PHISHING ATTACK PREDICTION BY SMART MOBILE DEVICES

A.L.Hanees[1], M.S. Shafana[2]
[1]Department of Mathematical Sciences, Faculty of Applied Sciences, South Eastern University of Sri Lanka, [2]Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka
hanees.al@gmail.com, zainashareef@gmail.com

ABSTRACT: In recent times, phishing is a wide spread technique to steal user's authentication information, especially password. The key issue is that it is difficult for user to differentiate fake Login User Interface from normal login. This paper presents a unique method to predict phishing by smart device. In our technique, a smart device pre-stores feature information of Login User Interface. Before entering authentication information, a plug-in of Web browser at host side will verify the validation of Login Inter face according to pre-stored Login Interface information. Wi-Fi provides a communication channel between the plug-in and the smart device. Furthermore, the smart device can automatically fill the field of user id and password to the Login User Interface if Login User Interface passes the verification of smart mobile device. Compared with other solutions, this solution cans greatly improve the security of authentication.

Key words: Phishing, Authentication, Login User Interface

1. INTRODUCTION

Phishing seriously threatenstheconfidential personal informationincurrentInternet [1-4].Newest reportfromAPWG(Anti-PhishingWorkGroup)shows that thereare24,853 reported phishingattacksinMarch,2007[12].Phishing attacksusebothsocial engineering and technicalsubterfuge[2]tosteal consumers'personalidentity dataandfinancialaccount credentials.

Oneofthemost importantfeaturesin phishing attack is that it is difficult for common user to distinguishfake LUIfromnormalLUI.Anotherfeature inphishing attackis thatthereis akey–loggerspy-ware whichrecordsthekeyclicks.Whichthekey-loggercan leakthe passwordofthe usertoattackers.

This paper proposes a novel method to anti-phishing by smart mobiledevice. Here smartmobiledevicereferstosmartphoneorPDA (Personal Digital Assistant).Thesmartmobiledevicecanprovide morepowerfulcomputing capability to manage personalinformation.This paperappliesthecapability tostorethelegalLUIinformation,andverify theLUI information beforethecommonuserorthe plugininputsauthenticationinformation,especially password, intoa website.

Thesmartdevicecanalsoautomatically inputthe authenticationinformationintoUIof authentication module.Thisfunction canresolvethetwoissuesof password management: rememberissueandinputissue. Intheirmemberissue,itisdifficultforcommonuser to rememberacomplexpassword.Becausethesmart devicecanrecordthe password, the commonuserneed not rememberthepassword.Inthe inputissue,itis

difficultforcommonuserto inputacomplexandlong password.Inourmethod, thesmartmobiledevicewill input the password viaWi-Fichannelautomatically.

2. BACKGROUND AND MOTIVATION

2.1PHISHING AND ANTI - PHISHING

Phishingattack is threatening people's confidence to usetheWebtoconductonlinefinance-related activities.Phishing attacksusebothsocialengineering and technical subterfuge [2] to steal consumers' personalidentity dataandfinancialaccountcredentials. Social-engineering schemesuse spoofede-mailstole ad consumers tocounterfeitwebsitesdesignedtotrick recipients intodivulgingfinancialdatasuchascredit card numbers, account usernames, passwords andsocialsecurity numbers.Hijackingbrandnamesof banks,e-retailersandcreditcard companies,phishers oftenconvincerecipientsto respond.Technical subterfugeschemesplantcrime-wareontoPCs to steal credentials directly, oftenusing Trojan key-logger spy-ware.

There are many technical schemes of anti-phishing,amongwhichphishingWeb pages detectionanduserauthenticationarethe mostpopular ways.PhishingWebpagesareforgedWebpagesthat are createdbymaliciouspeopletomimicWebpagesof realWebsites.MostofthesekindsofWebpages have highvisualsimilaritiestodefraudtheirvictims.Some ofthesekindsofWebpageslookexactlylikethe real ones.Unwary Internetusersmay beeasilydeceivedby thiskindof scam.Victimsof phishingWeb pagesmay expose theirbankaccount, password, credit card number,orotherimportantinformationto thephishing Web pageowners[9].Aneffectiveapproachtodetect phishingWebpagesiscalculatingthe visualsimilarity ofWebpages.Authenticationisany processbywhich youverifythatsomeoneis reallywhotheyclaimthey are.Thisusually involvesausername andapassword, but canincludeanyother methodof demonstratingidentity.

2.2 AUTHENTICATION WITH ATTACHED DEVICE

Authenticationwith attacheddeviceisnow oneof themostpopularwaysagainstphishing.The typical applicationof authenticationwithAttachedDevice is RSA SecurID[14].RSA SecurIDhardwaretokens provide "hacker-resistant" two-factor authentication, whichresults ineasy-to-use andeffectiveuser identification.BasedonRSA Security'spatentedtime synchronizationtechnology, thisauthenticationdevice generatesasimple,one-time authenticationcodethat changesevery60seconds [5].

2.3 MOTIVATION

This paperintroduces the application ofsmartmobiledeviceto managepersonalauthentication information,includingUIinformationof authentication moduleandpassword.

Thesolutionproposedinthispaperwillresolve thefollowing issuesinpasswordmanagement:

- **Anti-Phishing**: Phishing seriouslythreatens theauthenticationinformationof commonuser.The proposedsolutionprovidesaplug-inof Web browsertoverify thevalidationofLUI;furthermore,the plug-incan automaticallyfillthe useridandpasswordtoLUI.
- **Anti-Pharming**:Pharmingisalsoaseriousattack to stealuser'spassword. Pharming crime-ware misdirectsusers tofraudulentsitesorproxy servers,typicallythroughDNS hijackingor poisoning. The proposedsolutioncanpre-store the legalpairof (URL-IP),andcancheckthe validationoftheIP whichcanbegottenbyURL before theuserinputthepassword.
- **Password Management**: the proposedsolutioncan record thepersonalpasswordinsmartmobile device, and automatically fill user id and passwordtoLUIiftheplug-inconsiderstheLUI islegal.
- **AutomaticLock**:becausesmartdevice,suchas smartphone, isalways takenwiththe user,the plug-in candetectthestrengthof Wi-Fisignaltojudgewhethertheuseriscontrollinghe host.Oncetheplug-injudgestheuserisleaving thehost,theplug-inwillautomaticallylockthe OS(OperationSystem).

3. SYSTEM ARCHITECTURE

Thissectionintroducesthe architectureofour solution. Figure 1 s h o w s the a r c h i t e c t u r e i n our solution.

There are two mainpartsinthearchitecture: mobiledeviceside and hostsidewhichmay bea notebook, desktop orother server. The host is combined with desktopclientand Web applicationclient.

Mobile deviceside: It includes twomodules: WI – Fi ConnectionManagement (WFCM) and AccountManagement(AM).WFCMis responsiblefor communication withthehostbyWi - Fi.WFCMalso encryptsand decryptsmessagesbetweenmobile deviceand hostso thatthose messageswillbemore secure.AM isresponsibleformanagingaccount.The accountiscomposedwithapairof LUIand authenticationinformation.AMpre-storesthe LUI informationreceivedfromthehostsideand mapsthis informationwiththe username/password.AM provides thefunctionof creating,modifying,deletingand searchingfortheaccount.

Figure1: Brief Description of Architecture

Hostside:It isaplug-inof Web browser.It communicates with mobiledeviceside to realize account registeringandloginsessionmanagement. Before the userlogin,the plug-inwillgatherthe LUI information,andsend itback to mobiledeviceside.If mobiledeviceside authenticatestheLUIinformation accordingtopre-storedLUIinformation,theplug-in willfilltheuseridandpasswordintoLUI.

Host side also has WFCM, whichprovidesthe loginsessionmanagement.TheWFCM ofhostjudges iftheuserofthemobilephone hasleftthehost accordingtothestrengthofWi – Fisignal.Ifthe signalbecomesweak,itmeanstheuserhasleftthehost withthemobilephone,thentheWFCMofhostwill lockthe OSautomatically.Ifthesignalistoneup,after checking thevalidityoftheOS, theplug-in willautomaticallyun-locktheOS.

3.1 ACCOUNT DEFINITION

Accountisoftenconsideredas authentication information, such asa pairofuseridand password, fingerprintorasmartcard. So,itispossiblethat customerinputs his/herauthenticationinformationinto fake LUIwhichlookssimilarwiththerealone.

Inoursolution,wedefineaccountasapairof LUIinformationandauthenticationasfollow:

DEFINITION1: Account=(LUI,Authentication Information)

AnaccountinDEFINITION1 means some authenticationinformationina legalLUI.

We givethedefinitionofLUIasfollows:

DEFINITION2:LUI= (HOST?,URL,IPs, InputArea*, CertHash)

InDEFINITION2,HOSTmeansthe hostwith which usercan input authenticationinformationtologin. The element ofHOSTisoptionalforLUI, becauseconstraintfromHOSTelementwilldecrease theavailabilityofthesolution.Fordetaileddefinition ofHOST,pleaserefertoDEFINITION3.URLrefers tothelegalURL ofLUI;IPsrecordsthepossibleIP addresseswhichURLmapsinDNS.InputArearecords theDOM (DocumentObjectModel)pathofinput widgetssuchasinputfieldof userid;CertHashrecords the Hashcode ofthecertificate inthe LUI.

We givethedefinitionofHOST asfollows:

DEFINITION 3: HOST= (Hostname, OSInfo, NICMAC,DiskID)

InDEFINITION3,Hostname referstothe hostname of the HOST; OSInforefers to the informationofoperatingsysteminstallinginthe HOST. Forexample

OSInfocanbe“MicrosoftWindowsXP Professional2002ServicePack2”;NICMAC refersto theMACaddressofnetworkcard;DiskIDreferstothe informationofthediskofthe HOST.

Finally,becausegeneralLUIisthe mechanismof userid-password,we give thedefinitionof AuthenticationInformation...

DEFINITION4:AuthInfo =((UserID, InputAreaRef), (Password, InputAreaRef));

InDEFINITION4,InputAreaRefrefersto the elementof InputAreainDEFINITION2.(UserID,InputAreaRef)means authenticationinformationof UserIDwillbe filledintheinputwidgetfiguredoutby InputAreaRef.

3.2 SMART AUTHENTICATION

s is shown in figure 2, on the bases of the definitionofAccountinsection3.1,weintroducethe mainworkflowof smartauthenticationforLUI.

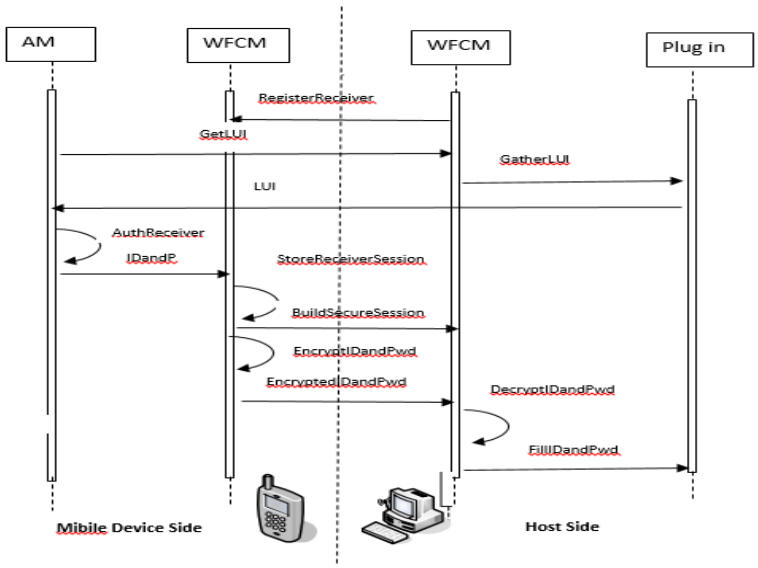

Figure 2: Smart Authentication for LUI

Infigure 2,AM,WFCMof mobiledevicesideand hostside,plug-inhavebeendescribedinsection3.1. The firststepbetweenmobiledevice andhostisbuilda Wi-Ficonnection and WFCM atHost side registersasa legalreceiver.AMwillverifywhetherthe HOSTislegal bythefollowingmethod: AMsends GetLUIrequesttoWFCM, and thenWFCM willredirectthe requesttoPlug–inofthebrowsertogather LUIinformation.Plug-inwillsend LUIinformationto AMrelayedby WFCM(ignoredinfigure2).AM authenticatesthe LUIinformationfromPlug-in accordingtopre-storedLUIinformation.Once theLUI informationpassestheAM’s authentication,AM will send the relevant useridandpasswordtoplug-in. During the

transmission, the data of userida n d password mustbeen encryptedbetweenthe twoendsof WFCM.

Afterlogin,theplug-inwillrecord thevalidlogin, andmaintainthesessionaccordingto thestrengthofWi-Fisignal.

4. PROTOTYPE IMPLEMENTATION

4.1 SYSTEM DESCRIPTION

Wehavesetup aprototypeforoursolution.The mobiledeviceisSamsung J7withWi-Fi.The hostis aDesktopwithCPU (PD2.66G),RAM(1G),OS (Windows XP), Browser(IE 6), BI Wi-FiUSB Dongle(Wi-Fi).Intheabove environment,we implementallfunctionsdescribedinsection3.

4.2 KEY ISSUES DURING IMPLEMENTATION

During the implementation we find the following key issues:

4.2.1ConnectivityofWi - Fi

In our solution, Wi-Fi is a bridge between smart mobile device and host. The requirements of our solution include: (1) Wi-Fi channel must be setup as quickly as possible once the mobile device is near the host ;(2) **Host can sensitively check the strength of Wi-Fi signal to** judge whether the user is leaving host.

According to our test, it takes more time (about several times more) to set up a connection between mobile device and Wi-Fi USB Dongle at the first time. But after the mobile device has recorded this connection, the following connection will be set very quickly.

The reasonable connection distance of Wi-Fi is about15m,but in office environment ,the wall and desktop will affect the valid transmission distance.

4.2.2SecurityofMobileDevice

Mobiledevicewillstore allLUIinformationand relevant authentication information, including multi-seriespasswords. Theplug-inwilltrust LUI accordingto theverificationresultof AMinmobile device. So the securityof mobile deviceisamainfactorofthesecurity ofoursolution.Fortunately,the mobiledeviceisconsideredmoresecure thandesktop. Virusandattackeventsare muchlessthanthosein traditional computingenvironment, suchas desktopwithwindows.

Inoursolution,the LUIinformationand authenticationinformationwillbe encryptedbefore beingstoredintomemory ofmobiledevice.Thisstep can realize the storage security of these LUI informationandauthenticationinformation.

4.2.4OneTimePassword

One Time Password (OTP), especially time-synchronizedtoken,canbeconsideredasoneof thebestsolutionsto anti– theftof password,which includes phishingand pharming. With smartmobile device,wecaneffectivelyimplementanOTP solution. That is, the smart device will create a time-synchronized passwordevery60seconds.

ComparedwiththeRSASecureID,thecostofour solutionislower.

5.SecurityAnalysis

Thissectionanalyzesthesecurityofoursolution by comparisonwiththatofothersolutions.The compared solutionsincludetraditional ID&Passwordwhich meansthecommonuserremembers theID and password,andmanually inputIDandpasswordwhen the usermeetsaLUI;RSASecureIDwhichisafamous solutionof time-synchronized token;and apassword managementsoftware.

The description of every term is as follows: Multi-Passwords means the solution supports multi-series(userid, password);LUIAuthentication meansthe solutioncanauthenticateLUIinformation;

Auto-Loginmeans thesolutionsupportsautomatically loginto the operatingsystem;PasswordRemember refersto thedifficultyof rememberpasswordinthe solution;PasswordInputreferstothedifficulty of inputtingpasswordinthesolution;Costreferstothe costdeployingthesolution.

Basedonthe resultof comparisonintable1,our solutionhas moreadvantagesoverothersolutions. Especially,LUIAuthentication,Anti-Pharming and Auto-Lockare absent inothersolutions.So,we can concludethatoursolutionis moresecurethanother solutions.

Table1. Comparison of solutions of password management

PasswordManagement	OurSolution	Traditional ID&Password	RSASecureID	Password Management Software[14]
Multi-Passwords	Support	Weak	NO	Support
LUIAuthentication	Yes	NO	NO	NO
Anti-Pharming	Yes	NO	NO	NO
Anti-Keylogger	Yes	NO	Weak	Yes
Anti-TrojanHorse	Weak	NO	Weak	NO

Auto-Lock	Yes	NO	NO	NO
Auto-Login	Yes	NO	NO	Yes
PasswordRemember	Easy	Hard	Easy	Easy
PasswordInput	Easy	Normal	Normal	Easy
Cost	Low	Low	High	Low

6. DISCUSSION

As is introduced insection1 and 2, Phishingattacksusebothsocialengineering andtechnical subterfuge.Sotheuser'ssecurity awarenessisan important factor toanti-phishing.Thesolution proposedinthispaperonly providesatechnical mechanismtoanti-phishing,buttrainingcommonuser toincrease his/herawarenessofphishingis also important.

Inoursolution,weassume themobiledeviceand plug-inat hostside aresecure,butthemaliciouscode, such as Trojan Horse, could intrude the host, and by-passtheplug-inorsniffthecommunicationbetween mobile device and host. So, oursolutioncan notentirelyrealizeanti-TrojanHorse.

Therestorationofauthenticationinformationis a bigissueinour solution,becausethemobiledevice couldbe missing.Thoughbackup authentication information is a feasible solution to restore authenticationinformation,

yetitwilldecrease the securityofoursolution,foritwillincrease the attacked pointinoursolution.Thatis,theattackercanexploit thebackupfiletogainauthenticationinformation.

7. CONCLUSION AND FUTURE WORK

This researchintroducesasolutiontoprotect authenticationinformationagainstphishing attack.In comparisonwithothersolutionsof password management,oursolutioncanprovidemore powerful capabilitiestoprotectauthenticationinformation.

Work still to be done is to research the connectivityofWi-Fi. Especially whenthe distanceofvalidtransmissionislongerinnewversion ofWi-Fi,wecouldnotjudgewhetherthe useris leaving thehost accordingtostrengthofWi –Fisignal.Onthe otherhand,protectingthe LUIand authenticationinformationstoredatmobiledevice need tobe deeplystudied.

References

[1] Xia , H. Aand Brustoloni, J. C. Hardening Web BrowsersagainstMan-in-the-Middle and EavesdroppingAttacks,*Proceeding ofthe14th International Conference on World Wide Web*,May10–14,2005 ,Chiba, Japan, 489-498.

[2] APWG.http://www.anti-phishing.org/.

[3]Litan, A.(2004)PhishingAttackVictimsLikelyTargets forIdentity Theft".FT-22-8873,GartnerResearch.

[4] Geer, D.SecurityTechnologies GoPhishing,

IEEE Computer. June 2005, 18-21.

[5] RSASecurID. http://www.rsa.com.

[6] Me,G . and Pirro, D. and Sarrecchia, R.A Mobilebased Approachto StrongAuthenticationonWeb". *Proceedings ofthe International Multi-Conferenceon Computing intheGlobal InformationTechnologyICCGI'06*,

August2006,101-105.

[7] Jakobsson,M and Ratkiewicz, J.(*2006*)Designing ethical phishingexperiments:astudy of(ROT13)rOnl query features.*WWW*,

May 23–26,2006, Edinburgh, Scotland,513-522.

[8] Yahoo.http://mail.yahoo.com/.

[9] Anthony,Y. F. and Liu,W. and Deng,X. Detecting PhishingWeb PageswithVisualSimilarity AssessmentBasedonEarthMover's Distance (EMD)".*IEEETransactions onDependableand SecureComputing*,October2006,Volume3(4),301-311.

[10]Dhamija, Rand Tygar , J. D.The Battle againstPhishing:DynamicSecuritySkins.*Proceedings ofthe2005symposium onUsablePrivacyand SecuritySOUPS'05,*July 2005,Pittsburgh,PA, USA,

[11] Brainard,J.and Juels,A. and Rivest,R.L. and Szydlo,M. and Yung , M .Privacy andauthentication:Fourth-factor Authentication:Somebody youknow". *Proceedingsofthe13th ACM conferenceon Computerandcommunicationssecurity(CCS'06)*, October2006,168-78.

[12]APWG. Phishing Activity [13]http://www.antiphishing.org/reports/apwg_report_march_2007.pdf

[14] http://www.51logon.com/.

[15]MPWG. https://www.trustedcomputinggroup.org/Groups/mobile.

[16]E. Ray, E. and Schultz,E.E. AnEarlyL o o k at Windows VistaSecurity,*Computer Fraud&Security*,2007(1), 4-7.