MULTI LEVEL AUTHENTICATION MECHANISM FOR GRID APPLICATION USING ONE-TIME PASSWORD

ARMAGHAN BEHNIA

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

To my beloved family for their endless support and encouragement

ACKNOWLEDGEMENT

I would like to acknowledge my supervisors, Dr. Imran Ghani and Dr. Aboamama for their support, encouragement, guidance..

My lovely parents; thank you for your perpetual encouragement and support. Your unwavering love that have shaped my mind and opened the doors of opportunity leading me to become the person I am today.

I would like to thank my lovely brothers Arash and Nima and all of the individuals who have helped me during my thesis study.

ABSTRACT

Grid applications often involves large amount of data that requires secured resources access and sharing. The multi-institutional nature of a Grid environment introduces challenging security issues, especially with regard to authentication. The goal of this project is to propose an advance authentication mechanism which will furnish users with more secured and also practical environment. Although there are different available mechanisms such as PKI, KX.509, Kerberos, One-Time password and etc., proposing a Multi-level mechanism to provide better security and more reliability still is in demand. However a large number of the existing mechanisms used X.509 certificate, beside all its advantages due to its long period of validity it may compromise through brute force attacks or dictionary attacks. In order to come up with a solution to this vulnerability, this project attempts to propose an advance mechanism by three different levels. Experiments show the structure is flexible and it can improve efficiency and reduce the risk of dictionary attack

ABSTRAK

Aplikasi Grid sering melibatkan jumlah data yang besar yang memerlukan akses terjamin sumber dan perkongsian. Sifat pelbagai institusi persekitaran Grid yang memperkenalkan isu-isu keselamatan yang mencabar, terutama yang berkaitan dengan pengesahan. matlamat projek ini adalah untuk mencadangkan satu mekanisme pengesahan terlebih dahulu yang akan memberikan pengguna dengan persekitaran yang lebih terjamin dan juga praktikal. Walaupun terdapat mekanisme didapati berbeza seperti PKI, KX.509, Kerberos, kata laluan One-Time dan lain-lain, mencadangkan satu mekanisme pelbagai peringkat untuk menyediakan keselamatan yang lebih baik dan kebolehpercayaan lebih masih dalam permintaan. Walau bagaimanapun sebilangan besar mekanisme sedia ada yang digunakan sijil X.509, selain semua kelebihan kerana tempoh yang panjang sah ia mungkin menjejaskan melalui serangan kekerasan atau serangan kamus. Dalam usaha untuk tampil dengan penyelesaian kepada kelemahan ini, projek ini cuba untuk mencadangkan satu mekanisme terlebih dahulu oleh tiga tahap yang berbeza. Eksperimen menunjukkan struktur adalah fleksibel dan ia boleh meningkatkan kecekapan dan mengurangkan risiko serangan kamus.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Advances in computer technology have made this technology part of everyone's daily life. This in turn has created a demand for various applications to run on different machines. While these applications were running over different machines, some of the resources of those machines were not used by the applications. In this case, theory of resource sharing was introduced to the world. By this theory, each machine can share its resources while it is connected through a network with other computers. This is called Grid computing. Network can be varied from a local network to a larger network such as internet. When internet is going to be the backbone of such resource sharing only verified users must have the access to these shared resources. In such a sensitive situation, secured methods and algorithms must guarantee the access to legitimate user while unknown users' access must be restricted. This is the prologue of authentication over Grid networks.

Numbers of methods and algorithms have been proposed since the introduction of Grid computing authentication such as Kerberos, X509, One-time password, Identity Based Encryption (IBE) and etc. some optimizations have been done over these proposed methods and these methods are going to be discussed in next chapter.

1.2 Statement of Research Problem

User authentication has an undeniable role to verify users' access to the shared resource. Secured methods of authentication must guarantee this authentication with great security banning eavesdroppers of accessing verification data. To secure this transmission proposed methods must be improved day by day. This improvement needs precise study to discover better and secured solution. By having a precise look over the existence mechanism, mechanisms like Hybrid to provide more reliability and confidentiality usually present different levels of authentication and by considering the advantages of these mechanisms, X.509 certificate is one of the authentication types that generally used in most of these mechanism.

