RESEARCH ARTICLE OPEN ACCESS

Security issues in mobile banking using cloud based services

*Mr. P. Gurava Reddy, **Dr. M. Ashok
Assoc. Professor, Dept. of CSE,CMREC., Principal, SSJEC, hyd.
E-Mail: gurvap@gmail.com, Email: maram_ashokssjec@yahoo.com

Abstract:
with the rapid growth of mobile users and they are converting to use mobile phones for banking applications instead of using personnel computers. Mean while mobile computing is changing the landscaper of mobile banking application as the future of the mobile. However mobile cloud computing still facing the security issues, this paper address the security issues of mobile banking cloud which relates to the banking application with the help of secure browser search engine. Security has become a major issue for mobile devices when users browsing malicious sites. It is necessary to migrate banking application to cloud based service to overcome the limitations of internet banking. The system uses mobile cloud-based virtual computing and provides each user a Virtual Machine as a security proxy where all Web transactions are redirected through it. Within the VM, the SSE uses crawling technology with checking services to validate addresses and certificates. A Phishing Filter is used to check URLs with an optimized execution time.

Keywords: Mobile Cloud computing, Security, Web.

INTRODUCTION

Mobile banking helped to give any time accessing of bank to their customers due to this customers can check out their account details, get their bank statements , money transactions and more services with more comfort. However the biggest limitation of internet banking is the requirement of a PC with an internet connection. Using mobile devices, the web-based communications have become more targets for attackers of end-to-end communications, e.g., using Man-in-the-Middle attacks and deploys malicious phishing sites to confuse Internet users to ex-pose their private information. Cryptography enhanced Internet protocols have been widely used to prevent Internet users from being attacked. However, strong cryptography algorithms cannot prevent security protocol designers from looking the weakness of human beings in the types of security protocols. SSL supported browsing is an example of this kind. In this paper, our research focuses on two major security problems caused due to human errors: e.g. MITM attack and web based phi-shing attack, which require users to be involved to make decisions on accepting or rejecting a web site.

In SSL-Strip attack, attackers explore the vulnerability that a user may request a web site by initiating an insecure HTTP request. The attacker can intercept the request through spoofing [5] or poisoning [6] attacks and then confuse the user to send the request. Once received the request, the secure web server sends an HTTP message to ask the user to initiate an SSL session. The attacker then intercepts the redirect message and initiates an SSL session to the web server without sending the redirect message to the user. After setting up an SSL connection to the server, the attacker sends unencrypted web page to the user. It is quite similar for users overlooking the protocol name, which could be changed from HTTP to HTTPS, and a lock logo will be appear in the bottom of the web browser. This problem becomes severe when lightweight mobile devices are used. If the user edits his username and password in the web page, which is required by most financial sites for authentication of the user, the username and password will be transmitted to the attacker.

Phishing is another way to expose the human weakness by using fake sites. Similar to SSL-attack, Phishing-attacks also present the exact same web page content and page layout of users, except the web address is different and the lock logo does not appear on browser’s status bar. To address phishing attacks, many existing browsers, e.g., Firefox, incorporate anti phishing filters by checking web site repositories, and then give alerts to users if it happen to visit a phishing web site. Based on our testing, the false negative rate is very high this is due to several reasons. First, as cost of hosting sites has become less and there are tools like dyndns.org, which could map the dynamic changes of IP with a domain name attackers can easily change their domain name and corresponding IP. In addition, most of phishing site repositories require users to send reports to them for phishing changes, which introduce delay and makes the information in repositories quickly. More severely, many phishing-sites may not be detected previously, and thus cannot be detect by web browser's Phishing Filter.

The rest of this paper is organized as follows. Section II describes related works. Section III describes the detailed designs of the system. Finally, section IV concludes and describes future work.

RELATED WORK

In [10], authors given solutions for countering a web-based MITM attacks by introducing context of certificate verification and specific password warning aware type of browsers. This technique validates a certificate and checks if a password or address is sent in an unsecured way. In[11]. Jackson et al introduced Force HTTPS, which forces the web browser to open a secure connection to the destination. If the destination does not support an SSL connection, then the user needs to set a policy in Force HTTPs. This approach does not prevent MITM type attacks since attackers can insert the HTTPS request and return a "no-HTTPS-support" message and force the browser to initiate HTTPS sessions.

Researchers in [12] developed an anti phishing tool for web browsers. However, studies showed in [13], around 23% of the people do not see at the address bar, status bar, and security indicator when they are browsing the web sites, and let alone have small screen size when using mobile devices. In [14], the authors differentiated the effectiveness of using different-phishing tools such as Firefox2, IE7, Spoof guard [12], etc. Their results given that all evaluated tools are less effective in finding phishing web sites. Zhang et al, in [15], proposed a Phishing Filter "CANTINA", where they make use of hyperlinks and *t*erm frequency - *i*nverse *d*ocument *f*requency ($tf{-}idf$), here $tf - idf$ is a technique to give less priority to the common occurring words. When a URL is fed into "CANTINA", it first calculates the ($tf{-}idf$)scores for the page, then it calculate the lexical signature using the top-5 ($tf - idf$) , and finally it uses Google Search engine to verify if the web site is in the top *N* results. The drawback with this technique is that "CANTINA" depends on the Google's Crawler. When a new web site is up, it can stay online for approximately 53 hours [16] that means it cannot be crawled by Google search engine immediately.

To address the MITM and phishing issues, a number of personal proxy based security models have been proposed. Tahoma [17] uses a browser Operating System running on top of a client-side Xen managed virtual machine to serve as a local security proxy to scan web applications. Flash proxy [18] proposed the performance and security of Flash object browser on mobile devices. Web-Shield [19], Spy-Proxy [20], Ajax-Scope [21] and Browser-Shield [22] proposed similar proxy-based web security-models here they use a sandbox on the remote proxy to perform and render the web application while detecting the security threats by monitoring application behaviors. These approaches include overheads when switching from one virtual machine to another virtual machine. Moreover, since they share virtual machines among different users, the user's privacy will be an issue.

ARCHITECTURE AND IMPLEMENTATION

This section gives the architecture and devices of the mobile cloud-based SSE system. The terminology is based on [24], which gives the basic components and models to implement an efficient and scalable search engine.

Xen server that provisions VM resource pools. Here The Xen platform provides Xen-APIs, which are used by the web server to provide VM management and configuration functions to the mobile users.

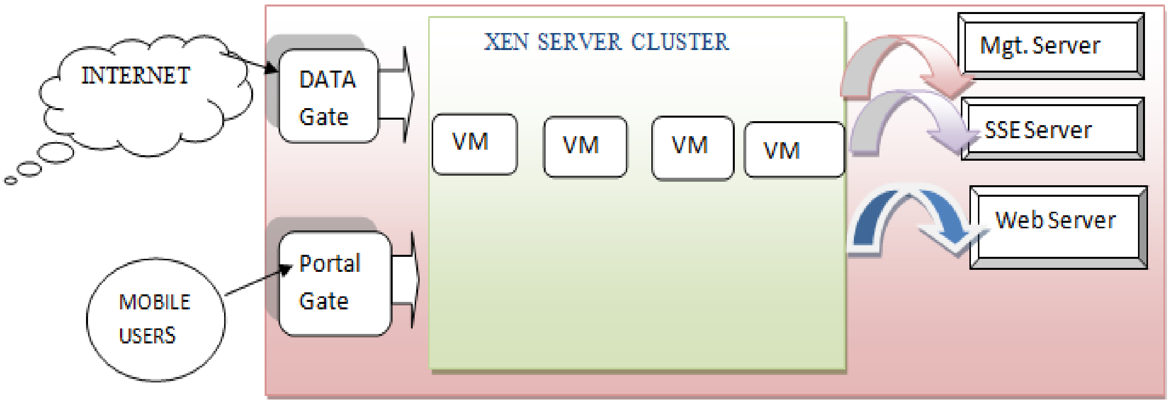


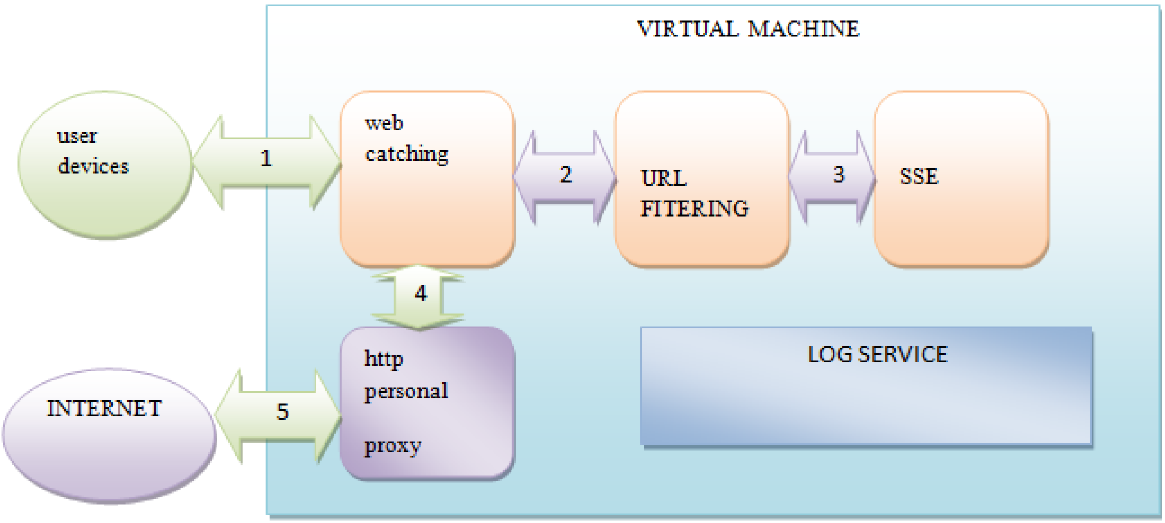
Fig 1: Xen server cluster

• Web Server: The web server contains a website to provide a management portal for users and system administrators. A database in the web server manages their DNS names, IP and VM software configurations. The web server will also work with XEN other servers in the cloud to perform system admin instructions. For instance, it works with DNS/DHCP servers to provide domain names and IP addresses to the newly generated VMs.

• Mobile User VM: Each mobile cloud user has a VM that incorporates many services to provide features like http-proxy, caching and logging. The VM works with the SSE service to detect and correct the MITM and phishing-attacks. Fig. 2 shows the components of a user VM.

Portal Gateway & Portal Network: The Portal Gate-way is the access point for mobile users to access internal VMs and web services. The Portal Network serves as a data exchanging channel between different internal servers.

Fig2: Components of the virtual machine



- SSE Server: It provides the SSE service and the Management Server is in charge of the system resource allocation.

Data Gateway: The networks used by VMs and SSE fetch the web data content from the Internet and send it to the user mobile devices.

A. Secure Search Engine

1) Secure Search Engine Architecture: The SSE is a service it can be used by every mobile user VM to provide web proxy and caching functions, a mobile user VM provides multiple components, as shown in Fig. 2. The implementation of SSE using a layered service architecture, where the higher layer makes use of the service at its immediate lower layer.

• SSE service: SSE service answers all the mobile user queries given by web browsers. Response of the SSE services is made from the SSL verifier and the Phishing-Filter.

• SSL verifier: SSL verifier is one of the major services in SSE. It picks up an URL, collects the certificates from one or more domains which are running on the server. It also verifies the certificate chain and stores the validation results in the repository of the SSE.

• Phishing Filter: Phishing Filter is another service provided by SSE, in which it checks each and every web page linked, Using the learning algorithm explained, It checks only if a web site is a legitimate site or a phishing-site

• SSE Crawler: The SSE Crawler is an auto program that collects security information and web page information of URLs for providing SSL verifier and Phishing-Filter.

Algorithm 1 SSE Processing:

```
1: URL = get the URL();
2: else
3: It sends the message msg = redirect to SSE service (URL) to SSE;
4. If SSE found msg in a phishing site in its database then SSE sends a warning message to the browser;
5:If the user ignores warning then it sends the HTTP request to the web server;
6: else
7: The web browser drops the HTTP request;
8: end if
9: else if SSL Verifier returns “the web server
```

supports HTTPS” AND Phishing Filter returns “the web server is not a phishing site” then
10: SSE sends the certificate information to the browser; The browser sends secure HTTPS Request to the web server;
11: else if SSL verifier returns the web server and phi-sing filter returns the web server is not a phi-sing site then
12: SSE informs the web browser;
13: the browser sends the HTTP Request to the web server;
14: else SSE sends a Warning message to the web browser;
15: the browser goes to step 4
16: end if;

CONCLUSION AND FUTURE WORK

This paper presents a mobile cloud-based secure web referral services to counter based MITM and phishing attacks on the mobile nodes. In the central of the system, SSE serves as the foundation for secure web referral framework and involves minimum interventions of humans for security decisions. SSE Phishing Filter generates low false positives and false negatives. In the future, SSE can be extended to counter other web attacks, such as Cross-site Scripting attacks.

References

[1] B. Hayes, “Cloud computing,” *Common. ACM*, vol. 51, no. 7,2008, pp.9–11.

[2] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach,and T. Berners-Lee, “Hypertext transfer protocol – http/1.1,” 1999.

[3] M.Moxie,“Sslstripsoftware,” http://www.thoughtcrime.org/software/sslstrip, 2009.

[4] A.Freier, P.Karlton, and P.Kocher, “The SSL protocol version 3.0,”1996.

[5] S.Whalen, “An introduction to arp spoofing,” *Node99 [OnlineDocument], April*, 2001.

[6] D.Sax, “DNS spoofing (malicious cache poisoning),” *RL:http://www.sans.org/rr/firewall/DNS spoof.php November*, vol. 12,2000.

[7] Dijiang Huang et. al., “Mobile cloud computing,” http://mobicloud.asu.edu, 2010.

[8] D.Huang, “Mobile Cloud: A Secure Mobile Cloud Computing Platform,”*E-Letter of Multimedia Communications Technical Committee (MMTC), IEEE Communications Society (invited paper)*, 2011.

[9] D. Huang, Z. Zhou, L. Xu, T. Xing, and Y. Zhong, “Secure data processing framework for mobile cloud computing,” in *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, april 2011, pp. 614 –618.

[10] H. Xia and J. Brustoloni, “Hardening web browsers against man-inthe- middle and eavesdropping attacks,” in *Proceedings of the 14th international conference on World Wide Web*. ACM New York, NY, USA, 2005, pp. 489–498.

[11] C. Jackson and A. Barth, “ForceHTTPS: Protecting high-security web sites from network attacks,” 2008.

[12] N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. Mitchell, “Client-side defense against web-based identity theft,” in *Proceedingsof the 11th Annual Network and Distributed System Security Symposium (NDSS04), San Diego*. Citeseer, 2005.

[13] R. Dhamija, J. Tygar, and M. Hearst, “Why phishing works,” in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM New York, NY, USA, 2006, pp. 581–590.

[14] Y. Zhang, S. Egelman, L. Cranor, and J. Hong, “Phinding phish: Evaluating anti-phishing tools,” in *Proceedings of the 14th Annual Network and Distributed System Security Symposium*. Citeseer, 2007.

[15] Y. Zhang, J. I. Hong, and L. F. Cranor, “Cantina: a content-based approach to detecting phishing web sites,” in *Proceedings of the 16th international conference on World Wide Web*. New York, NY, USA: ACM, 2007, pp. 639–648.

[16] G. Aaron and R. Rasmussen, “Anti phishing working group - global phishing survey:,” http://www.antiphishing.org/reports/APWG GlobalPhishingSurvey2H2008.pdf, 2008.

[17] R. Cox, J. Hansen, S. Gribble, and H. Levy, “A safety-oriented platform for web applications,” in *Security and Privacy, 2006 IEEE Symposium on*, may 2006, pp. 15 pp. – 364.

[18] A. Moshchuk, S. D. Gribble, and H. M. Levy, “Flashproxy: transparently enabling rich web content via remote execution,”in *Proceeding of the 6th international conference on Mobile systems, applications, and services*, ser. MobiSys ’08. New York, NY, USA: ACM, 2008, pp. 81–93. [Online]. Available:http://doi.acm.org/10.1145/1378600. 1378611

[19] Z. Li, Y. Tang, Y. Cao, V. Rastogi, Y. Chen, B. Liu, and C. Sbisa, “Webshield: Enabling various web defense techniques without clientside modifications,” in *NDSS*, 2011.

[20] A. Moshchuk, T. Bragin, D. Deville, S. D. Gribble, and H. M. Levy, "Spyproxy: execution-based detection of malicious web content,"in *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*. Berkeley, CA, USA: USENIX Association, 2007, pp. 3:1–3:16. [Online]. Available: http://dl.acm.org/citation.

[21] E. Kiciman and B. Livshits, "Ajaxscope: a platform for remotely monitoring the client-side behavior of web 2.0 applications," *SIGOPS Oper. Syst. Rev.*, vol. 41, October 2007, pp. 17–30.

[22] C. Reis, J. Dunagan, H. J. Wang, O. Dubrovsky, and S. Esmeir, "Browsershield: Vulnerability-driven filtering of dynamic html," *ACM Trans. Web*, vol. 1, September 2007. [Online]. Available: http://doi.acm.org/10.1145/1281480.1281481

[23] Zscaler Inc., "Zscaler cloud services overview," July2011.[Online].Available: http://www.zscaler.com/cloudservicesoverview.html

[25] Xen, "Xen Virtualization Open Source Project." [Online]. Available: http://xen.org

*Gurava reddy pathakota pursuing Ph.D in JNTUH, having more than 7 years of teaching experience in teaching and has guided around 30 UG & 6 PG students, currently working as Asst Prof at CMR of Engineering College, Hyderabad. My research areas include Cloud Computing, computer networks.

*Dr. M. Ashok working as Principal SSJEC, hyd. He has 20 years of Experience in teaching, published 16 Journals at International level, attended 8 national and international conferences, and guiding number of students in their research work, his research areas includes image processing, cloud computing.