Using Web-Referral Architectures to Mitigate Denial-of-Service Threats

[1]Srikanth Bethu, [2]J. Sasi Kiran, [3]K. Kanthi Kumar
[1]Dept. of CSE, HITS Engineering College, JNTU, Hyderabad, AP, India
[2]Dept. of CSE, MNR College of Engg. & Tech, Medak, AP, India
[3]Dept. of ECE, HITS Engieering College, JNTU, Hyderabad, AP, India

Abstract

The web is a complicated graph, with millions of websites interlinked together. To use this web site-graph structure to mitigate flooding attacks on a website, using new web referral architecture for privileged service ("WRAPS"). WRAPS allows a legitimate client to obtain a privilege URL through a simple click on a referral hyperlink, from a website trusted by the target website. Using that URL, the client can get privileged access to the target website in a manner that is far less vulnerable to a distributed denial-of-service (DDOS) flooding attack than normal access would be. WRAPS does not require changes to web client software and is extremely lightweight for referrer websites, which makes its deployment easy. The massive scale of the web site-graph could deter attempts to isolate a website through blocking all referrers. WRAPS enables legitimate clients to connect to a website smoothly in spite of a very intensive flooding attack, at the cost of small overheads on the website's ISP's edge routers. The security properties of WRAPS and a simple approach to encourage many small websites to help protect an important site during DOS attacks.

Keywords

Distributed Denial-of-Service, ISP's Edge Routers, URL

I. Introduction

The web is a complicated referral graph, in which a node (website) refers its visitors to others through hyperlinks. This chapter proposes how to use this graph (called a site graph) as a resilient infrastructure to defend against Distributed Denial of Service (DDoS) attacks that plague websites today. Suppose eBay allows its trusted neighbors (websites linking to it) such as PayPal to refer legitimate clients to its privileged service through a privileged referral channel. A trusted client needs only to click on a privileged referral hyperlink on PayPal to obtain a privilege URL for eBay, which certifies the client's service privilege. When eBay is undergoing a DDoS attack and not accessible directly, routers in its local network will drop unprivileged packets to protect privileged clients' flows. As such, a client being referred can still access eBay even during the attack. Referral relations can be extended over the site graph: e.g., PayPal may refer its neighbors' clients to eBay. In this way, a website could form a large-scale referral network to fend off attack traffic. The architecture we propose to protect websites against DDoS attacks, which is refer to as the "Web Referral Architecture for Privileged Service" or "WRAPS", is built upon existing referral relationships among websites. Incentives for deployment, therefore, are not a significant barrier, provided that the overhead of the referral mechanism is negligible. Indeed, a website that links to others provides a better experience to its own customers if the links it offers are effective, and so websites have an incentive to serve privileged URLs for the sites to which they link.

The overheads experienced by this website's users will be either nonexistent if the website offers privileged referrals to only customers that have already authenticated for other reasons, or minimal if the website will refer any client after it demonstrates it is driven by a human user (in the limit, asking the user to pass a reverse Turing test or "CAPTCHA"). The referrer incurs only negligible costs in order to make referrals via our technique. In order to evaluate the likely efficacy of WRAPS, we implemented it in an experimental network environment which includes a software router and Linux-based clients and servers. WRAPS enables clients to circumvent a very intensive flooding attack against a website, and imposes reasonable costs on both edge routers and referral websites. A limitation of WRAPS is that it requires modifications to edge routers, as many capability-based approaches do. However, unlike those approaches, WRAPS does not require installing anything on a Web client. This chapter explores the importance of web site-graph topology to the efficacy of WRAPS.

A. Problem Definition

Overlay-based approaches assume the existence of an overlay infrastructure in which a set of dedicated nodes collaborate to protect an important website, and need to modify protocols and client-side software. Overlay routing could increase end-to-end latency, though such overheads can be significantly reduced using techniques such as topology aware overlays and multipath overlays.

In capability based approaches, the capability distribution service itself could be subjected to DDOS attacks. The problem becomes serious on open computing environment, where a service provider may not know most of its client beforehand. All exisisting capability-based approaches require modifications to client side software. Both Overlays based and capability based approaches works only in human-driven activities to identify authorized but unknown clients, which has been subjected to various attacks.

1. Objectives

A trick a compromised privileged client can play is to craft packets with TTLs too small to reach the target website in order to cause congestion on the path toward that website. This attack is still subject to rate limiting if the congestion happens within the protection perimeter of our mechanism. However, since the packets used in the attack will not reach the target website, the website's mechanisms for detecting malicious clients will be avoid. In solution to this threat is to let the edge routers "refill" the TTL value of every packet destined for a host within the ISP's network when it enters the network from the outside. The refill sets the TTL to 255 so as to ensure that the packet will reach its destination.

