Anti-Phishing System

Neha Chandrakant Mutha
Assistant Professor
SNJB's KBJ College of Engineering, Chandwad, Maharashtra, India

Abstract— The antiphishing system uses visual characteristics to identify fake and phishing sites and suspicious pages similarity to actual sites registered with the system. In the initial two sequential processes in the Site Watcher system runs on local email servers and monitors emails for keywords and suspicious URLs. The second process then compares the potential phishing pages against actual pages and assesses visual similarities between them in terms of key regions, page layouts, and overall styles. The project is a research on the Internet Utility which is mainly used for detecting the Phishing attacks which is mainly used for monitoring every popup used with another website, monitoring the authentication of every websites and use of image containing an institution's corporate logos and artwork.

Key words: Hypertext Transfer Protocol (HTTP), Transmission control protocol and Internet protocol(TCP/IP), Database(DB), Electronic mail(E-mail), Domain Name Server(DNS), Windows Application Programming Interface(Win API), Internet Information Services server(IIS Server), Security Socket Layer(SSL)

I. Introduction

Phishing is a form of identity theft in which deception is used to trick a user into revealing confidential information with economic value. Similar forms of identity theft, in which worms or viruses install key loggers, are sometimes also referred to as phishing. There are many variations on this scheme. It is possible to phish for other information in addition to user names and passwords, such as credit card numbers, bank account numbers, social security numbers or mothers' maiden names. With HTML email readers, it is also possible to provide a replica of a login page directly in email, eliminating the need to click on a link and activate the user's web browser. In browser-based attacks, it is possible to use JavaScript to take over the address bar or otherwise deceive the user into believing he or she is communicating with a legitimate site. Phishers use a wide variety of technologies, with one common thread. All technologies employed by phishers have the goal of deception. The most common front-line defense against phishing e-mails is the use of anti-phishing/anti-spam filtration technology at the outermost border Mail Transport Agent (MTA) or e-mail server. This is usually done using the same anti-spam software that the ISP already has in place to detect and filter spammed.

A. *How Phishing Take Place*

To best understand the context in which phishing counter measures operate, it is important to understand the information flow in a phishing attack.

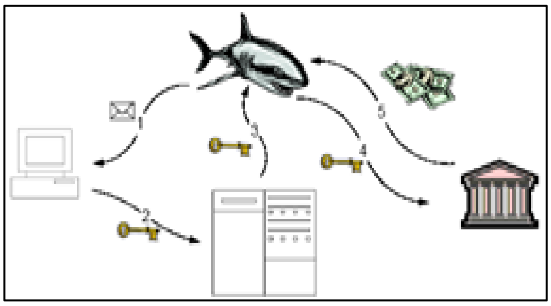


Fig. 1: Information Flow in a Phishing Attack

1) *Flow of Information in a Phishing Attack Is*

1) A deceptive message is sent from the phisher to the user.
2) A user provides confidential information to a phishing server (normally after some interaction with the server).
3) The phisher obtains the confidential information from the server.
4) The confidential information is used to impersonate the user.
5) The phisher obtains illicit monetary gain.

Steps 3 and 5 are of interest primarily to law enforcement personnel to identify and prosecute phishers. The discussion of technology countermeasures will center on ways to disrupt steps 1, 2 and 4, as well as related technologies outside the information flow proper.

2) *Example of Phishing Attack*

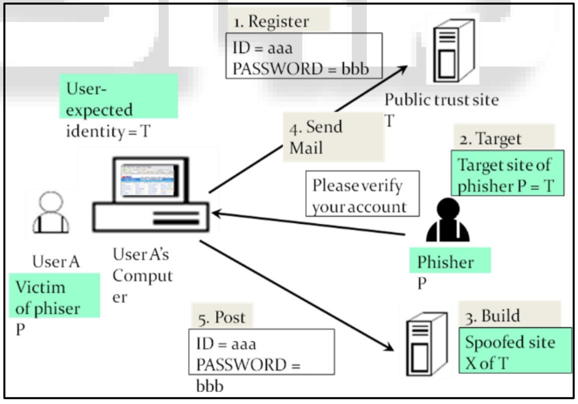


Fig. 2: Example of Phishing Attack

B. *Concept of Anti-Phishing*

Anti-phishing System" is developed with a view to provide an instant, automatic, comprehensive system level solution to perform email protection, webpage authentication and webpage detection against phishing.

