Enhanced Web Referral Architecture with Flexible Security Service

Ramesh R
IEEE and ACM, student member
Department of CSE, VJCET
Ernakulam, Kerala, India

Resmi Cherian
Department of CSE, VJCET
Ernakulam, Kerala, India

ABSTRACT

Web hierarchy can be utilized for setting up an effective referral service among trusted parties such that an alternative path for web service can be made available, even when the target or destination server is under DDoS attacks. In our proposed referral service, we are employing a third party server for protecting a hierarchy of websites from DDoS attacks. The security architecture is designed in such a way that the clients referred from source to destination server using the proposed methodology are properly evaluated using a socially based trust system and source server specifies the privilege level of the referred clients to destination server using a Persistent Referral Service architecture. Our method thwarts attack attempts by compromised source servers and malicious referred clients towards target servers. We also show that our system can be extended for handling phishing attacks. For that the financial or banking websites should implement this referral service.

General Terms

Web Referral, Privilege Channel.

Keywords

denial of service; referral; web sitegraph; web services architecture; phishing.

1. INTRODUCTION

Most important of all networking attacks from a server point of view indeed points to distributed denial-of-service attacks (DDoS). Even with advanced communication protocol system currently implemented in the protection perimeter (consisting of local routers, edge router and powerful firewall) in target server, DDoS attack seems hard to avert. Internet service providers are increasingly impatient to have a communication protocol that not only avoids IP spoofing, flooding attacks etc but also provides more security against DDoS attacks.

Existing referral service coupled with Persistent Referral Service Architecture (PRS) can augment the security of web-servers from DDoS attacks. The referral service could be employed from one website A to another website B in Site-Graph [1] in a transitive model. That is, the referred client should be a member of website A as well as website B. Also the existing system taken advantage of the referral tree can expand the security perimeter around an important web server, there by enhancing the security of an important web server under DDoS attacks.

In this paper, we are proposing a system in which the reliability of the popular search engines such as Google, Yahoo etc. can be utilized for providing value-added service to important web servers even under DDoS attacks. The main advantage of this system is that, here normal users are also given privileged channels. Even though the bandwidth quota in this service would not be similar to the bandwidth provided in normal WRAPS [5] privilege channel to important websites, privilege channel access to websites is ensured. The proposed system exploits the existing reliability and serviceability offered by popular search engines. This system can also serve as an alternative for establishing safe channel connection to important financial websites.

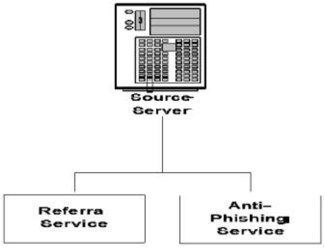

Figure1. Proposed dual service using PRS

Most of the anti-phishing mechanisms necessitate us to install a third party toolbar software or browser controlled plug-in. Each methodology has its own drawback which clearly shows that not all phishing attacks can be prevented. This indeed creates a sense of insecureness in users for using online banking system. Online banking is not a new buzz word for computer enthusiasts like us but it is indeed a new thing for users who actually started using Internet and unaware about phishing attacks, even not necessitating for the creation of similar looking websites for stealing user information. We are proposing an idea that can be implemented in web search sites like Google as a way to attract new users apart from users willing to join social networking or other fun related sites. The idea is to implement a tool in web search engines with the help of a centralized database system that can be used to mitigate phishing attacks. This centralized system can provide a secure way to perform online banking transactions. This method will not require installing any anti-phishing software in the user's side. The entire security system is going to be implemented at the source server itself. Anti-phishing attacks are normally handled using inbuilt tools used in Internet browsers or by installing other toolbars integrated with the web browser. There are several approaches available to avert phishing attacks.

2. RELATED WORKS

Familiar works in the field of web server protection involves Overlay node architecture [8], [9], [10] and [11], Capability token approach [6] and [7], Web referral architecture for privilege service [4], etc. In overlay node architecture, the target website to be protected is surrounded by overlay nodes, which provides suitable protection perimeter for the inbound and outbound traffic of the web server. Because of its implementation complexities, Capability token approach came into existence. In this approach, any remote or referral web server willing to establish a reliable channel with the target website, need to pass through a capability token acquisition process. But the main drawback of this approach undermines the very existence of this method, as the server providing the token might come under denial of service attack. Then a more sophisticated approach called web referral architecture for referral service was developed.

In WRAPS [4] smaller websites provides referral service to important web servers, such that under DDoS attacks on important websites, the privileged service offered by these smaller or other important websites could be utilized to provide privileged clients the privileged channels. In this, websites offering WRAPS service to important websites will generate privilege URL or a privilege referral hyperlink using a script. This privilege URL will be a fictitious URL, which differs from normal hyperlink URL, such that in this a capability token will be hidden within the URL. The privilege URL with the help of meta-refresh redirection will redirect the client's browser to the target website. The websites willing to offer WRAPS service to important websites register as referrers with the target website. This will be on a contract basis. The main inclination for smaller websites to provide WRAPS service is that, they will be provided with rewarding links from important websites which improves there siterank [1]. In WRAPS, the used methodology stresses upon the privileged service for privileged clients. Also WRAPS requires modifications of the routing and network communication protocols to work properly at edge router. Our paper illustrates a method of offering valid clients (i.e. normal users) a privilege channel service to the target web server in real time using simplistic web-referral architecture.

3. DESIGN

PRS (Persistent Referral Service) can be used to implement an architecture using popular search engines like Google, Yahoo etc, such that sites can register with these search sites on contract basis. These search engines provides a privilege channel to target web server for valid clients only.

The proposed system mainly focuses on providing valid clients a privilege or reliable service channel to target server through search sites. The client after authenticating with the particular search site gets referral service to other valid registered sites. When the client search for the target site, normal search results will be displayed. Whenever the client clicks on the target site's URL, search engine performs a validation check of that particular target website. If it is a registered site, depending upon the privilege of valid client, a privilege URL (containing the capability token) will be generated at the target server and will be forwarded to the source server requesting service and using meta-refresh redirection command, browser will be redirected to target website. If the clicked target server is not registered, then a normal hyperlink will be provided.

The target web servers in need of this service have to register with the search engines or other social networking websites. Since this is a value added service, contracts similar to ad-click service like Google ads can be offered. The main security issue for target servers is to protect their port number from being identified. Here the search engines are referred as Source servers.

A small program at the source server calculates the privilege level of valid clients depending on several factors like account access rate by viewing his/her login information , then checking number of emails sent or received, number of linked email accounts etc. We have come-up with a solution, which not only eliminates client-side modifications, but also consider normal users for establishing privilege channel. That is the proposed method is implemented within source site, third party server and target site.

In the initial design, the automatic referral calculator was invoked only at search time. But this method can be improved by reducing the background programming overhead while searching, by providing an option of enabling or disabling referrals from the settings option. Whenever referral service from settings is enabled, the referral level is automatically calculated from his/her social behaviour. The activities of the user automatically update the privilege level. This way we can reduce the overhead at runtime for the calculation of privilege level.

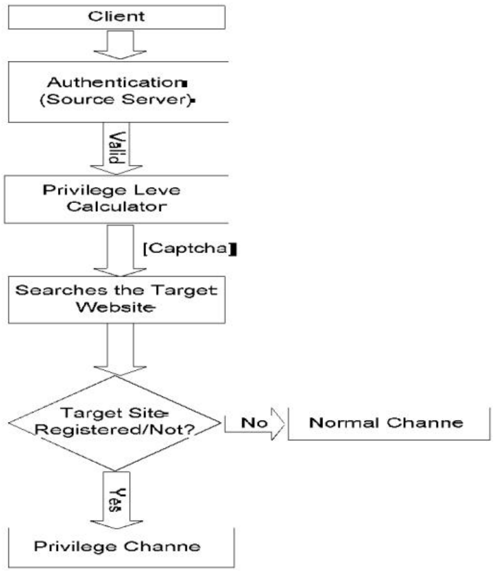

Figure 2. Referral service

In order to prevent new users from misusing PRS system to launch DDoS attack against a registered site, we are using one Captcha test [12] for getting the search page. So that even if numerous users try to create new accounts and launch DDoS attack, Captcha test will further delay the propagation of packets from individual requests. Hence DDoS attacks by creating newer accounts can be prevented.

