A Novel Time based Authentication Technique for Enhancing Grid Computing Security

Avijit Bhowmick
Dr.B.C.Roy Engg. College
Fuljhore, Durgapur
West Bengal, India

Chandan Koner
Dr.B.C.Roy Engg. College
Fuljhore, Durgapur
West Bengal, India

C T Bhunia
National Institute of Technology
Yupia, Papum Pare
Arunachal Pradesh, India

ABSTRACT
Secure data communication is the most vital and crucial concern in Grid computing environment, where data flows across multiple components in different organizational domains that are not under control of the single data proprietor. An appropriate authentication mechanism is the very basic requisite for building a protected Grid environment. In this paper we have analyzed authentication related issues in Grid and proposed a novel Time Variant Authentication technique that will check the authenticity of remote user time to time throughout the accessing of the remote server which enhances Grid security.

Keywords
Grid computing, virtual organisation, security, Time variant key.

1. INTRODUCTION
The conception of Grid states a potent wide area distributed parallel computing architecture with advanced services which is first presented by Ian Foster et al. [1,2,3].The key characteristic of this architecture is virtual organization (VO), where geographically distributed resources like CPU cycles, storage, software etc. are shared and accessed across the multi administrative domains.

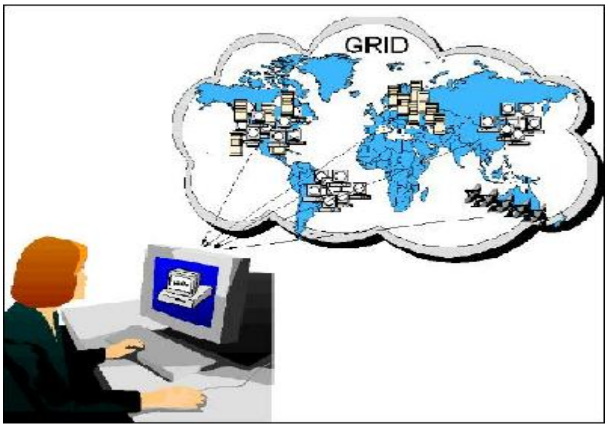

Fig.1: Typical Grid computing environment-User's View [IBM Redbooks paper]

In Grid environment different heterogeneous resources and users are incorporated together without affecting the system. Accordingly, the Grid provides open and standard protocols and application interfaces to build up all the measures for resource sharing [4].Thus the most important feature of the Grid is allowing development of Virtual Organization combining different sites of different administrative domains. Because of this VO concept in Grid, secured data transmission is most vital concern across multiple domains.

The requisite conception behind Grid is: data security, resource administration, data administration and information discovery and controlling [2].Among all other issues data security in Grid computing environment is the most crucial issue.

The five main vital areas of security in Grid:
- Authentication.
- Authorization.
- Confidentiality.
- Integrity.
- Management.

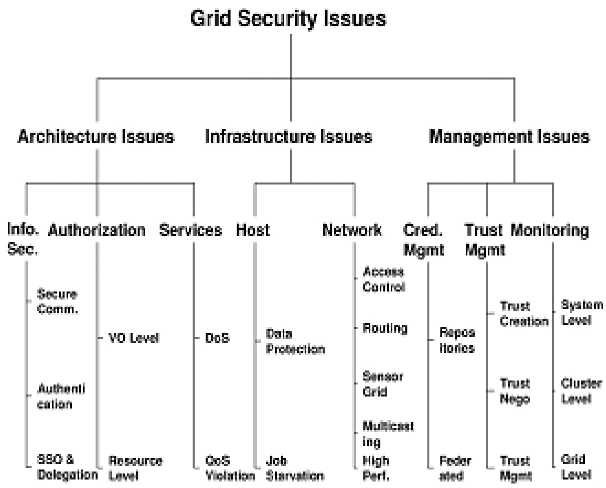

Fig. 2: Security Issues in Grid Computing Environment [17]

Authentication
Sometimes it gets confused between the terms authentication and authorization.

Authentication is to ascertain whether a person is bona fide. Authorization is to decide whether they are allowed to perform some given action. Below are a short list of issues relating to authentication.