The Anti-Phishing concept means to prevent our system before phishing begins. As per describing the above steps which happens for which phisher set the area preventative domain registration may reduce the availability of deceptively named domains. As email authentication technologies become more widespread, email authentication could become a valuable preventive measure by preventing forged or misleading email return addresses. Some services attempt to search the web and identify new phishing sites before they go "live," but phishing sites may not be accessible to search spiders, and do not need to be up for long, as most of the revenues are gained in the earliest period of operation. The average phishing site stays active no more than 54 hours.

C. *Preventing a Phishing Attack Before It Begins*

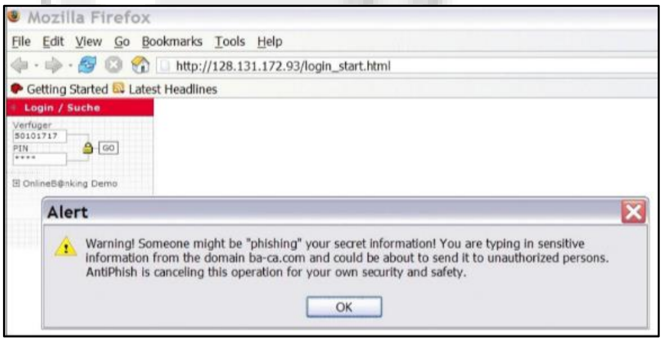
Before steps 1-5 above, a phisher must set up a domain to receive phishing data. Pre-emptive domain registration may reduce the availability of deceptively named domains. Additionally, proposals have been made to institute a "holding period" for new domain registrations during which trademark holders could object to a new registration before it was granted. This might help with the problem of deceptively named domains, but would not address the ability of phishers to impersonate sites.

As email authentication technologies become more widespread, email authentication could become a valuable preventive measure by preventing forged or misleading email return addresses. Some services attempt to search the web and identify new phishing sites before they go "live," but phishing sites may not be accessible to search spiders, and do not need to be up for long, as most of the revenues are gained in the earliest period of operation. The average phishing site stays active no more than 54 hours

D. *Personally Identifiable Information*

The simplest way to reduce the deceptiveness of phishing messages is to include personally identifiable information with all legitimate communications. For example, if every email from bank.com begins with the user's name, and every email from bank.com educates the user about this practice, then an email that does not include a user's name is suspect. While implementing this practice can be complex due to the widespread use of third-party mailing services, it is an effective measure.

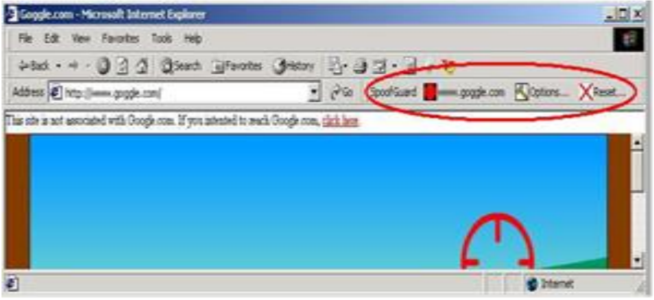
E. *Alerting Message for Phishing Attack*


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://128.131.172.93/login_start.html
Getting Started Latest Headlines
Login / Suche
Verfuger
50101717
PIN
****
GO
OnlineB@nking Demo
Alert
OK

Warning! Someone might be "phishing" your secret information! You are typing in sensitive information from the domain ba-ca.com and could be about to send it to unauthorized persons. AntiPhish is canceling this operation for your own security and safety.

Fig. 3: Alert Message for Phishing Attack

Anti-Phishing Action When the victim inserts his username and password to an entrusted website, an alert is raised before sensitive information are sent to the phisher.