2. Challenges

A privilege URL hides a capability token inside the suffix of the destination IP field (last one or two octets) and the whole destination port field. The following fields are present in the token:

(i). Key Bit (1 bit)

This field is used to indicate the "authentication key" currently in use. Priority field. This is an optional field which allows the website to define more than one service priority. Here, we use one priority class to describe the approach for clarity of presentation.

(ii). Message Authentication Code (MAC)

A MAC prevents adversaries from forging a capability. The algorithm computing a MAC over a message takes as inputs a secret key k and the message to produce a bit tag. MAC generation is ideally based on a cryptographically strong pseudorandom function (PRF) so that the probability to compute the right tag without knowing k is negligibly larger than 2 For a privileged client i, its MAC is denoted by MAC IPi, where IPi is i's IP address.

II. Related work for Web – Referral Architecture for Privileged Services

This section deals with information and communications technologies take up, development-commerce and check the privileged client communicate to server.

A. Introduction of Web - Referral

Several current and prospective features of Information and Communication Technology (ICT) have facilitated technology enabled crime. These include: ICT becoming intrinsically connected to daily personal and business life computer systems and networks that facilitate commercial and private use but also create risks of subsequent exploitation by criminals computer data that are intrinsically hard to control, this is particularly the case with the internet which was designed to resist outside attempts to control its content or fields of operation computer networks that are global, with information flowing via a number of networks and through a number of jurisdictions computers and computer networks that are fast[1]. Broadband facilitates the rapid downloading and uploading of large video, music and software files. The fact that many computers are now permanently connected to the internet, when coupled with the poor security awareness of many domestic users, renders such computers prone to exploitation. The potential rationale for such attacks could include the obtaining of personal information for identity theft or the use of the computer as a 'zombie' or storage facility for illegal material as has been found to be the case with commercial and university systems. These dangers are likely to be exacerbated by activities such as peer-to-peer file sharing programs or the downloading of files from unknown senders. Fast download times have also facilitated dissemination of content such as pornographic images and pirated software and music particularly through peer-to-peer platforms. Most peer-to-peer software is free and it is believed may contain overt or covert advertising related software. There is also the danger that the software may contain spyware [2].

The increasing use of mobile phones and PDAs, each with ever-increasing storage capacity, constitutes another opportunity for online attacks. Research has indicated, for example, that such devices are routinely used to store personal data and corporate information. The advent of wireless networking increases the likelihood of such information being uploaded and downloaded. In 2005, 22 percent of people reported losing their mobile devices, and, of those, 81 percent had not encrypted the information contained therein [3] .Wireless networks themselves may bring a number of vulnerabilities, key among which is the fact that networks and their data can be accessed without physical access being required. This facility assists both the user and the criminal.

The literature on technology-enabled crime threats is replete with references to 'cybercrime' and 'organized' cybercrime. The extent has been major growth in criminal behavior and activity as a direct or indirect result of technological developments is starting to be questioned. As Wall observes, when so-called cases of cybercrime come to court, they often have the familiar ring of the "traditional" rather than the "cyber" about them'. Indeed, the IBM survey on cybercrime did not, in fact, define cybercrime. There is a possibility that corporations attesting to the presence of cybercrime within their particular sector could actually be commenting upon a range of disparate security intrusions ranging from spam to major viral contamination, only some of which are truly technology-enabled.

Wall [4] has suggested that the globalization of crime opportunities may be constituted by globalization and 'globalization'. The globalization of crime through increased connectivity of computer networks has led to a new law enforcement relationship that is between the global and the local that is, 'global'. The internet has transformed criminal opportunities in three major ways: the communication vehicle of the internet has allowed the increase of information flow that is useful to criminal individuals and organizations.

The impact of e-commerce in the form of increased and increasing global connectivity of computer systems and networks is the creation of more complicated operating systems and reliance upon technology as much as human interaction. Detecting individual malfeasance in such an environment becomes more difficult and the evidence trails perpetrators leave can quickly gain anonymity within a corporate network. There is a danger that organizations incorporate new technology without necessarily being cognizant of the potential criminal exploitation of that technology and the vulnerability to which they open themselves through lack of well-trained staff. As has been noted, the internet was never designed to be secure from exploitation. The strength of the internet in terms of its rapid communication facility has become one of its weaknesses. Extraterritoriality, the notion that the internet has no geographic boundaries, has driven the e-commerce revolution. Unfortunately, the criminal fraternity operates online under the same free market principles, while legislative and law enforcement endeavors launched against them suffer from geographical and cultural restrictions.

