fairly symmetric. The Pearson correlation coefficient between the technical competences of social network users and the user's perceived level of social media system reliability is 0.63, which indicates a fairly strong positive correlation. The P-value in testing the zero correlation is less than 0.1%, which means the correlation is very significant. Therefore hypothesis cannot be rejected.

Table 7: Data of the Security Awareness and level of user's trust

	Observation number	First quartile	Third quartile	Median	Mean	St.Dev
Security Awareness	357	2,78	42.2	45	4.82	1.46
Trust	357	3.43	5	4.22	4.15	1.01

CONCLUSION AND SUMMARY

Social networks definitely can be fun, but users should be aware of the threats and the risks of social media and behave with the needed level of skepticism. There are in fact real and perceived consequences of inappropriate use of social media networks which may lead to information and financial loss consequence caused by security and privacy incidents.

This study was conducted online targeting youngsters as a sample of the study. Although social networks are quite popular among the youngsters worldwide, comparing these findings with elder people who used the social networks may give a new insight.

In the study five hypotheses were test related to security threats created from using social networks. The first two hypotheses test users' attitudes towards social media and awareness of risks associated with. The study shows that in spite of the users' awareness of social media networks risks but they act positively in using them. In the third hypothesis the peers word of mouth association with security threats of social networks is tested, the study reveals that peers word of mouth is positively associated with security risks of the social media. In the fourth and fifth hypotheses users' awareness of security threats to their privacy and trusting against the social media networks is tested. Results show positive correlation between security threats to both privacy and trust.

Based on the results of the presented data analysis and besides focusing on the awareness of the risks of the use of social media, and to further extend the benefits of this study, we have collected that have to do with the participants' perceived benefits and drawbacks of the social media networks. We found that almost all participants (94%) agree that the social network media makes it easier to keep in touch with family and friends, especially if they live far away, and 76% of the participants indicate that they can make new friends by connecting with friends of friends that they might not know. Most of participants of the study (68%) do not think about the negative effects of having social networking accounts, even though they agree that not setting the privacy settings properly or liking someone's photo can have a negative results. In addition, 43% only believe that social networking can ruin relationships as people may get jealous when they find out their companion (husband, wife, boyfriend or girlfriend) is

exchanging messages with other people. However, almost half of the participants (49%) believe that it can be a waste of time as people can visit a site to check on thing and end up spending more time (on the social media website) than they originally anticipate, and as a result, not doing anything useful during that time. We believe that the results are due to the unique characteristics of social media: openness, participation, and sharing. However, despite rapid adoption, we find that a growing concern and skepticism regarding the use of social media exists among the social network users.

RECOMMENDATIONS FOR USERS

Although many people around the world use social networking, it should only be used as a tool. There are positives to this new technology but also there are negatives. These social networks allow an individual to have thousands of "friends." However, these supposed "friends" are really no more than strangers. Therefore, careful attention needs to be paid when using the social network sites; else it may be affecting users in negative ways. As a user you may review a site's privacy policy. Some sites may share information, such as email addresses or user preferences, with other parties. If a site's privacy policy is vague or does not properly protect your information, do not use the site.

Do not assume privacy on a social networking site. Review a site's privacy policy. Some sites may share information, such as email addresses or user preferences, with other parties. If a site's privacy policy is vague or does not properly protect your information, do not use the site. Even if the privacy policy properly protects your information, confidential information should not be shared. You should only post information you are comfortable disclosing to a complete stranger. Also be careful whom you add as a "friend," or what groups or pages you join. The more "friends" you have or groups/pages you join the more people who have access to your information. Taking all things into consideration, it's important to determine your individual use of social networking and decide how it affects you personally.

REFERENCES

Aichner, T. and Jacob, F. (March 2015). "Measuring the Degree of Corporate Social Media Use". International Journal of Market Research 57 (2): 257–275.

Agarwal, R., Gupta A.K. & Kraut, R. (2008) Editorial Overview: he Interplay Between Digital and Social Networks. Information Systems Research, 19(3), pp. 243-252.

Boyd, D. and Ellison, N. (2007) Social network sites: Definition, history, and scholarship, Journal of Computer Mediated Communication, 13 (1), 210-230.

Chen HT and Kim Y. (2013). "Problematic Use of Social Network Sites: The Interactive Relationship Between Gratifications Sought and Privacy Concerns". Cyberpsychology, Behavior, and Social Networking 16 (11): 806–812.

Duggan, M (2015). Mobile Messaging and Social Media 2015. PEW RESEARCH CENTER. Retrieved from the WWW on January 10, 2016 at: http://www.pewinternet.org/2015/08/19/mobile-messaging-and- social-media-2015/

Gao, H., Hu, J., Huang, T., Wang, J., and Chen, Y.(2011). Security Issues in Online Social Networks. EEE INTERNET COMPUTING, 14(4), pp. 56-63

Hafez, A. I., Al-Shammari, E. T., Hassanien, A. E., Fahmy A. A. (2015). Community detection in social networks using logic-based probabilistic programming, Journal of Social Network Mining, 2(2), pp.158-172

Jayson, S. (2014). Social media research raises privacy and ethics issues USA TODAY 6:03 p.m. EDT March 12,2014. Retrieved from the WWW on Mrch 11, 2016 at: http://www.usatoday.com/story/new s/nation /2014/03/08 /data-online-behavior- research/5781447/&gt

Kaplan A. M. and Haenlein M.(2010). "Users of the world, unite! The challenges and opportunities of social media". Business Horizons 53 (1). p. 61

Ma, M., R. Agarwal. 2007. Through a glass darkly: Information technology design, identity verification, and knowledge contribution in technology-mediated communities. Information Systems Research. 18(1) pp. 42–67.

Metcalfe, H. R. (2010). Libel in the blogosphere and social media: Thoughts on reaching adolescence. Charleston Law Review, 5(3), 481–501.

Oinas-Kukkonen, H, Lyytinen, K. and Yoo, Y(2010) .Social Networks and Information Systems: Ongoing and Future Research Streams.Journal of the Association for Information, 11(2) 11(2)

Obar, J. A. and Wildman, S. (2015). "Social media definition and the governance challenge: An introduction to the special issue". Telecommunications policy 39 (9): 745–750.

odri, V., and Adamopoulos, P. (2014. "Social Commerce: An Empirical Examination of the Antecedents and Con sequences of Commerce in Social Network Platforms," ICIS 2014, Auckland, New Zealand, p. 16.

Schejter, A.M.; Tirosh, N. (2015). ""Seek the meek, seek the just": Social media and social justice". Telecommunications policy 39 (9): 796–803.

Semitsu, J. P. (2011). From Facebook to mug shot: How the dearth of social networking privacy rights revolutionized online government surveillance. Pace Law Review, 31(1), 291–381.

Taylor, K. R. (2014). Anything you post online can and will be used against you in a court of law: Criminal liability and First Amendment implications of social media expression. National Law Guild Review, 71, 78–106.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005

Notes: