Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 4 Version 1.0 July-1 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Research Analysis of Cyber Security

By Rabea Masood, Qaria Zainab & Mehreen Sarshar
Fatima Jinnah Women University, Pakistan

Abstract- In an age of cyber technology with it fast pacing and ever evolving, securing data in cyber space is a major enigmawhich needs to be resolved.With vulnerabilities everywhere, data security and privacy is always at risk. This specially comes in play when services of third party are used knowingly or unknowingly. Government and business organizations are testing and implementing security and monitoring techniques to stand a better chance in raging war against cyber-crimes. Moreover, the formulation of new methods also poses new limitations of the systems as well as the users like lack of efficiency or complexity which need to be resolved in order to get better results. In this research paper some of those limitations and their solutions are discussed.

Keywords: cybercrime, security, complexity, usage, efficiency.

GJCST-E Classification : C.2.0

Research Analysis of Cyber Security

Rabea Masood [α], Qaria Zainab [σ] & Mehreen Sarshar [ρ]

Abstract- In an ageof cyber technology with it fast pacing and ever evolving, securing data in cyber space is a major enigmawhich needs to be resolved.With vulnerabilities everywhere, data security and privacy is always at risk. This specially comes in play when services of third party are used knowingly or unknowingly. Government and business organizations are testing and implementing security and monitoring techniques to stand a better chance in raging war against cyber-crimes. Moreover, the formulation of new methods also poses new limitations of the systems as well as the users like lack of efficiency or complexity which need to be resolved in order to get better results. In this research paper some of those limitations and their solutions are discussed.

Keywords: cybercrime, security, complexity, usage, efficiency.

I. Introduction

One of the major issues of today's ever updating technology dependent world is the safety of their private data. Whether it is data of the major organizations launching a new product or secret military operation details, the safety and protection of that data is the most important enigma.

In present time, the ratio of cybercrimes is increasing by each day. In a recent list presented by FBI, it is very clear that cybercrimes now are not only limited to small data theft or simple hacks through malware, but their scope is expanding way behind that horizon. Some of the recent cases of FBI (Cyber Crime branch) areRansom-ware, more than 2000 ATM hits at once, Phishing attacks and more crimes of same nature.

Even though research is being done in cyber security field and practices are also being updated but the problem of cyber-crimes is far from being solved. According to recent researches, the main limitation seems to be the approach used. The methods used are not evolving fast enough to combat the problem.

While many approaches have been implemented, there are limitations that arise with their use. Major limitations are complexity for local user, if more than one different security infrastructures used. Some of other known limitations are decrease in usage, etc. In order for these limitations to be efficiency, data collection, need for monitoring of resolved, more work needs to be done especially in field of research. Research needs to be done starting at institution level. For this purpose, usage is also needed to be monitored to study the user habits and patterns.

Another issue that needs attention is validation of software used and methods and standards used to test or validate them. This is the issue that calls out for attention desperately. As with the ever growing trend of third-party applications and new launch of software every day, there is no telling which one is safe and which is not. So to check their validity and to declare them safe or non-safe, old methods are not enough.

New methods should be built based on International Society of Automation (ISA) standards. The importance of organizational level security is also discussed.

Through this work the importance of cyber security in the modern world has been conveyed. It has also been discussed as to which limitations need to be resolved for it to be effective.

II. Related Work

Even though research is being done in cyber security field and practices are also being updated but the problem of cyber-crimes is far from being solved. According to recent researches, the main limitation seems to be the approach used. The methods used are not evolving fast enough to combat the problem.

While many approaches have been implemented, there are limitations that arise with their use. Major limitations are complexity for local user, if more than one different security infrastructures used. Some of other known limitations are decrease in efficiency, data collection, need for monitoring of usage, etc.

In order for these limitations to be resolved, more work needs to be done especially in field of research. Research needs to be done starting at institution level. For this purpose, usage is also needed to be monitored to study the user habits and patterns.

Another issue that needs attention is validation of software used and methods and standards used to test or validate them. This is the issue that calls out for attention desperately. As with the ever growing trend of third-party applications and new launch of software every day, there is no telling which one is safe and which is not. So to check their validity and to declare them safe or non-safe, old methods are not enough.

