International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:11, 2013

Survey Based Data Security Evaluation in Pakistan Financial Institutions against Malicious Attacks

Naveed Ghani, Samreen Javed

***Abstract*—**In today's heterogeneous network environment, there is a growing demand for distrust clients to jointly execute secure network to prevent from malicious attacks as the defining task of propagating malicious code is to locate new targets to attack. Residual risk is always there no matter what solutions are implemented or whet so ever security methodology or standards being adapted. Security is the first and crucial phase in the field of Computer Science. The main aim of the Computer Security is gathering of information with secure network. No one need wonder what all that malware is trying to do: It's trying to steal money through data theft, bank transfers, stolen passwords, or swiped identities. From there, with the help of our survey we learn about the importance of white listing, antimalware programs, security patches, log files, honey pots, and more used in banks for financial data protection but there's also a need of implementing the IPV6 tunneling with Crypto data transformation according to the requirements of new technology to prevent the organization from new Malware attacks and crafting of its own messages and sending them to the target. In this paper the writer has given the idea of implementing IPV6 Tunneling Secessions on private data transmission from financial organizations whose secrecy needed to be safeguarded.

***Keywords*—**Network worms, malware infection propagating malicious code, virus, security, VPN.

I. Introduction

As the defining task of propagating malicious code is to locate new targets to attack, viruses search for files in a computer system as to which to attach, whereas worms search for new targets as to which to transmit themselves to. Depending on their method of transmission, malicious code writers have developed different strategies for finding new victims. Worms transmitted via email have had great success propagating themselves because they find their next targets either by raiding a user's email address book or by searching through the user's mailbox. Such addresses are almost certain to be valid, permitting the worm to hijack the user's social web and exploit trust relationships [10], [5].

In most cases, the worm will craft its own message to send to the target, but some will wait for the user to send a message and attach them. Network worms, those that attack network services, must determine their next victim's IP address. Most of the decision makers are unaware of the fact that there is no silver bullet for the security [6], [3], [4].

The aim of this research is to identify defects in security measures taken in different financial institutions of Pakistan, what are the sources of those defects and what are the risks associated with those defects. This Research work also analyzed the malicious attacks effects on customer data and the use of different hardware and software's against this attacks. The updating and the security steps are followed or not. Using work done with the help of survey from different banks and financial institute persons related to IT security in this report, the quality of security against malicious attacks can be improved to a certain extend [3], [4]. Banks wants to protect its information from security breaches. Fortunately, as Info-world's Malware Deep Dive explains, there's a lot one can do to minimize the risk of malware infection in any financial institutions. It starts with educating owner users about today's most common threats and investing in technologies that provide defense and analysis [1].

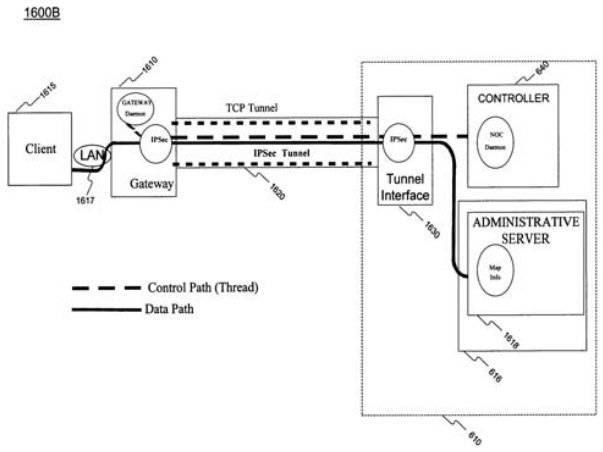

Fig. 1 Systematic diagram of tunneling the traffic (Showing the TCP tunneling and IP Sec tunnel with the control path (thread) and data path between clients is and the administrative server through the gateway).

A. Tunneling Your Traffic

One can fix this problem by creating an encrypted tunnel through which data can send. The web traffic originates from the end user and ends at a known location (the tunnel "endpoint"). From there, the tunnel routes the web requests to the public Internet. Of course, once the traffic is outside the tunnel, it's subject to the usual potential scrutiny from ISPs and law enforcement agencies, but while the data is traveling through the publicly accessed Wi-Fi hotspot, such web surfing is secure [2], [7].

Assistant Professor Naveed Ghani is with the Department of Computer Science, Bahria University, Karachi. Pakistan (e-mail: naveed_ghani@hotmail.com).
Ms. Samreen Javed (e-mail: ms.samreenjaved@gmail.com).

B. How to Set Up a Secure Web Tunnel

If one works on the go fairly often, then it's highly likely that a public wireless network is accessed at least once or twice. It should also be looked into as to how to keep the data safe when one is on such a network, by taking precautions such as using their company's virtual private network if available, or an encrypted web tunnel such as Hotspot Shield [9].

If one does not have a company VPN and don't wish to deal with Hotspot Shield's banner ads, however, one can still secure the wireless traffic without breaking the bank by setting up a self-owned secure web tunnel and gaining a private, encrypted Internet connection free from eavesdroppers [8].

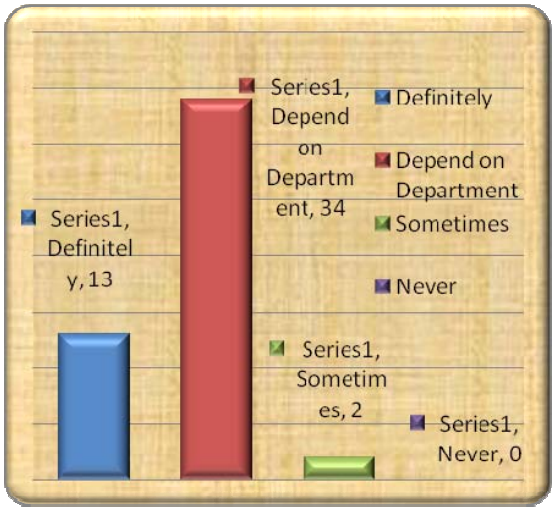

Fig. 2 The graph showing the organization level of handling the urgent backup and recovery in case of malware attack

TABLE I
FREQUENCIES

Statistics

		Security12	Malware
N	Valid	50	50
	Missing	0	0

TABLE II
FREQUENCY TABLE

Security12

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	16	32.0	32.0	32.0
	1.08	14	28.0	28.0	60.0
	1.17	7	14.0	14.0	74.0
	1.25	1	2.0	2.0	76.0
	1.33	2	4.0	4.0	80.0
	1.42	6	12.0	12.0	92.0
	1.67	2	4.0	4.0	96.0
	1.92	2	4.0	4.0	100.0
	Total	50	100.0	100.0	

Q: Can organization handle urgent backup and recovery?

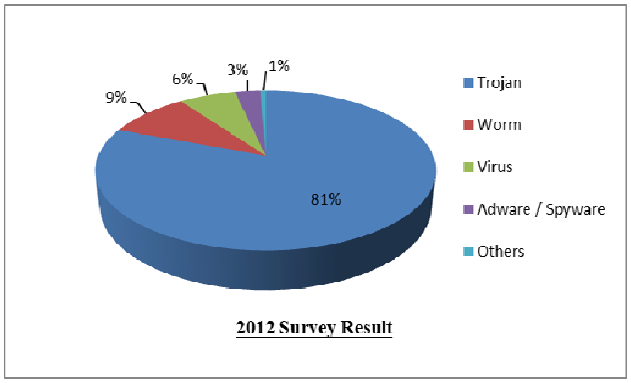

Fig. 3 Result analysis

TABLE III
MALWARE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	24	48.0	48.0	48.0
	1.20	9	18.0	18.0	66.0
	1.40	11	22.0	22.0	88.0
	1.60	4	8.0	8.0	96.0
	2.00	2	4.0	4.0	100.0
	Total	50	100.0	100.0	

Table shows the descriptive statistics of security levels and employees satisfaction at organizational level.

TABLE IV
DESCRIPTIVE STATISTICS

	N	Minimum	Maximum	Mean	Std. Deviation
Security12	50	1.00	1.921.1783		.23023
Malware	50	1.00	2.001.2120		.26002
Valid N (list-wise)	50				

According to respondent's opinions the rating on dependent variable job satisfaction in banking sector was highest with a mean of (3.7820). The rating of work relationship was second highest with a mean of (3.7725), the rating of good working condition was third highest with a mean of (3.6800), the rating of independent variable skills and abilities was fourth highest with a mean of (3.6340), and the rating of work activities was fifth highest with a mean of (3.5533). And the rating of pay and promotion is lowest with a mean of (3.5500).

TABLE V
CORRELATIONS

		Security12	Malware
Security12	Pearson Correlation	1	.935(**)
	Sig. (2-tailed)		.000
	N	50	50
Malware	Pearson Correlation	.935(**)	1
	Sig. (2-tailed)	.000	
	N	50	50

** Correlation is significant at the 0.01 level (2-tailed).

The standard deviation of respondents' opinion on pay and promotion was the highest (0.60503), as compared to other

dimensions. This indicates that there is a low involvement of pay and promotion in banking sector of Karachi.

TABLE VI
REGRESSION

Variables Entered/Removed(b)			
Model	**Variables Entered**	**Variables Removed**	**Method**
1	Security12(a)		.Enter
a All requested variables entered.			
b Dependent Variable: Malware			

The R value show coefficient of correlation is the numerical measure of strength of the linear relationship between two variables. The R value (.505[a]) is show that there is positive correlation between the good working condition and dependent variable job satisfaction.

The R Square show coefficient of determination defines the square of coefficient of correlation. The R Square values (.255) mean 25% reliable to be used for estimation of population.

The Std. Error is important because they reflect how much sampling Fluctuation a statistic will show. The Std. Error value show that 42% Fluctuation of sampling mean.

The R change shown that differences between R-value & Adjusted R square.

TABLE VII
MODEL SUMMARY

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	.935(a)	.874	.872	.09309
a Predictors: (Constant), Security12				

TABLE VIII
ANOVA(B)

Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	**Regression**	2.897	1	2.897	334.251	.000(a)
	Residual	.416	48	.009		
	Total	3.313	49			
a Predictors: (Constant), Security12						
b Dependent Variable: Malware						

TABLE IX
COEFFICIENTS(A)

Model		**Un-standardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	**(Constant)**	-.032	.069		-.467	.642
	Security12	1.056	.058	.935	18.283	.000
a Dependent Variable: Malware						

The std. error is important because they reflect how much sampling fluctuation a statistic will show. The st.d error of a statistic depends on the sample size in the general the larger sample of the st.d error. St.d error of constant (.265) value shows the 26% of fluctuation of sampling mean and the st.d error of independent variable good working condition is (.071) value shows the 7% of fluctuation of sampling mean.

Standardized coefficients are the coefficient that you would obtain if the predictors and the outcomes variable were standardized prior the analysis and the comparing the size of the coefficient across variable. The t value of independent variable good working condition is (5.796). According to the rules if t value is greater that 2 (t>2.5) than null hypothesis will be rejected and alternate hypothesis will be accepted.

Table showing the coefficient of good working condition

TABLE X
COEFFICIENTS

		Un-std. Coeff.		Std. Coeff.		
Model		B	Std. Error	Beta	t	Sig.
1	Constant	2.269	.265		8.575	.00
	Good working condition	.411	.071	.505	5.796	.00
a. Dependent Variable: job satisfaction						

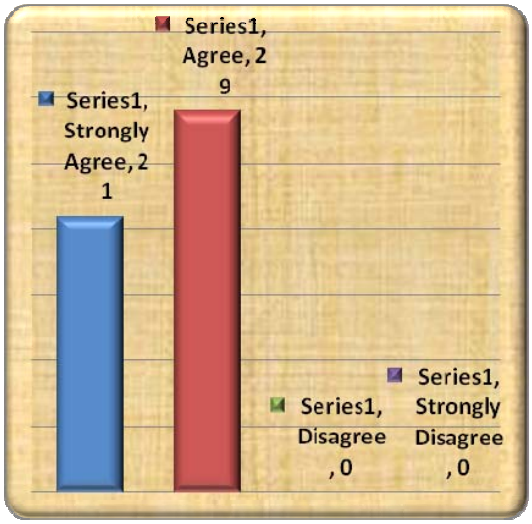

Fig. 4 Graph showing the level of employees agreed for the awareness program done in one organization

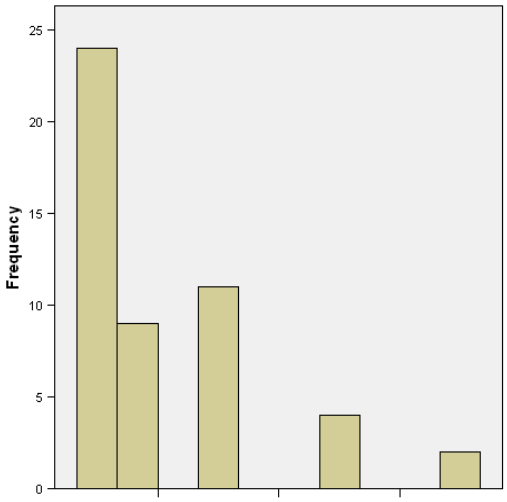

Fig. 5 Graph showing the frequency of different attacks on a single organization

Q: Is there any virus awareness program done in your organization?

II. Survey Questionnaire

A. Objective of Questionnaire:

Research methodology is based on the literature study of experts' articles in the field of computer security against malicious attacks on the financial institutions of Pakistan. The articles are gathered from various reliable sources and banks such as HBL, NBP, and KASB etc. This section describes the method used to gather the material from the different sources and the method used for conducting the survey among experienced professional and their opinion on managing risks in computer security against malicious attacks on financial institutions to save customer data and secure transaction.