In [5] describes that organizations had improved the protection of their IT systems in the three key areas of the use of security technologies, the use of information security policies, practices and procedures and the use of information security standards or guidelines. There remained, however, a number of vulnerabilities such as inadequate staff training in computer security management, and poor security culture within organizations. Along with a general recognition that information security breaches are increasing, most respondents to the survey dissatisfied with the level of funding allocated to IT security within the organization.

A major factor in technology-enabled crime threats remains the human element, with a continuation of the movement from syntactic (attacking the computer) to semantic (attacking the computer user) attacks likely. An indication of human vulnerabilities may be seen in 2006 on the rationale for the success of phishing attacks. This chapter shows 22 participants 20 web sites and asked to determine which were fake and why. The best phishing site was able to fool more than 90 percent of participants. Indicators that are designed to signal trustworthiness were not understood or even noticed by many participants. Five of the 22 participants (23%) only used the content of the website to evaluate authenticity, without looking at any portions of the browser. Fifteen of the 22 participants proceeded without hesitation when faced with a popup warning about fraudulent certificates. Participants proved vulnerable across the board to phishing attacks. In our study, education, age, sex, previous experience, and hours of computer use do not show a statistically significant correlation with vulnerability to phishing [6].

B. Information & Communication Technologies Take Up

A primary vehicle for technological innovation has been, and will continue to be, the internet which was created in 1969 as a research network sponsored by the Advanced Research Project Agency (ARPA) for the Department of Defense in the United States, hence its original name, ARPANET. The internet's primary function at this time was to maintain the flow of defenses-related information during a catastrophic nuclear attack. Given that rationale, it was not required, nor designed, to be a highly developed or intelligent system. Internet use has grown since the initial handful of ARPA machines so that in June 2006, there were 439,286,364 internet hosts (Internet Systems Consortium 2006) and in December 2006 there were 1,091,730,861 users (Internet World Stats 2006). However, the basic nature of the internet, a vehicle for conveying packets of data between devices – the 'end-to-end principle' – has remained unchanged and the resultant architecture, whilst embracing the original unfettered communication precept of the internet, has facilitated an increasing vulnerability to inadvertent technical failings as well as to advertent criminal activity.

C. Development

Moore's Law predicts that the number of transistors able to be positioned per square inch on an integrated circuit will double every year (which to date has proved to be a correct assertion) and a common route to imagining the technological future is to consider the performance of technology in terms of its relative speed, size or cost. The first computer occupied 70 cubic meters of floor space. In the 1970s a megabyte of semiconductor memory cost approximately $550,000. In the 1990s it cost $4. Microprocessors in the 1990s were 100,000 times faster than their 1950s predecessors. Based on those rates of change, a desktop computer in 2020 will be as powerful as all the computers currently situated in Silicon Valley in the United States. Miller and colleagues have suggested that such rapid improvement may be accelerated by computers that combine optical and silicon technology to facilitate transfer of data within a computer chip via laser. The National Nanotechnology Initiative in the United States (National Science and Technology Council) projected that developments in Nano -science and Nano-engineering were likely to change the way things are designed and made things like vaccines, computers, automobile tires and objects not yet imagined. In relation to such technology the likely increased use of micro electro mechanical systems (MEMS) is set to have a great potential impact and significance.

MEMS are small from a micrometer (one-millionth of a meter) to a millimeter – devices or systems that combine electrical and mechanical components and currently permit industry to add beams, gears and springs to minute devices. A potential future use of MEMS might be to enhance information storage, processing and communication. In the next few decades significant progress is likely to be made in relation to the application of technology or, as Deloitte Touché Tohmatsu prefer, TMC (Technology, Media and Communications).

III. Design and Implementation

WRAPS depends on the target's ISP's edge routers to classify inbound traffic into privileged and unprivileged, and to translate fictitious addresses of privileged packets to the real location of the service. It also depends on routers inside the website's local network to protect privileged flows. We implemented these functions in a Click software router. Click is modular software architecture for creating routers.

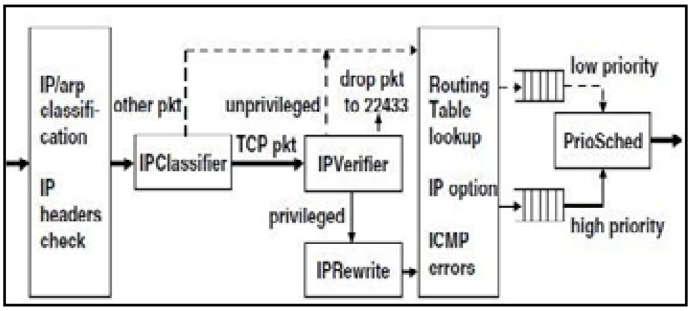


Fig. 1: WRAPS Elements on a Click Packet Forwarding Path

A Click router is built from a set of packet processing modules called elements. Individual elements implement certain router functions such as packet classification, queuing and scheduling. A router is configured as a directed packet-forwarding graph, with elements on its vertices and packet flows traversing its edges. A prominent property of Click is its modularity, which makes a Click router extremely easy to extend.