Each site uses different parameters for calculating the privilege level. Facebook may take factors like number of pictures, number of friends in his/her network, his/her normal interaction within the site (activity pattern) etc. yahoo may use factors like number of valid mails received or sent, number of friends, linking accounts etc.

4. PRIVILEGE LEVEL ESTIMATOR

In today's World Wide Web, features of one site differ from another considerably. As such the methodologies employed in the calculation of privilege levels by the respective source servers also differ. In this paper, we assume the source server to be Google. Google is one of the best and popular search engines presently outshining all other search engines which is evident from its huge share in the advertisement business in the Internet. Also the widely accepted social networking site presently is Facebook.com which has around 750 million registered users. Then Twitter.com which is the best in the blogging segment of the Internet. All these sites produces considerable traffic and in order to protect their reputation, these sites not only offers uninterrupted 24X7 service but also ensures users, the best serviceability in terms of speed while offering referral and other services to neighboring sites.

If the privilege level is calculated by the respective source servers only, a problem may arise. If the user is going to search for a referral service from Google without a valid Google account then the service will not be available. In order to avoid this scenario, we have come up with an idea of integrating account verification of popular websites. This feature is already in use in Yahoo.com, as it can verify account information of user's Google, Facebook, and Twitter as well as all popular sites and can display their respective inbox or front page in the same webpage itself. In India, Yahoo.com has its reputation for having millions of members registered. Also Yahoo.com is widely used in India along with Google, Facebook, and Twitter etc. The notable features of Yahoo are news presentation, sports-cricket related information etc.

We can see in detail how various sites calculate privilege level based on user's social interaction. Google.com is one of the popular search engines used globally. It offers Gmail email service, Youtube video service, Orkut social networking service etc. Orkut and Gmail service uses same account verification in Google. Notable features taken into account for the formulation of privilege level are linked email accounts, number of valid email accounts in the contact list, frequency of emails sent or received per week, number of friends in the friends list of Orkut service and chat service etc. So privilege level is estimated by properly taking into consideration of the above features. Facebook can use features like number of friends in the friends-list or number of neighbors in any of the social networking game, number of people tagged on the user's picture etc. In Twitter, most notable features are number of people following the user, number of people followed by this user, number of friends etc. All these websites can integrate their service in providing privilege level of users by authenticating the accounts. As such, a Facebook user not having a Google account can login to Facebook from Google itself and get his/her privilege level.

But there arise another concern. Privilege level calculated from these websites differs. We are using a range for privilege level from 0 to 10. Level-0 means the user have no valid account or the account was newly created. Highest level-10 indicates the user is having high privilege level. But in order to make the range in more general format, 3-level range can be employed-Low, Medium and High. Low level range includes privilege levels 1 and 2, medium level range includes privilege levels 3, 4, 5 and 6 and finally privilege levels 7, 8, 9 and 10 included in high level. So depending upon different levels, separate privilege channel can be allocated. We will be using 2 bits for representing the privilege level, and the privilege level is meaningful only if the target or searched site is registered with the source site. If the target is not registered with the source site, it is denoted as 00. Then low, medium and high privilege level is represented as 01, 10 and 11 respectively.

But even after generalizing the privilege levels, again their do exist some vital information ie; the social behaviour within the target website to which the user may be willing to get privilege service. Users not, at all times may be having accounts in the target website, in that case above discussions are meant to provide such users privilege service from source search or social networking website to the target website. But if the user is indeed a valid account holder of the target site, his/her privilege level from target server should also be taken into consideration.

4.1 Account verification of target website and getting the privilege

This is a more reliable method for obtaining privilege level for the clients for establishing the privilege channel. Even if the privilege level offered by the source site is low, he/she may be a valuable customer for sites like eBay.com, Paypal.com etc as they may have been using some value added service in those sites. Hence before establishing privilege channel, he/she should be given the option for login to the target site and getting the privilege level. This method can be improved by offering privilege level transfer option from target website. After making payment within a e-Commerce or e-Shopping site, the site can offer privilege points or quota points which can be transferred to another site's account of the user (which offers privilege channel service).

4.2 Quota settings

Using PRS, a normal user can establish connection with the target server. Now target server can provide a limit for the number of times the privilege channel can be established by the respective user. Quota or limit for privilege channel depends upon his/her current privilege level at target server. Valuable customers will be having higher privilege levels and hence higher chance of obtaining privilege channels. After completing purchases or any value-added transactions from target servers, target server will offer privilege points which can be assigned to any of client's social networking site account. Target site prompts the user to authenticate any social networking site which is registered with them, and then transfer the privilege points to that account. Using these privilege points the quota in their respective source servers will be increased accordingly. For this to happen, target server should be linked with almost every social networking site and other popular websites which offers privilege service.

So less important websites which are prone to DDoS attacks can employ this method for providing their users uninterrupted 24x7 service. For this, these sites need to register with the source servers offering privilege service on contract basis similar to Google ad-click service. The sole purpose of this method is to provide value added service to sites, depending on number of clicks made from source server to target server.

Once privilege level is calculated, along with the source IP of client, it's been sent with the request packet from source server to target server. Third party server now evaluates the validity of source server with the valid list of referrers. The request packet contains encrypted unique identification number provided by destination server. Third party server decrypts the encrypted UID for authenticating the request, if valid, request is forwarded to target server. The destination server now inputs the source IP obtained through the request at privileged port into the allowed client's list of firewall. Only after this step, the valid client is said to be privileged. Acknowledgement from target server is given to source server. Upon reception of acknowledgement from target server, source server gives the encrypted UID and URL of third party server. Now client's browser gets automatically redirected to the destination server after validation at third party server. The valid client's channel bandwidth is in between normal channel and normal privileged channel.

5. PROPOSED ALGORITHM

5.1 Registration (Figure 3)

Source servers visits target server and register for referral service. For each source server a unique identifier (UID) and source identifier (SID) will be generated at target server after

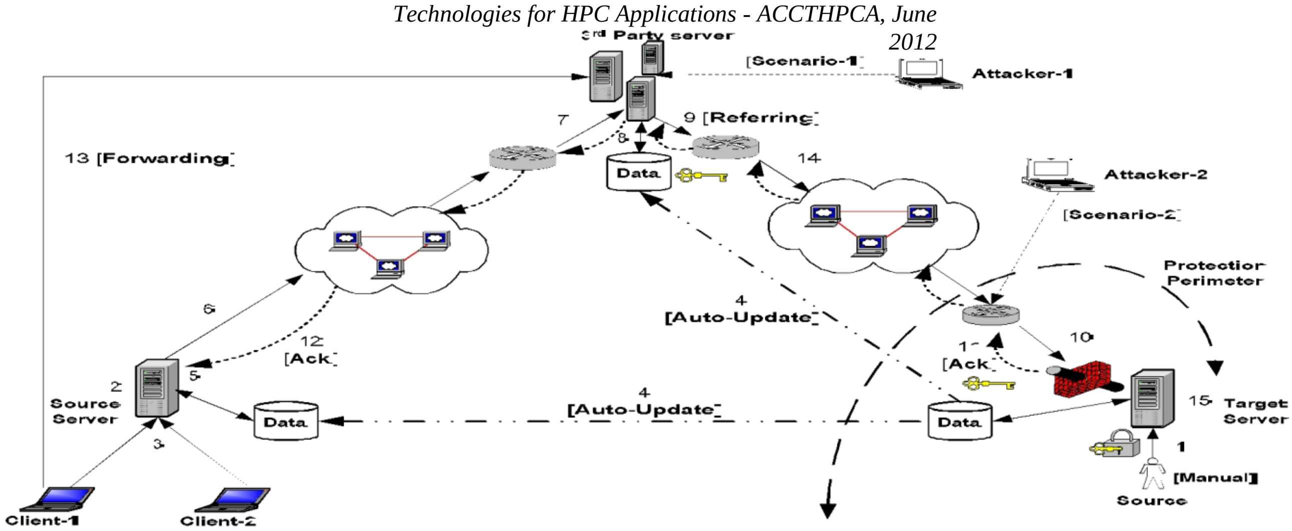

Figure 3. Overall enhanced referral service architecture

registration. Source server will get the URL of third party server along with parameters like encrypted UID, SID and TID.

5.2 Enabling referral service

For enabling referral service between source and target server respective databases should be updated automatically. Privilege level calculator should also be enabled in the respective source servers.

5.3 Auto-periodic database update

The encrypted UID and shared key are periodically updated from target server's database to source and third party database respectively. The key used for encrypting UID for respective SID will be updated periodically between third party and target server. Hence even if compromised referrer or clients crack the current key, it causes no big trouble to the target server‘s traffic as the current key will be updated periodically. Third party server can be varied according to the target server's convenience.

5.4 Target redirection

After authentication of client at source server referral service will redirect the client's browser to target website.

Steps:

- *Step1*: Source servers manually visit target site and register for privilege service. Target server offer URL of third party server along with encrypted unique ID Enc[UID], SID and TID, where SID denotes unique source identifier and TID, unique target identifier.
- *Step2*: Source updates the code for link towards target server with the newly obtained URL-r.
- *Step3*: Registered clients get authenticated at source server.
- *Step4*: The private key shared between third party and target server will be automatically updated. Simultaneously automatic updation is performed for Enc[UID] between source and target server.
- *Step5*: Client clicks for referral link.
- *Step6*: Request for target site is send to third party server along with client-IP, SID, TID, Enc[UID] and 2 bit privilege level.
- *Step7*: If SID is valid, third party fetches Enc[UID] and TID.
- *Step8*: Third party server decrypts Enc[UID] with the current key being shared with target server and checks whether UID is correct.
- *Step9*: Third party sends a request along with client IP, to target server.
- *Step10*: Client IP is put into the database of target server.
- *Step11,12*: Acknowledgement been given to both third party and source server.
- *Step13,14*: Now client will be automatically redirected to target server.
- *Step15*: Target server checks whether client's IP is in its database. Thus valid clients are connected to target website using the privilege referral service.

Discussion

Our proposed technique uses 2 bits for finding out the importance of clients been referred to destination. Previous related papers like Dos limiting network architecture [14], preventing Internet denial-of-service with capabilities [15], path identification mechanism to defend against DDoS attacks [16], etc. uses either destination controlled protocol or uses both router-based and destination-based protocols. But none of the previous methods take into consideration the importance of source servers. Even though source servers previously are not employing any referral service, they should play an active role in referral mechanisms. This makes sure that some overhead in handling referral service is distributed between destination and source servers.

The encryption process at destination server and decryption process at third party are highly flexible, but all that matters is the *periodic update time*, P_t. P_t should be proportional to the best-case cracking-time of the particular encryption-decryption algorithm chosen. Cracking time for a particular encryption algorithm depends upon the probability of predicting the right decryption key for a message authentication code of w bits. So our proposed methodology is flexible enough, so that any encryption-decryption algorithm can be used at target and third party servers respectively.

At the third party server, the privilege bits are utilized for scheduling requests, specifically using priority queuing. Requests with high privilege level should be handled first and low privilege requests are handled later.

The source server communicating with third party server need Enc[UID], SID, TID and client-IP as parameters in request. Also referred clients are enforced by quota settings at source servers. So even if attacker tries out IP spoofing it won't work as Enc[UID] will be updated periodically. Source servers will not try to send numerous requests for congesting the link to third party by compromising their service, because they can be easily tracebacked using SID information. Some of the existing traceback mechanisms are [17], [18], [19] etc.

6. IMPLEMENTATION

The implementation code is done using Java as a Web Application. Apache servers are used for setting up the target, source and third party websites. For encryption and decryption, RSA algorithm is utilized. Encryption key is generated at target site and the key is shared automatically with third party site. Encryption process is performed at target site and the decryption process is performed at third party site. Source server's administrator manually visits target web site and register for referral service. Source site will get an Sid, Tid, Enc[Uid] and URL-r from Target website, where Sid is source id, Tid is target id, Uid is unique id generated for Sid, URL-r is URL of third party server. Source server updates its code of hyperlink [referring] with URL-r. Clients register in source website in usual manner. If necessary quota check can be performed by the respective source servers. Target server updates databases of source and third party server automatically, i.e. the values of new private keys are updated in third party and encrypted [UID] in source server.