Beside its advantages custom security implementations that use X.509 certificates may depend on custom extensions that are not widely used or understood. The validity period of an X.509 certificate tends to be much longer than that of other types of security tokens. For example, passwords are normally changed at shorter intervals, such as every 30 days. For this reason, it is critical to be aware of any possible compromise of an X.509 certificate private key, because it will be useful to an attacker for a considerably longer time than the secret key used in other security token types that have a much shorter lifespan. It means mechanisms like Hybrid which has been used X.509 certificate are faced with possibility of a brute force or dictionary attack to guess that could recover the passwords. As we have shown in chapter 5, by testing the Dictionary attack via THC-Hydra logon cracker, the x.509 certificate revealed the weakness and we found the password after completing the fourth round by THC-Hydra. So it is needed to provide a mechanism that besides employing the advantages of x.509 certificate also covering its weakness and vulnerabilities.

1.3 Purpose of Study

By the advent of computer technology, the backbone of computer networks was introduced widely. The same as other technology, computer networks has too many benefits for human society but no one can deny the problems which this technology brought to the humanity. One of these problems was security over networks. Nowadays, security is highlighted as one of the remarked topics over the networks study.

As it has been discussed, Grid computing is known as resource sharing to process massive applications needing vast processing power such as processor and main memory sharing. Whereas these resources are shared over internet, it means that other users can access the inside of the machine. It can be harmful if this access is done arbitrarily and without precision. Network security must depict its great role by managing the safety of the resource access. Providing a safe and reliable mechanism by enhancing the existence mechanism for authenticating the user can be named as one of the greatest purpose of the study done and the report written as follow.

1.4 Objectives of Study

Restriction, verification and permitted access to the users can be named as the reasons for the study. While resources of each machine are shared through internet, just verified users must have the ability to access to these resources. Unverified users may force great overheads to the networks' traffic and machines' shared resources. Furthermore, they can force great risk of damage to those systems because these users may be invaders with the goals of hacking and harming the system. Objectives of this study can be list as below:

- To study and compare existing authentication mechanisms in Grid in order to find out possible limitation and problems.
- To propose and Implement a Multi level authentication mechanism based on hybrid authentication using mod_auth_mysql, OTP and quantum technology to provide a more secure mechanism.
- To evaluate the security and performance of proposed authentication mechanism.

1.5 Scope of the Study

In the present study in order to achieve aforementioned objectives some limits will be taken which can be listed briefly as below:

- This study will only take into account security issues related to authentication mechanism for Grid application.
- The comparative study of previous Grid authentication mechanisms will be deemed.
- This study focuses on hybrid, mod_auth_mysql, One-Time Password mechanisms which support x.509 certificate.
- The implementation has been limited to the third level of proposed mechanism which is combination of X.509, mod_auth_mysql and One-Time Password mechanism.
- The implementation is done on a local grid by using a WampServer, PHP and My SQL.
- Project Security evaluation will be accomplished by THC-Hydra logon cracker which is open source software to modeling the Dictionary attack.
- Project performance evaluation will be accomplished by AnVir task manager and Argus monitor

1.6 Research Question

One of the eldest methods helping the improvement of science was bringing questions up about from any aspect. This method helps to excavate the problems deeply to find the right answer.

The same as other sciences and methods, authentication over Grid computing networks must be questioned too. These questions can be round about the matters that can help to make the issue much stronger. The questions in this report which are going to be discussed can be mentioned as follow:

- What can be the innovation to make existing methods much secure?
- What are the new algorithms/ methods which can change the security of authentication?
- Is there any problem which can be detected in existed algorithms/ methods?

1.7 Significance of the Study

This research is carried out to earn ability of using shared resource over internet to attain much more power in processing. To challenge with the need of Grid environment some of these processing must be on time, reliable and secured.

Currently, variety of the existence authentication mechanism use X.509 certificate as a part of their methods and unfortunately most of them did not provide a methods to cover the X.509 certificate vulnerabilities.

By considering the proposed mechanism of this research, the outcome of this study will serve as the basis for future plans of proposing and improving the grid

authentication mechanisms. Hopefully, the result of proposed mechanism would be more secured, reliable and computationally optimized.

1.8 Thesis Preview

This thesis includes the following chapters.

- Chapter 1 “Introduction” introduces the background knowledge for grid network and authentication, the problem to solve, scope and our research objective and significance of study.
- Chapter 2 “Literature Review” goes through security issues, grid architecture, current Security issues, current existence mechanisms for grid and a comparison between mentioned mechanisms.
- Chapter 3 “Methodology” discusses on the methodology used in this research
- Chapter 4 “System Design” is analyzing and designing the authentication mechanism. The implementation details have been described.
- Chapter 5 “System Test and Evaluation” conducts tests and justify the security and efficacy of mechanism by Dictionary attack and also shows the performance of the proposed model.
- Chapter 6 “Conclusion” presents conclusion for the authentication mechanism, from the perspectives of security goals, performance and Flexibility. Future work is also briefly mentioned.

REFERENCES

Aulds, C. (2002). "Linux apache web server administration (Craig Hunt linux library,)." America **104**: 106.

Barton, T., J. Basney, et al. (2006). Identity federation and attribute-based authorization through the globus toolkit, shibboleth, gridshib, and myproxy.

Bellovin, S. M. and M. Merritt (1990). "Limitations of the Kerberos authentication system." ACM SIGCOMM Computer Communication Review **20**(5): 119-132.

Berman, F., G. Fox, et al. (2003). Grid computing: making the global infrastructure a reality, John Wiley & Sons Inc.

Bonneau, J. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. Security and Privacy (SP), 2012 IEEE Symposium on, IEEE.

Buyya, R. and S. Venugopal (2010). "Market‐Oriented Computing and Global Grids: An Introduction." Market‐Oriented Grid and Utility Computing: 1-27.

Chakrabarti, A. (2007). Grid computing security, Springer Verlag.

Czajkowski, K., D. Ferguson, et al. (2004). From open grid services infrastructure to ws-resource framework: Refactoring & evolution, March.

Dusek, M., O. Haderka, et al. (1998). "Quantum identification system." Arxiv preprint quant-ph/9809024.

Dušek, M., O. Haderka, et al. (1999). "Quantum identification system." Physical Review A **60**(1): 149.

Florêncio, D. and C. Herley (2008). One-time password access to any server without changing the server. Information Security, Springer**:** 401-420.

Foster, I. (2005). "Globus toolkit version 4: Software for service-oriented systems." Network and parallel computing: 2-13.

Foster, I. (2006). "Globus toolkit version 4: Software for service-oriented systems." Journal of Computer Science and Technology **21**(4): 513-520.

Foster, I., C. Kesselman, et al. (1999). A distributed resource management architecture that supports advance reservations and co-allocation, IEEE.

Foster, I., C. Kesselman, et al. (2001). "The anatomy of the grid: Enabling scalable virtual organizations." International journal of high performance computing applications **15**(3): 200-222.

Foster, I., Y. Zhao, et al. (2008). Cloud computing and grid computing 360-degree compared, Ieee.

Gold, S. (2010). "Cracking passwords." Network Security **2010**(8): 4-7.

Grimshaw, A., M. Morgan, et al. (2009). "An open grid services architecture primer." Computer **42**(2): 27-34.

Hallsteinsen, S. and I. Jorstad (2007). Using the mobile phone as a security token for unified authentication. Systems and Networks Communications, 2007. ICSNC 2007. Second International Conference on, IEEE.

http://www.anvir.com/anvir-task-manager.htm.

http://www.argusmonitor.com/en/.

Huang, C.-Y., S.-P. Ma, et al. (2011). "Using one-time passwords to prevent password phishing attacks." Journal of Network and Computer Applications **34**(4): 1292-1301.

Ismail, S. A. and M. A. Ngadi (2011). New security authentication mechanisms in grid computing web environment, IEEE.

Jie, W., J. Arshad, et al. (2011). "A review of grid authentication and authorization technologies and support for federated access control." ACM Computing Surveys (CSUR) **43**(2): 12.

Khurana, H., R. Bobba, et al. (2010). Design principles for power grid cyber-infrastructure authentication protocols, IEEE.

Kunszt, P. Z., S. Maffioletti, et al. (2011). "GridCertLib: Use Shibboleth to Access the Grid from Web Portals." Arxiv preprint arXiv:1101.4116.

Lo, H. K., T. Spiller, et al. (1998). Introduction to quantum computation and information, World Scientific Pub Co Inc.

Lock, R. and I. Sommerville (2002). "Grid Security and its use of X. 509 Certificates." Department of Computer Science Lancaster University. Funded

by EPSRC project studentship associated with the UK EPSRC DIRC project grant GR N **13999**.

Ma, L. and Y. M. Zhang (2009). A kind of hiberarchy status authentication mechanism in information grid, IEEE.

Matsuo, T. (2007). "Proxy re-encryption systems for identity-based encryption." Pairing-Based Cryptography–Pairing 2007: 247-267.

McBride, D. W. (2009). "Building a Better Grid Authentication System with Kerberos."

Min-Jie, W. and P. Wei (2008). "Quantum secure direct communication based on authentication." Chinese Physics Letters **25**: 3860.

Nakada, H., Y. Tanaka, et al. (2003). Ninf‐G: A GridRPC System on the Globus Toolkit, Wiley Online Library.

Nicanfar, H., P. Jokar, et al. (2011). Smart grid authentication and key management for unicast and multicast communications. Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES, IEEE.

Olmedilla, D., O. Rana, et al. (2005). Security and trust issues in semantic grids.

Prodan, R. and T. Fahringer (2007). Grid computing: experiment management, tool integration, and scientific workflows, Springer-Verlag.

Satoh, A., Y. Nakamura, et al. (2012). SSH Dictionary Attack Detection Based on Flow Analysis. Applications and the Internet (SAINT), 2012 IEEE/IPSJ 12th International Symposium on, IEEE.

Scavo, T. and V. Welch (2007). A grid authorization model for science gateways.

Singh, R. K. and A. R. Pais (2009). Secure Web Based Single Sign-On (SSO) Framework Using Identity Based Encryption System, IEEE.

Su-qin, L. and L. Xingsheng (2009). Research and implement of the grid security authentication model, IEEE.

Travostino, F., J. Mambretti, et al. (2006). Grid Networks, Wiley Online Library.

Vaidya, B., S. Lee, et al. (2006). Using one-time password based authentication for wireless IP network. Intelligence and Security Informatics, Springer**:** 739-740.

Wei, D., Y. Lu, et al. (2010). An integrated security system of protecting smart grid against cyber attacks, IEEE.

Wolfgarten, S. (2004). Apache Webserver 2, Pearson Deutschland GmbH.

www.thc.org/thc-hydra.

Zhen-hua, L. and X. Xue-lin (2010). The Research on Authentication Protocol in the Environment of Manufacturing Grid. E-Product E-Service and E-Entertainment (ICEEE), 2010 International Conference on, IEEE.

ZHENG, Y., H.-y. WANG, et al. (2008). "Grid authentication from identity-based cryptography without random oracles." The Journal of China Universities of Posts and Telecommunications **15**(4): 55-59.

Zhou, N., G. Zeng, et al. (2005). "Cross-center quantum identification scheme based on teleportation and entanglement swapping." Optics communications **254**(4): 380-388.

Zhu, Y. C. and X. F. Zhang (2011). "The Research of Authentication Framework Based on PKI and ID-PKI." Applied Mechanics and Materials **63**: 21-24.