In this added WRAPS modules to an IP router configuration. WRAPS elements planted in the standard IP forwarding path are illustrated in above figure (1). The above architecture added 5 elements such as IP Classifier, IP Verifier, IP Rewrite, Priority queue and Preached. IP Classifier classifies all inbound packets into TCP packets which are forwarded to IP Verifier, and other packets, such as UDP and ICMP, which are forwarded to the normal forwarding path. IP Verifier verifies every TCP packet's capability token embedded in the last octet of the destination IP address and the 2-octet destination port number. Verification of a packet invokes the 4- byte input (the source IP address) and a 64-bit secret key. The packets carrying correct capability tokens are sent to IP Rewrite, which sets a packet's destination IP to that of the target website and destination port. Unprivileged packets, except for those destined for port, follow UDP and ICMP traffic, unprivileged traffic to port is dropped.

In this implementation, the target website first blocks all access to its privilege port. Whenever a new client obtains privilege, a script running on the web server adds a new filter rule to IP tables, explicitly permitting that user's access to the privilege port. Direct utilization of IP tables may potentially cause the performance degradation of net filter when there are many privileged clients. Our general approach, however, could still scale well after proper modification of the net filter module, adding a fast searching algorithm like Bloom filters to the kernel. To establish a privileged connection, packets from the target web server to a privileged client must bear the fictitious source address and port in that client's privilege URL. In this implementation, to modified the target server's Linux, Kernel to monitor the privilege port. Whenever a packet is emitted with that source port, the kernel employs the secret key and the MAC to generate a capability token, and embeds this token into last octet of the source IP field and the source port field. This address translation can also be done in the firewall, and configured to support more than two priority classes.

A. Modules

1. Client, WRAPS, DDOS, Server, EDGE Router

(i). Client

A client may obtain a privilege URL either directly from the target website or indirectly from the website's trusted neighbors. A website offers a client a privilege URL if the client is referred by one of the site's trusted neighbors, or is otherwise qualified by the site's policies that are used to identify valued clients, for example, those who have paid or who are regular visitors. A qualified client will be redirected to the privilege URL generated automatically using that client's identity, service information, and a server secret.

(ii). WRAPS

When a website is under a flooding attack, legitimate but as yet-unprivileged clients will be unable to visit that site directly, even merely to apply for privileged service. The central idea of WRAPS is to let the trusted neighbors of the website refer legitimate clients to it, even while the website is under a flooding attack. The target website will grant these trusted neighbors privilege URLs, and may allow transitive referrals: a referrer can refer its trusted neighbor's clients to the target website.

(iii). DDOS Server

An adversary may perform an extensive search on the short MAC in a privilege URL. Specifically, the adversary first chooses a random MAC to produce a privilege URL for the target website. Then, it sends a TCP packet to that URL. If the target website sends back some response, such as snack or reset, the adversary knows that it made a correct guess. Otherwise, it chooses another MAC and tries again. This threat has been nullified by this protection mechanism. The firewall of the target website keeps records of all the website's privileged clients and only admits packets to privilege port from these clients. If the adversary uses its real IP address for sending query packets, the website will not respond to the probe unless the adversary has already become the site's privileged client. If the adversary spoofs a privileged client's IP address to penetrate the firewall, the website's response only goes to that client, not the adversary. Therefore, the adversary will never know whether it makes a correct guess or not.

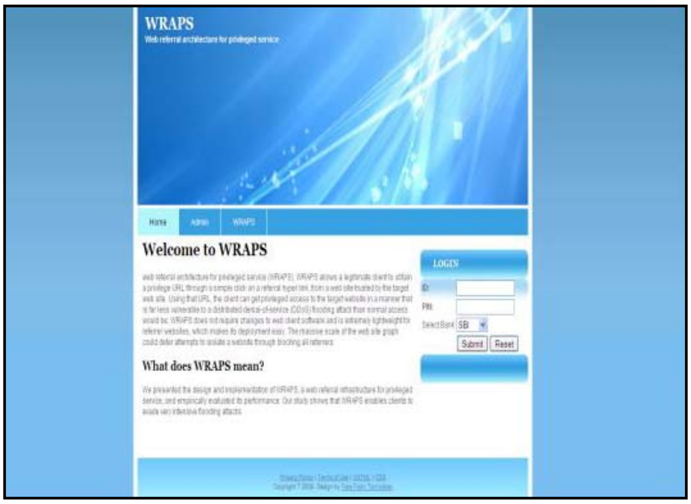
This section must stress here that this approach does not introduce new vulnerabilities. Only a client trusted by the target website directly or referred by trusted neighbors will have its IP address on the firewall's white list. The storage for the white lists is negligible for a modern computer recording a million clients' IP addresses takes only 4 Mbytes. Therefore, our approach does not leave an open door to other resource depletion attacks.