Author α : Department of Computer Sciences Fatima Jinnah Women University Rawalpindi, Pakistan. e-mail: rabeam@outlook.com

Author σ : Department of Computer Sciences, Fatima Jinnah Women University Rawalpindi, Pakistan. e-mail: qariazainab@gmail.com

Author ρ : Department of Computer Sciences, Fatima Jinnah Women University Rawalpindi, Pakistan. e-mail:msarshar@gmail.com

New methods should be built based on International Society of Automation (ISA) standards.

III. Conclusion

From the above work, the importance of cyber security is emphasized. It is also concludedthat closely monitoring systems and users provide and insight on the attacks and user reaction to them. Also monitored systems are less vulnerable to threats, data theft, phishing, frauds and other cyber-crimes.

Since the validation of software is necessary, so ISA standardized systems should be developed to validate them.

Also one of the major roles should be played by Government. It should take hold of every bit of events that occur in cyber space including formulation of new algorithms and techniques to prevent unauthorized access to any intruder.

In future, work would be done on monitoring techniques, their shortcomings and role play. Also, further research will include methods of secure authorizations.

a) Analysis

While analyzing the data, the first keen thing observed was the possibility of System being noncomplex as well as vulnerability free very narrow. If a system is to be secure to the highest level, user-friendliness or ease of access especially to users with basic knowledge cannot be provided. Also the fault tolerance of currently existing systems is very low, even in the high-end computers. It could only be increased by closely monitoring the capabilities of existing systems in their ability to treat vulnerabilities. The systems with higher level of robustness have more reliability rate.
Some other components related to cyber security are as follows:

b) Security

The most important and most basic requirement of any system is security. In order for any system to qualify as reliable, at least basic level of security need to be provided. With passing time, the need better cyber security seems to be the basic one.

c) Efficiency

Efficiency is to use least possible resources to achieve most functionality. Encryption, antispyware and secure routes etc. are used to achieve this purpose.

d) Ease of use

The user being able to operate even with basic skill is important. With increase in level of security comes the implementation of complex infrastructures, which makes it difficult to keep the system difficulty free for a basic skilled user. Open source development and other such methodologies are being used to achieve this.

e) Robustness

To achieve this at a standard level, iterative techniques and human brain inspired infrastructures are being developed.

f) Case study

Analyses not only at organization level but at much larger level are being conducted. To make comparisons using these studies, surveys and volunteer research are being conducted.

g) Testability

Testing plays extremely important role to check functionality of the systems. The security techniques before massive or global level implementation are tested several times on smaller networks.

h) System availability

The system availability to perform the necessary immunization steps before connecting to networks are to be done.

i) Fault tolerance

User participation in detecting vulnerabilities, phishing attacks and other such threats play an important role in increase of fault tolerance.

j) Monitoring

By closely monitoring the habits of users and keeping a close watch at young user habits can reduce the number of vulnerabilities at immense level.

IV. Acknowledgements

We wish to acknowledge the guidelines and effort provided by designated professors.

References Références Referencias

1. John Malgeri, “Cyber security: a national effort to improve”,Kennesaw State University, IEEE, September 2009.
2. Pal, R. ; Golubchik, L. ; Psounis, K. ; Pan Hui,“Will cyber-insurance improve network security? A market analysis”,INFOCOM, 2014 Proceedings IEEE, 2014.
3. Kowtha, S.; Nolan, L.A.; Daley, R.A.Homeland Security (HST), “Cyber security operations center characterization model and analysis”, IEEE, 2012.
4. Trim, P.R.J., Yang-Im Lee, “A security framework for protecting business, government and society from cyber-attacks”, IEEE, 2010.
5. Feglar, T.; Comput. Sci. Consultant, Prague; Levy, J.K., “Protecting cyber critical infrastructure (CCI): integrating information security risk analysis and environmental vulnerability analysis”, IEEE, 2004.
6. Teixeira, A.Amin, S.; Sandberg, H.; Johansson, K.H.; Sastry, S.S., “Cyber security analysis of state estimators in electric power systems”, Atlanta G.A, December 2010.