6.1 Databases used in the implementation:

Target-sec-info:

Sid	*Tid*	*Prv-Key*	*Mod*	*Uid*	*Enc[uid]*	*URL-r*

Source-sec-info:

Sid	*Tid*	*Enc[uid]*	*URL-r*

Third-sec-info:

Sid	*Tid*	*Prv-Key*	*Mod*	*Uid*	*URL*

When client click the referral link, *URL-r*, obtained during the registration with target server, request for target web server's page is given to third party server. Client request contains Cip, Sid, Tid, and Enc [Uid], where Cip is client IP address. Third party server accepts the request and fetch Sid, Tid and Enc[Uid] from request and validates the data with database third-sec-info. If valid, third party forwards the request to target server and Cip is put into target database. Target acknowledges the request from third party and third party in turn acknowledges the source server. Client's browser is redirected to target server on getting the URL of third party server, URL-r. is. Target server checks for client IP, Cip, in its database. In this way valid client gets the web page of target website.

Both the target server and third party server shares keys generated for source servers. Encrypted unique-id [Uid] of each source site will be given to respective source servers. Third party decrypts the enc[Uid] that comes along with request and check whether key and Tid are correct, for the respective Sid.

6.2 MAC-ID Verification

Clients can login to their source server accounts from different computers. So to prevent clients from making multiple login attempts simultaneously, their MAC-ID can be evaluated either at target server or at source server itself before providing the service. If client seems to be compromised, his quota can be reduced or his IP address can be blacklisted. But the latter method is of no real use if user is accessing his account from dynamically changing IP environment.

7. RESULTS

In the proposed paper we have studied 2 web-tree hierarchies one belonging to .Edu and another belonging to .Gov. We are on the assumption that PRS method is employed in each of the source servers. So whenever a particular site in this hierarchy is under DDoS attack, an alternative path to destination server can be employed using proposed methodology. Both test hierarchy we mentioned, need only one internal third party server each, since they trust each other. But in normal World Wide Web we have to consider a third party which is trusted by both source and destination servers.

From web referral hierarchy shown below (fig.4) (test domains selected were .Gov and .Edu) it is understood that the referral service using the proposed system will be required only at the top 2 or top 3 levels and lower levels can be managed by level 2 or level 3 domains. Fig.5 illustrates that top 40 % of domains can be handled with the referral service itself and the rest 60% lower domains can be handled by level 2 or level 3 domains. The lower domains will be under the direct supervision of level 3 domain in .Edu hierarchy and in .Gov hierarchy, lower domains are controlled by level 2 domain. Proposed referral service can be implemented in all levels of the hierarchy in order to provide an alternative linking service between important websites, even when respective servers are under DDoS attacks.

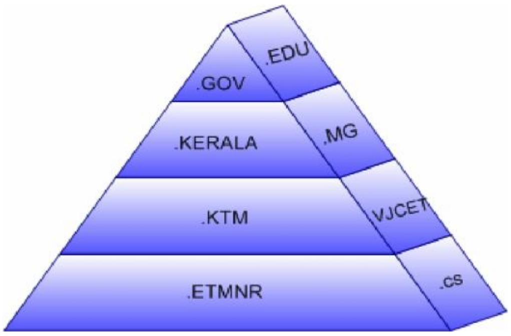

Figure 4. Web referral hierarchy

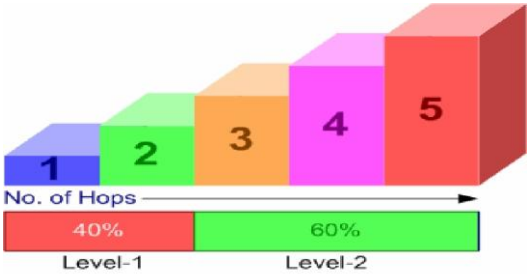

Figure 5. No. of hops required for different levels