(iv). EDGE Router

A website (the target) is protected by the edge routers of its ISP or organization, the routers inside its local network, and a firewall directly connected to or installed on the site's web server.

The target website shares a secret long-term key k with its edge routers on the protection perimeter. Using this key, the website periodically updates to all its edge routers a shared verification key. We call a period between updates a privilege period. The http server of the website listens to two ports, one privileged and one not. The local firewall controls access to those ports. Only the port corresponding to the unprivileged traffic, typically port 80, is publicly accessible. The other port can be accessed only by packets with source IP addresses explicitly permitted by the firewall (as instructed by the web server); this port is called the privilege port.

IV. Experimental Results



Welcome to WRAPS

web referral architecture for privileged service (WRAPS). WRAPS allows a legitimate client to obtain a privilege URL through a simple click on a referral hyper link, from a web site trusted by the target web site. Using that URL, the client can get privileged access to the target website in a manner that is far less vulnerable to a distributed denial-of-service (DDoS) flooding attack than normal access would be. WRAPS does not require changes to web client software and is extremely lightweight for referrer websites, which makes its deployment easy. The massive scale of the web site graph could deter attempts to isolate a website through blocking all referrers.

What does WRAPS mean?

We presented the design and implementation of WRAPS, a web referral infrastructure for privileged service, and empirically evaluated its performance. Our study shows that WRAPS enables clients to evade very intensive flooding attacks.

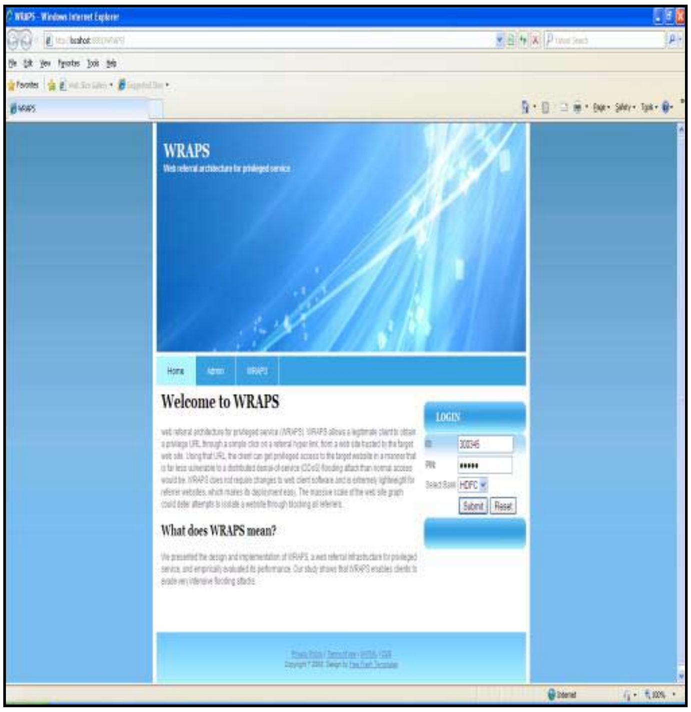
ID:
PIN:
Select Bank: SBI

Fig. 2: Home Page

Fig. 3 shows how the privileged user enter user ID with password and specific bank submitted to server. By using this page the privileged user to check his account details.

Fig. 4 contains the user account details which have two hyper links i.e. Account details and transactions.

Fig. 5 contains account details like account id, name, bank name account type and account balance.