B. Design of Questionnaire

The questionnaire was designed after a thorough study of the effective designing of a questionnaire. In brief, the questionnaire that was designed had a consistent flow. General information and questions formed general personal security measures the first section of the questionnaire, while the in depth questions about the topic formed in the second, process logical security measures section. Moreover, apart from the personal opinions of the respondents, the methods used in their respective companies were also collected. Most of the questions were multiple choice type questions.

C. Survey Analysis

In this section, the results gathered from literature review and experimental survey is listed down. Graphs are used for visual representation and easy understanding. Practices that are being followed by different organizations are tabulated and the defects and risks associated with these defects are identified.

D. Analysis of the Results

The results collected from the respondents, were then tabulated. The percentage was then calculated based on various parameters. In order to provide the reader with a visual representation for easy understanding, the tabulated data was plotted in a graph.

III. Conclusion

This research study of will provide significance to the financial institution security against malicious attacks. This survey can be improved by extracting more deep information from the financial institutes. The Benefits driven from this work is all related to the financial institute's security against malicious attacks as they are much common issues of this IT generation. This work will identify the loop holes in the technology used by banks for their IT security and also give recommendation to apply IPV-6 Secure Tunneling System. The research papers use in this thesis to have helped related to the malicious software's and attacks were also selected based on their reputation. Reliable authors from the previous work cited those research papers uses in this work. Goggle Scholar and IEEE site was used for this purpose. References were also gathered by studying the references used in the selected papers. The links are mention at the end of the report. One can fix this problem by creating an encrypted tunnel through which one can send web traffic that originates at one laptop and ends at a known location (the tunnel "endpoint"). From there, the tunnel routes one web requests to the public Internet. After routing the traffic outside the tunnel, its potential scrutiny is subjected from ISPs and law enforcement agencies. While data is traveling through the public-access Wi-Fi hotspot, web surfing is secure, easy and cheap by applying security via SSH.

IV. Future Work

Future research can be done in following:

- Working on the Implementation of Password Connector over IPV6.
- Analyze the existing malware security assures in Password Safe Role Based Access.
- Analyze the existing malware security assures in educational institutes.
- Analyze the existing malware security assures in different international institutes.
- The thesis work can be further extended by using different methods other than questionnaire. Also, the number of respondents can be increased to reduce the margin of error and to increase the quality of the result.

References

[1] Jae-Deok Lim, ETRI, Daejeon, Young-Ho Kim ; Bo-Heung Jung ; Ki-Young Kim, "Implementation of multi-thread based intrusion prevention system for IPv6 ", pp.10.1109/ICCAS.2007.4406938, ISBN:978-89-950038-6-2.

[2] Tahir, H.M., "Implementation of IPv4 Over IPv6 using Dual Stack Transition Mechanism (DSTM) on 6iNet", 10.1109/ICTTA.2006.1684921, INSPEC Accession Number: 9075857, Print ISBN:0-7803-9521-2.

[3] Huajun Huang , Browser-Side Countermeasures for Deceptive Phishing Attack, Print ISBN:978-0-7695-3687-3 ,10.1109/NISS.2009.80,INSPEC AccessionNo:10891791.

[4] Huajun Huang, Junshan Tan, "Countermeasure Techniques for Deceptive Phishing Attack" IEEE Conference, NISS 2009, June 30 2009-July 2 2009.

[5] Dan Boneh,D. Pointcheval, "How to encrypt properly with rsa," Crypto-Bytes, vol. 5, no. 1, pp. 10–19, 2002. http://www.rsa.com/rsalabs/cryptobytes/CryptoBytes_January_2002_final.pdf.

[6] Huajun Huang, Countermeasure Techniques for Deceptive Phishing Attack, doi>10.1109/NISS.2009.80 http://dl.acm.org/citation.cfm?id=1073009 , ISBN:1-59593-178-3, ISBN: 978-0-7695-3687-3.

[7] Douglas Rodrigues, USA ©2011, H. Liu, S. Pallickara, and G. Fox, "Performance of web service security," in Proceedings of 13th Annual Mardi Gras Conference, Baton Rouge, Louisiana, 2005, pp. 1-8. ISBN: 978-1-4503-0784-0.

[8] N. Gruschka, M. Jensen, L.Iacono, and N. Luttenberger, "Server-side streaming processing of ws-security," IEEE Transactions on Services Computing, vol. PP, no. 99, pp. 1–14, 2011.

[9] R. Engelen and W. Zhang, "An overview and evaluation of web services security performance optimizations," in IEEE International Conference on Web Services, 2008. ICWS '08, 2008, pp. 137–144.

[10] Yang-Seo Choi , 10.1109/ICACT.2005.245948, "Web services security (wss)tc," 2006, http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v...