Provision for Mutual Authentication
Provision for mutual authentication lies at the heart of the Grid model, as the Grid relies to a certain amount on trust between parties. An authorized person is trusted to exploit a service. An unauthorized person is not trusted to use a service.

You cannot determine authorization until the person in question is authenticated unmistakably as that person and not an impostor.

It is also necessary for a person to determine that a service is the one they are looking for and not an fake posing as that service, before handing over potentially important material. Therefore the requirement for mutual authentication provision is vitally important within any Grid software.

Third Parties

Many Grids make use of third party Certification Authorities (CA's) to facilitate mutual authentication. A CA is used to certify people who apply for certificates for use in mutual authentication. They ensure that a person is bonafide before handing them a certificate. That certificate is signed by the CA to state which CA issued it. Therefore in the mutual authentication process it is a trusted third party that is in result vouching for who a person is. This is a somewhat simplified view of what a CA does, but it suffices to say that it is a very important requirement that the role third parties play.

Use of Proxies

A proxy is a short-term credential used to make use of services without the desire for a user to individually authorize each demand. They are an important component of the mutual authentication process; though they are recognised to have security contravene implications. They are however found to improve the overall usability of systems extensively enough to make it necessary to provide a security provision for them.

Ambiguity

One of the benefits of Virtual Organisations (VO's) is their mobility; the geographical proximity of users is not important. Members of the same VO may communicate via different Grids entirely. This leads to the need for different Grids to inter-communicate; this task is unhurried by ambiguity in Grid software design. Grid security is potentially a major source of ambiguity due to the variety of security models in use by different Grids.

2. RELATED WORK

User authentication has been in treatise for a long time to enhance the security of any system at the access level itself. Different methods such as password based systems and ID based systems have been used. A hash-chain based remote user authentication in which all the passwords are encrypted is given in [6]. In all the initial remote based authentication systems, a verifier table is to be set up in the server side which becomes a problem if the server is compromised. In order to avoid maintaining a verifier table Hwang et al., proposed a non-interactive smart card based scheme without verifier tables [7]. A finger print based remote user authentication scheme was proposed in [8]. This scheme was found to be vulnerable to masquerade attacks and many other attacks [9], [10]. In [11], [12], [13], the biometric data itself is taken as a key for encryption/decryption. The secret data is extracted by using the biometric template as the key.

The biometric data is to be stored in the server side and used for comparison. But for effective Biometric authentication, the procedure is to be done in the client side [14] to avoid any difficulty due to the server being compromised [15]. In [16],the method has been optimized with the identical being done in the server side. But the server does not keep any biometric data in its database thereby protecting the privacy of the user.

The method in [16] provides a three factor authentication which is password – user knows it; smart card- something the user has; biometrics – something unique of the user.

The armed data sharing requirements take into consideration the place in which the user is positioned so as to find the location of any valid/invalid user. So, the susceptible areas of application require security with some amount of privacy preservation. By combining the biometric data with passwords and the location of the user, the security factors are further improved.

3. PROPOSED TIME BASED AUTHENTICATION TECHNIQUE FOR GRID ENVIRONMENT

Time Based Authentication Technique is a group of four different phases, namely, User Enrolment Phase, User Login Phase and User Accessing Phase, Time variant Password Phase.

3.1 User Enrolment Phase

For accessing the Server SR of another domain, firstly the User UR of another domain has to get enrolled SR. User enrolment phase is executed to enrol the UR. This phase is executed only once for one UR. The steps of execution of this phase are given below,

EUE1: The UR chooses his identifier I and password P1 and sends it as an enrolment request to the SR through a private channel.

EUE2: After receiving enrolment request from UR, the SR performs the following operations.

EUE2.1: Computes K = h(P1 XOR I), where h (.) is a one-way hash function and is a bitwise XOR operation.

EUE2.2: Stores the parameters <h (.), K, P1, I, E and D> into smart card CS, where E is encryption key and D is decryption key generated by SR using RSA algorithm in Key generation phase of Data authentication phase.

EUE2.3: Sends the CS to the UR through a private channel

3.2 User Login Phase

User login phase is executed every time when the UR wants to access the SR. UR inserts his CS to a card reader and enters his identifier I' and password P'1.

EUL1: The CS validates the entered I' and P'1 with the stored ones in CS. If they are correct then CS perform the following tasks otherwise rejects the login request.

EUL1.1: Computes B = h (P XOR I) XOR h (Tu), where Tu is the UR login time.

EUL1.2: Computes C = h (K XOR Tu)

EUL1.3: Sends the login request <B, C, Tu> to SR the through a public channel.

EUL2: SR receives the login request and authenticates the UR by the following steps,

EUL2.1: Computes h (P1 XOR I) = B XOR h (Tu)

EUL2.2: Computes C* = h(h (P1 XOR I) XOR Tu)

EUL2.3: Checks whether C = C*. If it holds good, accepts the login request of UR and gives permission to access. Otherwise rejects the login request of UR.

3.3 User accessing Phase

User accessing phase is executed to check authenticity of UR when UR is accessing the SR. This phase is executed at a regular interval during the time of accessing the SR by UR.

Let Ts is timestamp of SR when the UR starts to access the SR and at a ΔT regular interval the SR wants to verify the authenticity of UR.

Now let Ts + (ΔT +………………………) = Ts'

Assume the UR‘s message M which is sent to the SR, is a continuous bit stream. CS divides the M into different blocks of fixed size as the length of P1 in Date sending phase of Data authentication phase. Let the message blocks are M1, M2, M3,………., Mn.

The CS generates modified blocks by the following way,
P2 = P1 XOR M1,
P3 = P2 XOR M2
So, Pn = Pn-1 XOR Mn-1
Thus the password at ith position will be,
Pi = Pi-1 XOR Mi-1
Pi = Pi-2 XOR M i-2 XOR M i-1 and therefore
Pi = P1 XOR M1 XOR M 2 XOR …..........XOR Mi-2 XOR Mi-1
The CS sends Pi blocks simultaneously as message blocks to SR. The CS also uses Pi blocks one by one for every authentication checking execution after every ΔT regular interval.
EUA1: The SR sends <Ts'> as an authentication query to the CS through a public channel after every ΔT regular interval.
EUA2: After receiving the authentication query, the CS asks the UR to enter the I and P1.
EUA3: Then the UR enters his I' and P'1.
EUA4: The CS validates the entered I' and P'1 with the stored ones in CS. If the I and P1 are correct then executes the following steps, otherwise terminates the accessing,
EUA4.1: Computes, B' =h (Pi XOR I) XOR h (Ts')
EUA4.2: Computes, C' = h (K XOR Ts')
EUA4.3: Send (B', C', Ts') as authentication request to the SR through a public channel.
EUA5: After receiving the authentication request, the SR authenticates the UR the following steps,
EUA5.1: Computes, (Pi XOR I) = B' XOR h (Ts')
EUA5.2: Computes, C' * = h (h (Pi XOR I) XOR Ts')
EUA5.3: Checks whether C' = C'*. If it holds, then gives permission to access again otherwise terminates the accessing.

3.4 Password Change Phase

The user is authenticated by using the Password used primarily for login process. Now, there is a problem of keeping this password secure by the user from attacker. To overcome this issue one random generator generates binary number which is same length of password. Then every time a new password is produced after xoring with old password. Once authenticated, the user is asked to enter the new password. Once the new password is entered, the value of is replaced with. Thereby the user is allowed to further login by using the new password. Hence one time and same password has got higher probabilities of breaking threat by attacker.

4. EXPERIMENTAL RESULTS AND DISCUSSION

Suppose UR submits the following password and identifier to the SR,

User Password (P1): “User’sAuthentication”
User Identifier (I): “IdentityofRemoteUser”