Welcome to WRAPS

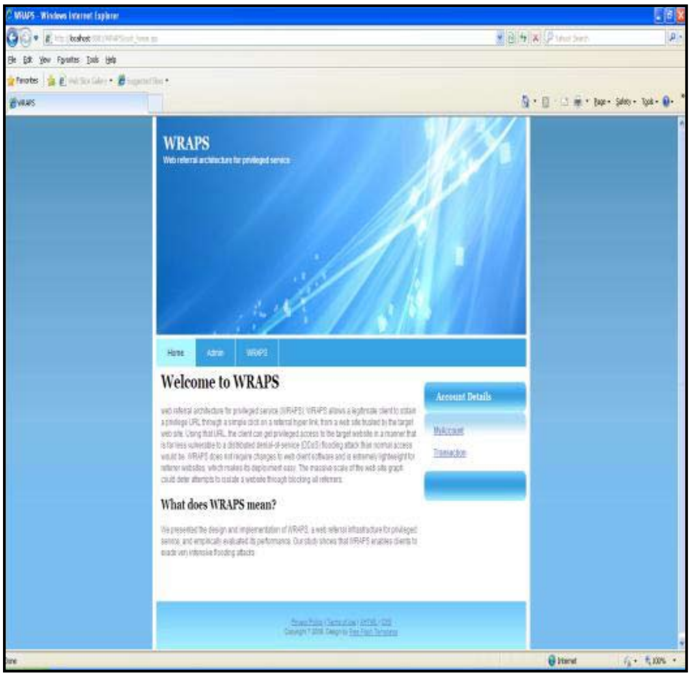
web referral architecture for privileged service (WRAPS). WRAPS allows a legitimate client to obtain a privilege URL through a simple click on a referral hyper link, from a web site trusted by the target web site. Using that URL, the client can get privileged access to the target website in a manner that is far less vulnerable to a distributed denial-of-service (DDoS) flooding attack than normal access would be. WRAPS does not require changes to web client software and is extremely lightweight for referrer websites, which makes its deployment easy. The massive scale of the web site graph could deter attempts to isolate a website through blocking all referrers.

What does WRAPS mean?

We presented the design and implementation of WRAPS, a web referral infrastructure for privileged service, and empirically evaluated its performance. Our study shows that WRAPS enables clients to evade very intensive flooding attacks.

ID: 30046
PIN: •••••
Select Bank: HDFC

Fig. 3: Home Page with Customer Login Page



Welcome to WRAPS

web referral architecture for privileged service (WRAPS). WRAPS allows a legitimate client to obtain a privilege URL through a simple click on a referral hyper link, from a web site trusted by the target web site. Using that URL, the client can get privileged access to the target website in a manner that is far less vulnerable to a distributed denial-of-service (DDoS) flooding attack than normal access would be. WRAPS does not require changes to web client software and is extremely lightweight for referrer websites, which makes its deployment easy. The massive scale of the web site graph could deter attempts to isolate a website through blocking all referrers.

What does WRAPS mean?

We presented the design and implementation of WRAPS, a web referral infrastructure for privileged service, and empirically evaluated its performance. Our study shows that WRAPS enables clients to evade very intensive flooding attacks.

Fig. 4: Customer Account Details Page

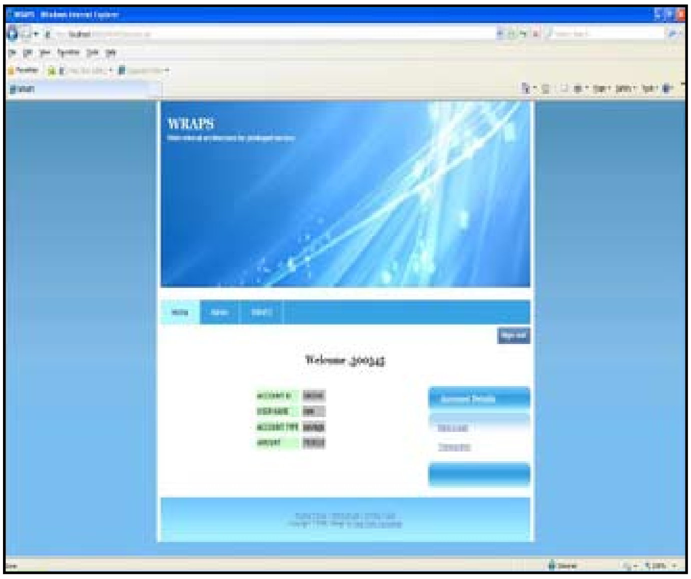


Fig. 5: Customer Account Details

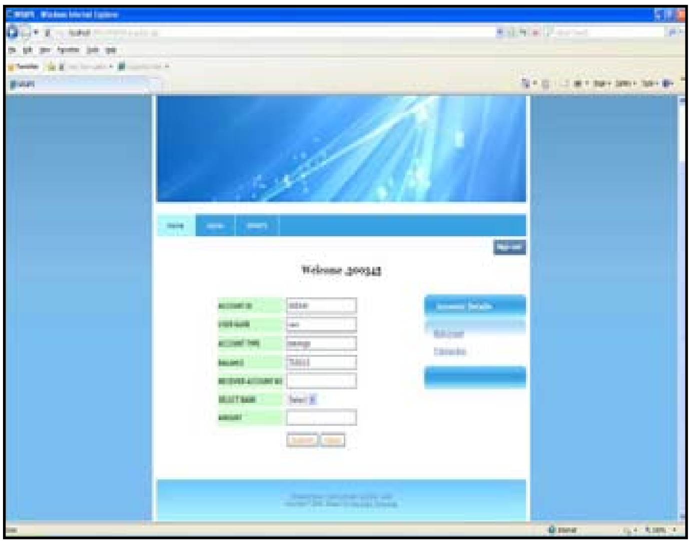
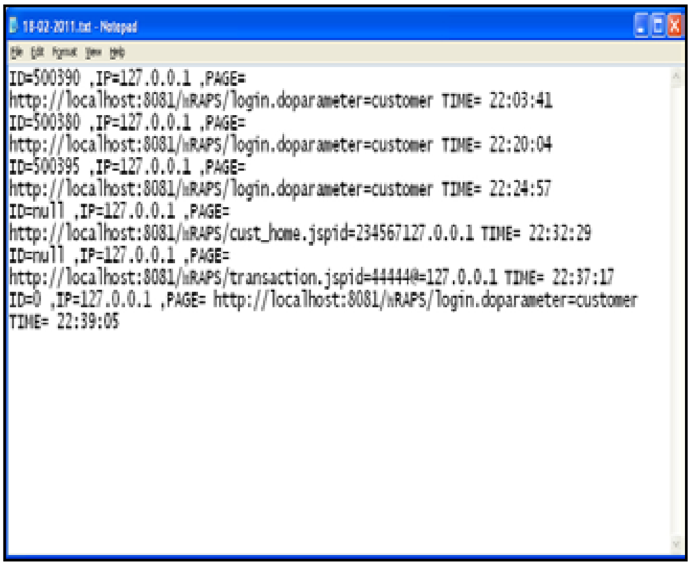
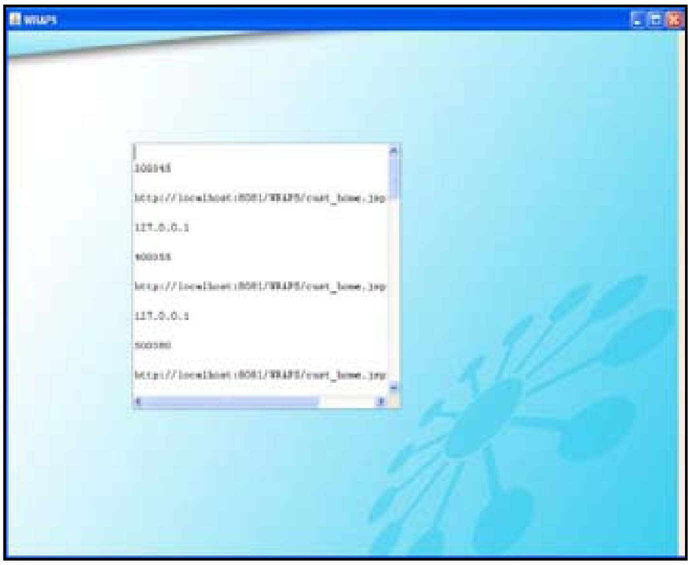


Fig. 6: Customer Transactions Details



```
ID=500390 ,IP=127.0.0.1 ,PAGE=
http://localhost:8081/WRAPS/login.doparameter=customer TIME= 22:03:41
ID=500380 ,IP=127.0.0.1 ,PAGE=
http://localhost:8081/WRAPS/login.doparameter=customer TIME= 22:20:04
ID=500395 ,IP=127.0.0.1 ,PAGE=
http://localhost:8081/WRAPS/login.doparameter=customer TIME= 22:24:57
ID=null ,IP=127.0.0.1 ,PAGE=
http://localhost:8081/WRAPS/cust_home.jspid=234567127.0.0.1 TIME= 22:32:29
ID=null ,IP=127.0.0.1 ,PAGE=
http://localhost:8081/WRAPS/transaction.jspid=44444@=127.0.0.1 TIME= 22:37:17
ID=0 ,IP=127.0.0.1 ,PAGE= http://localhost:8081/WRAPS/login.doparameter=customer
TIME= 22:39:05
```

Fig. 7: DDOS Monitor



```
300345
http://localhost:8081/WRAPS/cust_home.jsp
127.0.0.1
400355
http://localhost:8081/WRAPS/cust_home.jsp
127.0.0.1
500380
http://localhost:8081/WRAPS/cust_home.jsp
```

Fig. 8: Edge Router

Fig. 6 contains the user account details i.e. Account details which have My Account and Transactions. By using transactions we send amount to another bank account. If click account link to get the account details of specific privileged user.

Fig. 7 shows the DDOS monitor means it contains user ID, IP address login details. If it's more than 3 from null users it will go to put in different access.

Fig. 8 contains authorized IP addresses and user ids which are Web Referral Architecture for Privileged Services. In administrative page when to click WRAPS hyper link it displays these details.

V. Conclusion

DDOS flood attacks continue to harass today's Internet websites. This research shows that such threats could be mitigated through exploring the enormous inter-linkage relationships among the websites themselves. Improvement of Site-ranks with a Rewarding Link from an Important Website to propose WRAPS a web referral infrastructure for privileged service that leverages this idea. WRAPS has been constructed upon the existing web site-graph, elevating existing hyperlinks to privilege referral links. Clicking on referral links, a trusted client can get preferential access to a websites under a flooding attack.

The design and implementation of WRAPS, a web referral infrastructure for privileged service, and empirically evaluated its performance. WRAPS enables clients to avoided very intensive flooding attacks, connecting to a website smoothly even when any normal connection became unrealistic. The overheads of WRAPS are affordable to routers and almost negligible to referrer websites. A real web site graph to analyze the security properties of WRAPS, and found that the site graph had many features that would benefit WRAPS. WRAPS is a simple approach to encourage many small websites to protect the main website and facilitate the search for referrers during DOS attacks.

References

[1] J. Wu, K. Aberer,"Using Site rank for p2p Web Retrieval," Technical Report IC/2004/31,SwissFed.Inst. Technology,Mar.2004.

[2] X. Wang, M. Reiter,"Wraps: Denial-of-Service Defense through Web Referrals", Proc.25thIEEESymp. ReliableDistributedSystems (SRDS), 2006.

[3] L. von Han, M. Blum, N.J. Hopper, J. Langford, "CAPTCHA: Using Hard AI ProblemsforSecurity", AdvancesinCryptologyEUROCRYPT'03. SpringerVerlag, 2003.

[4] R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, S. Shenker,"Controlling High Bandwidth Aggregates in the Network", Computer Comm. Rev., vol. 32,no.3,pp.62-73, July 2002.

[5] J. Ioannidis, S. Bellovin,"Implementing Pushback: Router-Based Defense against DDoS Attacks", Proc. Symp.

Srikanth Bethu received his engineering degree B.Tech in Computer Science and Engineering from JNTUH, Hyderabad in 2008 and M.Tech from Osmania University, Hyderabad, in 2011.He has done his internship for M.Tech project during 2010 - 2011in implementing and generating AADHAR Biometric cards for the Government of A.P state using Biometric system, under 4G Identity solutions, Hyderabad. Now presently he is working as an Assistant Professor in Holy Mary Institute of Technology and Science, JNTUH, Hyderabad. His research works are in the areas of Parallel and Distributed Systems, Data mining and Warehousing, Web technology and Ontology, Network Security. He has been attended several International and National Conferences and presented several papers based on his research areas. He has published several International and National journals on his topics.

J. Sasi Kiran Graduated in B.Tech from JNTU in 2002. He received Masters Degree in M.Tech from Bharath University, Chennai, in 2005 and pursuing Ph.D from University of Mysore, Mysore in CSE .At present he is pursuing his research at Centre for Advanced Computational Research (CACR) of Anurag Group of Institutions (AGOI), Hyderabad. He served as an Associate Professor in Vidya Vikas Institute of Technology, Hyderabad from 2004 to 2013 and working as Associate Professor in CSE Dept. in MNR College of Engg. & Tech, Sangareddy, Medak Dt, A.P, India. His research interests include Image Processing, Data Mining and Network Security. He has published research papers in various National, International conferences, proceedings and Journals. He is a life member of IE, ISTE, ISCA, IAE, IS-USA, IACST, AIRCC and Management Committee Member of CSI. He has received significant contribution award from Computer Society of India in 2012.

K. Kanthi Kumar graduated in B.Tech (ECE) from Nagarjuna University in 2002. He received Masters Degree in M. Tech (C&C) from Bharath University, Chennai in 2005and pursuing Ph.D from JNTUK, Kakinada in ECE. He served as Assistant Professor at Newton’s Institute of Technology, Macherla from 2005 to 2007 and from 2007 he worked in Vidya Vikas Institute of Technology, Hyderabad as Associate Professor up to 2012. He is working as Associate Professor from 2012 at Holy Mary Institute of Technology & Science. His research interests are Network Security, Computer Networks, and Image Processing. He has published research papers in various National, International conferences, proceedings and Journals. He is a life member of ISTE.