Goggle.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.goggle.com/ Go
SpoofGuard www.goggle.com Options... Reset...
Internet

This site is not associated with Google.com. If you intended to reach Google.com, click here.

Fig. 4: Alerting for Phishing Site

Anti-phishing toolbars generally combine a visual safety indication with outbound data monitoring to attempt to prevent disclosure of confidential information to unauthorized parties, as discussed below. Vendor-specific anti-phishing toolbars are a good preventive measure. Many users use multiple services that could benefit from such protection, and it is not practical to install a separate toolbar for each one. In the long term, it will be necessary to combine knowledge about multiple sites into a single unified toolbar.

F. *Objective of Project*

To detect fake (phishing) sites using following techniques:

- DNS and IP matching
- Cookies detection
- DNS masking
- Logo Recognition

II. LITERATURE SURVEY

In IT companies employee attrition rate is high because of increasing attractions of higher salary and perks. Increasing Attrition rate is a major concern for organization and the Human Resource Managers As a result "Employee Relationship Management" (ERM) is an important job performed by the HR manager. For ERM a HR sends wishes to the employees at different occasions like birthdays, festivals, special days, etc. Sending reminders for important tasks via E-mails, SMS and popup has to be done regularly.

A. *Microsoft Phishing Filter in Windows Internet Explorer 7*

Microsoft Phishing Filter uses a combination of Microsoft's URL Reputation Service (URS) and local heuristics built into the IE 7 browser. These methods allow it to identify and warn users in real time of suspected phish URLs, and block them from accessing confirmed phishing sites that have been reported to the URS by either users or third-party data providers.

B. *Opera*

When Opera Fraud Protection is enabled, a server is contacted at Opera every time you request a Web page. HTTPS sites are checked via an encrypted channel, while IP addresses on the local intranet will never be checked. The server checks the domain name of the requested page against live white lists compiled by Geo Trust, and blacklists compiled by Geo Trust and Phishtank. Opera's fraud protection server downloads blacklists directly from Phishtank, and sends a query to Geo Trust.

C. *Mozilla Firebox*

Phishing Protection is turned on by default in Firefox 2 or later, and works by checking the sites that you browse to against a list of known phishing sites. This list is automatically downloaded and regularly updated within Firefox when the Phishing Protection feature is enabled.

III. Proposed Algorithm

A. Problem Statement

"Anti-phishing System is developed with a view to provide an instant, automatic, comprehensive system level solution to perform webpage detection against phishing"

Objective of project

To detect fake (phishing) sites using following techniques

- DNS and IP matching
- Cookies detection
- DNS masking
- Logo Recognition

Detail Description of Technology Used

Operating System: - Windows 2000/windows XP

Programming Language: - C# .NET 2005

Database: - SQL Server 2005

Web browser: – Internet Explorer

Web Server:-IIS Server

B. Working of System

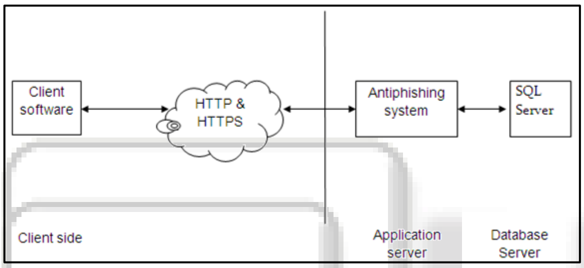


Fig. 5: Working of System

C. Product Features

Anti-phishing System detect fraud web site using DNS and IP match (Certificate DNS masking, Cookies detection, and maintain database for update patches.

Functionality

– *Hook internet explorer running instance*

1) Using System timer to fetch running instance of internet explorer
2) Get webpage URL
3) Get Navigation details
4) Get Documentation details
5) Hook all link from webpage
6) Hook logo image from webpage
7) Hook cookies from webpage

– *Cookies Detection*

1) Get cookies
2) Get webpage URL.
3) Find cookies creation of website
4) If webpage is creating cookies, cookies details show in list box and show page link on top of cookies
5) If webpage is not creating cookies, it show message for fake or phishing website.
6) Delete cookies
7) Select all details of cookies from list box.
8) Delete from list and permanently from temporary internet files.

– DNS and IP matching

1) DNS resolver
2) Get webpage URL
3) Resolved DNS or webpage URL
4) DNS and IP matching with database
5) Get webpage URL
6) Get DNS name and IP address from DNS resolver
7) Match DNS and IP address with Secure site and phishing site database
8) If successfully match with database, then website is secure(Secure DB) or website is phishing (phishing DB)

– Logo Recognition

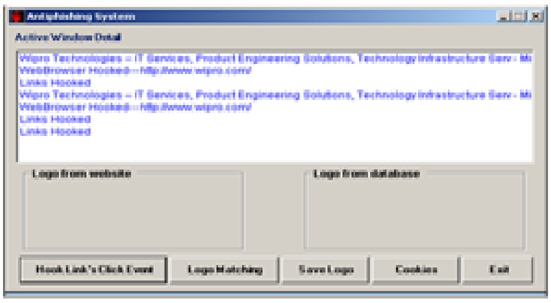
1) Logo grab from web site
2) Get webpage URL
3) Grab website logo
4) Display on Main Form form
5) Match logo with authorized or proper logo of particular website.
6) Retrieve logo image from Database and show on Main_Form form Match website logo with database logo

IV. Modelling Review

In order to access the Internet remotely with a secure connection that is platform- and device-independent, the .NET framework provides an effective and ideal solution by using the concept of web services. The applications of web services provide a safe and secure connection at one end and the process or operation at the other end of the connection. The framework also does not confine itself to computers and makes the whole operation inter compatible across devices. Thus, using the .NET framework in C#.NET, the code for operation programmed on a different server, which can be accessed using the web services protocols using a web interface to remotely access it.

A. Prototype Design

A prototype is expected which basically includes all the major features of the project. It includes the GUI / Front end to be prepared as follows



Wipro Technologies – IT Services, Product Engineering Solutions, Technology Infrastructure Serv - Mi
WebBrowser Hooked---http://www.wipro.com/
Links Hooked
Wipro Technologies – IT Services, Product Engineering Solutions, Technology Infrastructure Serv - Mi
WebBrowser Hooked---http://www.wipro.com/
Links Hooked
Links Hooked

Fig. 6: Hook the Event

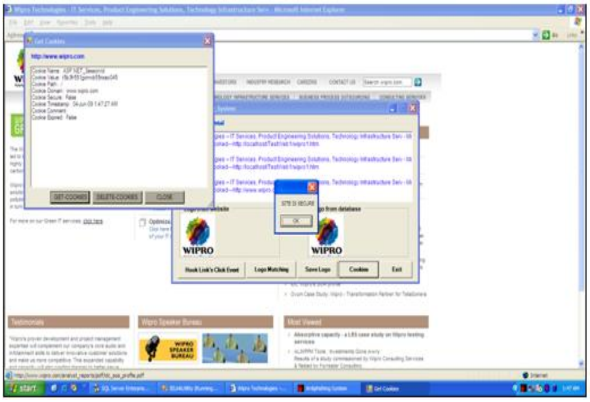
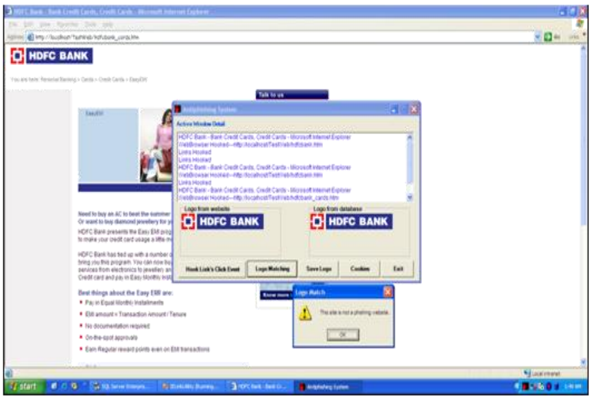


Fig. 7: Logo Matching



AntiphishingSystem

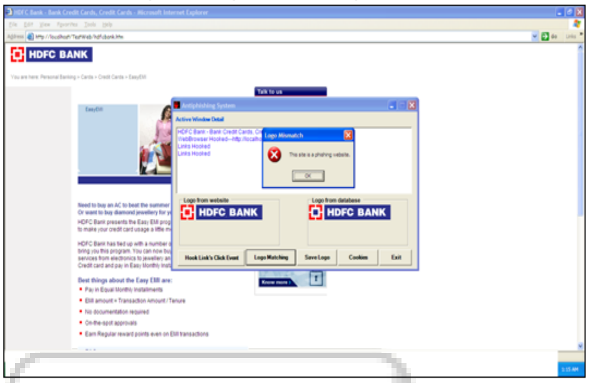
Active Window Detail

HDFC Bank - Bank Credit Cards, Credit Cards - Microsoft Internet Explorer
WebBrowser Hooked---http://localhost/TestWeb/hdfcbank.htm
Links Hooked
Links Hooked
HDFC Bank - Bank Credit Cards, Credit Cards - Microsoft Internet Explorer
WebBrowser Hooked---http://localhost/TestWeb/hdfcbank.htm
Links Hooked
HDFC Bank - Bank Credit Cards, Credit Cards - Microsoft Internet Explorer
WebBrowser Hooked---http://localhost/TestWeb/hdfcbank_cards.htm

Logo Match

The site is not a phishing website.

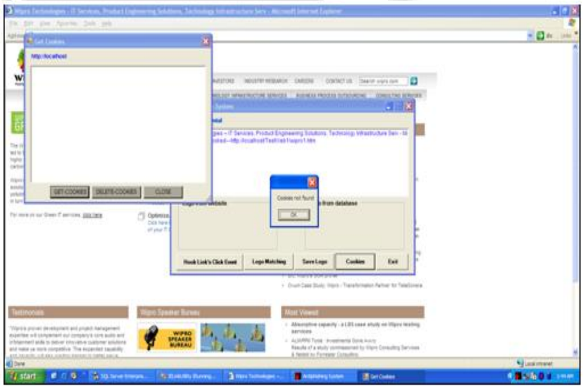
Fig. 8: Logo Matching (Correct)



Logo Mismatch

This site is a phishing website.

Fig. 9: Logo Matching (Incorrect)

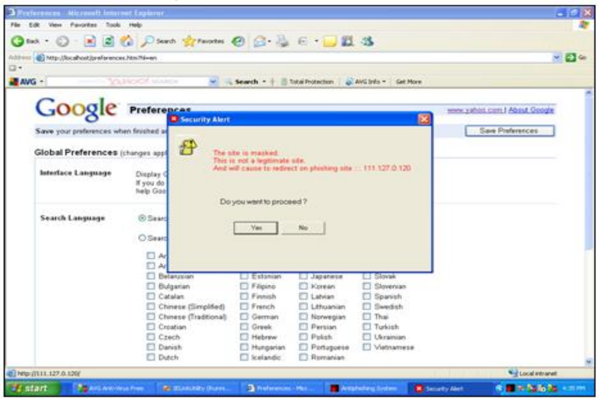


Get Cookies

http://localhost

Cookies not found

Fig. 10: Detection of Cookie



Security Alert

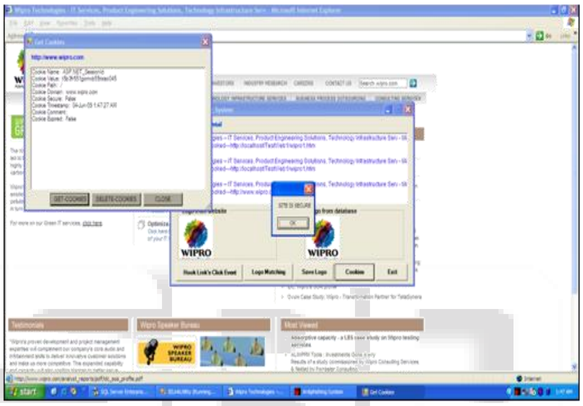
The site is masked.
This is not a legitimate site.
And will cause to redirect on phishing site ::: 111.127.0.120

Do you want to proceed ?

Fig. 11: DNS & IP Matching

V. TEST PLAN

A. *Assumption: Website URL should be in proper format.*



Get Cookies

http://www.wipro.com

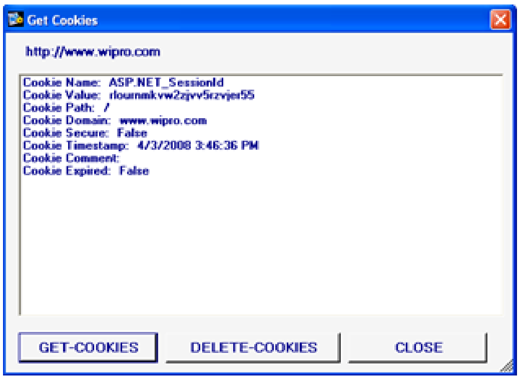
Cookie Name: ASP.NET_SessionId
Cookie Value: r5b3hf051gomsb5feoac045
Cookie Path: /
Cookie Domain: www.wipro.com
Cookie Secure: False
Cookie Timestamp: 04-Jun-09 1:47:27 AM
Cookie Comment:
Cookie Expired: False

SITE IS SECURE

Fig. 12: Logo Matching

Test case No.	Test case Description	Expected Result	Actual Result
1.	Enter proper DNS name or webpage URL>>In internet explorer http://www.wipro.com“	Hook internet explorer running instance hooked to use.	It hook internet explorer running instance hooked to use.
2.	Press on hook link’s click event button>> Hook event of internet explorer	Hook internet web URL link as per click event.	It hook internet web URL link as per click event.
3.	Press Logo matching button (logo images match)	Fetch logo image from website and database as per finding webpage URL and match with each other. And display message “it is not phishing site”.	Fetch logo image from website and database as per finding webpage URL and match with each other. And display message “it is not phishing site”.
4.	Press Logo matching button	Fetch logo image from website and database as per finding webpage URL and match with each other. And display message “it is phishing site”.	Fetch logo image from website and database as per finding webpage URL and match with each other. And display message “it is phishing site”.
5.	press cookies button	It should Show cookies window form	It Shows cookies window form
6.	Press on Exit button	It should Close whole application.	Close whole application.

Table 1: Test Case



http://www.wipro.com

```
Cookie Name:  ASP.NET_SessionId
Cookie Value:  rlournmkvw2zjvv5rzvjer55
Cookie Path:  /
Cookie Domain:  www.wipro.com
Cookie Secure:  False
Cookie Timestamp:  4/3/2008 3:46:36 PM
Cookie Comment:
Cookie Expired:  False
```

Fig. 13: Cookies Detection

Test case No.	Test case Description	Expected Result	Actual Result
1.	For Get cookies (Press get cookies button if webpage is creating cookies)	Show cookies details in list box	It shows the cookies detail in list box
2.	For Getting cookies(Press get cookies button if webpage is not creating cookies)	Did not show cookies details in list box and display message for fake website.	It not show the cookie detail in list box
3.	For deleting cookies(Press Delete-cookies button)	Show confirmation message for deleting cookies. And after delete cookies from temporary internet files.	It shows the message for deleting cookie
4.	For close cookies application (Press Close button)	Close cookies window and come back to main form	Close the window

Table 2: Test Case

VI. Conclusion

This application is successfully proven that it detect phishing website. It provides protection against phishing site, it provides automatic detection of fake site, Web page detection against phishing.

References

[1] Changhua He, John C Mitchell, Analysis of the 802.11i 4-Way Handshake, Electrical Engineering and Computer Science Departments, Stanford University, Pages 43-50, October 2004.

[2] Ronald Tögl, Fixing WEP Robust Security Networks with 802.11i, Pages 4-6,September 2004

[3] Jesse Walker, IEEE 802.11i Standard Improves Wireless LAN Security, Intel Corporation, Pages 3, 2005

[4] Magnus Falk, Final thesis Fast and Secure Roaming in WLAN Performed for Ericsson AB, Linköpings university, Pages 10-11, 2004

[5] Tin-Yu Wu,y, Cheng-Chia Lai and Han-Chieh Chao, Efficient IEEE 802.11 handoff based on a novel geographical fingerprint scheme, Department of Electrical Engineering, National Dong Hwa University, Taiwan, Republic of China, Pages 1 – 4

[6] Héctor Velayos, Gunnar Karlsson, Techniques to reduce the IEEE 802.11b handoff time, Dept. of Microelectronics and Information Technology, KTH, Royal Institute of Technology, Sweden, Page 1

[7] Ping-Jung Huang, Yu-Chee Tseng, A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks, Computer & Communications Research Laboratories, Industrial Technology Research Institute, Taiwan, Pages 1-3

[8] David Murray, Low Latency Handoff in 802.11a Networks, School of Information Technology Murdoch University, 2005, Pages 35-38

[9] Kira Kastell, Ulrike Meyer, Rolf Jakoby, SECURE HANDOVER PROCEDURES, Darmstadt University of Technology, Darmstadt, Germany, Pages 1-2.

[10] Arunesh Mishra Min-ho Shin William A. Arbaugh, Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network, Department of Computer Science, University of Maryland, Pages 1-11

[11] Cheng Lai Low, Peter Bertok, Fast Re-Authentication Protocols for Mobile and Wireless Networks, School of Computer Science & IT, RMIT University, Melbourne, Australia, Page 2, February 2004.

[12] Aruba Wireless Networks, Mobility in an 802.11i Enabled Wireless LAN, Aruba Mobile Edge Company, Pages 2, 2006

[13] Ioanna Samprakou, Christos J. Bouras, Theodore Karoubalis, Improvements on "IP – IAPP": A fast IP handoff protocol for IEEE 802.11 wireless and mobile clients , Springer Science+Business Media, June 2006

[14] Sangho Shin,Andrea G. Forte, Anshuman Singh Rawat, Henning Schulzrinne, Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs, Columbia University, New York University, Pages 2-3, 2004.

[15] Arunesh Mishra, Minho Shin, William Arbaugh, an Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process, Dept of Computer Science, University of Maryland, USA, Pages 1-3, 2004.

[16] Vladimir Brik, Arunesh Mishra, Suman Banerjee, Eliminating handoff latencies in 802.11 WLANs using Multiple Radios: Applications, Experience, and Evaluation, Pages 3, 6, 2005.

[17] Hahnsang Kim, Kang G. Shin, Walid Dabbous, Improving Cross-domain Authentication over Wireless Local Area Networks, IRIA,France, University of Michigan, USA, Pages 1,11

[18] Sangheon Pack and Yanghee Choi, Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model, School of Computer Science & Engineering, Seoul National University, Seoul, Korea, Pages 1,8

[19] Ishwar Ramani and Stefan Savage, SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks, Department of Computer Science & Engineering, University of California, San Diego, Pages1,10.

[20] Jyh-Cheng Chen, Ming-Chia Jiang and Yi-Wen Liu, Wireless LAN Security and IEEE 802.11i, Institute of Communications Engineering, National Tsing Hua University, Pages 2-12, 2004

[21] Jorg Ott, Dirk Kutscher, and Mark Koch, Towards Automated Authentication for Mobile Users in WLAN Hot-Spots, Helsinki University of Technology, Networking Laboratory, Technologiezentrum Informatik (TZI), University Bremen, Page 1

[22] Yair Amir, Claudiu Danilov, Michael Hilsdale, Raluca Mus_aloiu-Elefteri, Nilo Rivera, Fast Handoff for Seamless Wireless Mesh Networks
Johns Hopkins University, Department of Computer Science, Baltimore, Pages 1-2

[1] Nidal Aboudagga and Mohamed Eltoweissy and Jean-Jacques Quisquater, Fast Roaming Authentication in Wireless LANs, Universite Catholique de Louvain, UCL-Crypto group, Belgium and, Bradley Department of Electrical and Computer Engineering, Virginia Tech, USA, Page 1