So, P1=557365722773417574686566e7469636174696f6e
Suppose UR sends a message of 1600 bits to the SR,
User Message (M): “User authentication is the most vital issue among all security issues in grid computing. Time dependent Authentication technique will check the authenticity of user for time to time throughout the accessing of the remote server.”
So, the message blocks are,
M_1=41757468656e7469636174696f6e20696e207365
M_2=6e64696e6720696e666f726d6174696f6e206973
M_3=20612072657365617263682063686616c6c616e67
M_4=65652054696d652056617269616e742041757468
M_5=656e7469636174696f6e20746563686e697175
M_6=2077696c6c20636865636b2074686520617574
M_7=656e746963697479206f66207573657220666f
M_8=2074696d6520746f2074696d65207468726f75
M_9=686f7574207468652061636365737369 6e672
M_{10}=6620746865207265 6d6f746520736572766572
The CSgenerates the following new passwords after receiving every authentication query from SR,
P2: 06111a421d351c170911071b0743081a491c0b
P3: 27874253d5c727166636a7a732a6774697578
P4: 035806404e391303050b4a191b4b0b18081b1f
P5:3f2d785229235c335564792378753f2b597d6f
P6: 430c3b4a42285a3a0a59571d165745300c1a12
P7: 34655726624b325f693277697e326551796e7a
P8: 5a113e450b3f4b7f0654571c0d5717711f0108
P9: e7853202b4b245f723d3a792d237f0370746f
P10:57410d27005f23417f135e591c5e50166d1754

5. CONCLUSION

Mostly the development of different types of authentication mechanisms in Grid are based on public key infrastructure which works pretty well, but unnecessarily limits users and which may not be flexible or convenient. In this paper we have implemented the concept of automatic Variable Password and applied it to invent an efficient Time Variant Authentication technique that will check the authenticity of user of some different domain of Grid time to time throughout the accessing of the remote server. By adopting this technique, the remote communications among the resources in Grid environment are completely restricted within the proper authentic user and resource provider. In future, we propose to work to minimize the computational cost of our technique.

6. REFERENCES

[1] C. T. Bhunia, Information Technology Network and InternetNew Age International Publishers, India, 5 Edition (Reprint), 2006.
[2] F. Magoules, 1. Pan, Kiat-An Tan and A. Kumar, Introduction to Grid Computing, CRC Press Taylor & Francis Group, ISBN 978-1-4200-7406-2, 2009
[3] I Foster, C Kesselman (eds.). The Grid: Blueprint for a Future Computing Infrastructure. Morgan Kaufmann: San Francisco, CA, 1999.

[4] I Foster, What is the Grid? A Three Point Checklist Argonne National Laboratory & University of Chicago 2002

[5] C.T.Bhunia et al, Application of Automatic Variable Key in ECB with DES and RSA, Proc.Annual CSI ConferencMcGraw Hill, 2004, pp-135-145.

[6] Lamport. L., "Password Authentication with insecure Communication", ACM Communications 24(11), 770772, 1981.

[7] Hwang.T, Chen.Y, Laih. C. S, "Non-Interactive password authentication without password tables", IEEE Conference on Computer and Communication Systems, pp. 429-431.

[8] J.K.Lee, S.R.Ryu and K.Y.Yoo, "Fingerprint-based remote user authentication scheme using smart cards", Electron. Lett., vol.38, no.12, pp.554-555, 2002.

[9] C.C.Chang and I.C.Lin, "Remarks on fingerprint-based remote user authentication scheme using smart cards",ACM SIGOPS operating System Rev., vol.38,no.4, pp.91-96, 2004.

[10] C.H.Lin and Y.Y.Lai, "A flexible biometrics remote user authentication scheme", Computer Standards Interfaces, vol.27, no.1, pp.19-23, 2004.

[11] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain,"Biometric cryptosystems: Issues and challenges,"Proc. IEEE, Special Issue on Multimedia Security for Digital Rights Management, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[12] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith,"Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", in Eurocrypt 2004,pp. 523–540.

[13] Juels and M. Wattenberg, "A fuzzy commitment scheme", in Proc. ACMConf. Computer Communications Security, 1999, pp. 28–36.

[14] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice", IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 503–512, Sep. 2007.

[15] C.M. Chen and W.C. Ku, "Stolen-verifier attack on two new strong-password authentication protocol", IEICE transactions on Communications, E85-B (11), 20002,pp. 2519-2521.

[16] Chun-I Fan and Yi-Hui Lin, "Provably secure remote Truly Three-Factor Authentication Scheme with Privacy Protection on Biometrics", IEEE Transactions on information Forensic and Security, vol. 4, No.4,December 2009.

[17] Anirban Chakrabarti, "Grid Computing security",Springer, ISBN 978-3-540-44492-3, 2007.