7. PengXie,Li, Jason H.; XinmingOu; Peng Liu; Levy, R., “Using Bayesian networks for cyber security analysis”, IEEE, 2010.
8. Alex Malin, “Continuous monitoring and cyber security for high performance computing”, ACM, 2007-2013.
9. Sandhu, R.; Krishnan, R.; White, Gregory B., “Towards Secure Information Sharing models for community Cyber Security”, IEEE, October 2010.
10. Prof Marthie; Zama Dlamini; siphoNgobeni., “Towards a cyber-security aware rural community”, IEEE, 2011.
11. Dr. Peter R.J. Trim; Dr. Yang-Im Lee; “A Security Framework for Protecting Business, Government and Society from Cyber Attacks”, IEEE, 2015.
12. Rayne Reid ;Iohan Van Niekerk; “From Information Security to Cyber Security Cultures Organizations to Societies” ,IEEE, 2014
13. Jan Kallberg ;BhavaniThuraisingham; “Towards Cyber Operations, the New Role of Academic Cyber Security Research and Education”, IEEE, 2012
14. Robert K. Abercrombie; Frederick T. Sheldon; Ali Mili; “Validating Cyber Security Requirements: A Case Study” IEEE, 2014.
15. Ian ELLEFSEN; “The Development of a Cyber Security Policy in Developing Regions and the Impact on Stakeholders”, IEEE, 2013.
16. Anis Ben Aissa; Robert K. Abercrombie; Frederick T. Sheldon ; Ali Milli; “Quantifying Security Threats and Their Impact”, IEEE, 2013.
17. Dennis K. Holstein; Keith Stouffer; “Trust but Verify Critical Infrastructure Cyber Security Solutions”, IEEE, 2010.
18. Sajjan Shiva; Sankardas Roy; DipankarDasgupta; “Game Theory for Cyber Security” IEEE, 2010.
19. Rebecca LeFebvre; “The Human Element in Cyber Security: A Study on Student Motivation to Act”, IEEE, 2012
20. TziporaHalevi; James Lewis;NasirMemon; “A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits”, IEEE,2013

Evaluation parameters	Meanings	Possible value
Security	The proposed technique is able to detect and correct errors	Yes, No
Efficiency	System is efficient in terms of software	Yes, No
Case study	Examples can use to support the methodology	Yes, No
Ease of use	Software is easy to use or learn for the user	Yes, No
Robustness	System is able to correct errors that are not specified	Yes, No
Testability	Proposed design tested or not	Yes, No
Reliability	System is working or not till the time line given	Yes, No
System availability	The time when the application must be available for use	Yes, No
Fault tolerance	The ability to remain partially operational during a failure	Yes, No
Monitoring	To keep under systematic review	Yes, No

S #	Technique	Security	Efficiency	Case study	Ease of use	Robustness	Testability	System availability	Fault tolerance	Monitoring
1	J. Malgeri et al, 2009	Yes	Yes	No	No	No	No	No	No	Yes
2	R. Pal et al, 2014	Yes	No	Yes	No	No	No	No	No	No
3	S. Kowtha et al, 2012	Yes	Yes	No	No	Yes	No	Yes	No	No
4	L. yang et al, 2010	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No

5	T. Feglar	Yes	No	No	Yes	No	No	Yes	No	No
6	H.Sandberget al,2010	Yes	Yes	No	Yes	Yes	No	Yes	No	Yes
7	H. Peng et al 2010	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes
8	M. Alex et al,2013	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
9	R. Sandhu et al, 2010	Yes	Yes	No	No	No	Yes	Yes	No	Yes
10	D. Zama et al,2011	Yes	Yes	N.A	Yes	No	No	Yes	No	Yes
11	T. Peter et al,2010	Yes	Yes	Yes	No	Yes	Yes	N.A	Yes	No
12	R.Rayne et al, 2014	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
13	K .Jan et al, 2012	Yes	N.A	Yes	No	N.A	Yes	N.A	Yes	Yes
14	A. Robert et al, 2011	Yes	No	No	Yes	Yes	Yes	N.A	Yes	Yes
15	E. Ian, 2014	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	N.A
16	S. Robert et al, 2009	Yes	No	Yes	N.A	Yes	Yes	Yes	Yes	No
17	H. Dennis et al ,2010	Yes	N.A	No	No	Yes	Yes	Yes	Yes	Yes
18	D. Dipankaret al, 2010	No	No	Yes	No	No	Yes	No	No	Yes
19	F. Rebecca, 2012	Yes	No	Yes	Yes	No	No	Yes	N.A	Yes
20	L. James et al, 2013	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes