On Identity-Based Cryptography and Grid Computing*

H.W. Lim and M.J.B. Robshaw

Information Security Group
Royal Holloway, University of London
Egham, Surrey, TW20 0EX, UK
{h.lim, m.robshaw}@rhul.ac.uk

Abstract. In this exploratory paper we consider the use of Identity-Based Cryptography (IBC) in a Grid security architecture. IBC has properties that align well with the demands of Grid computing and we illustrate some trade-offs in deploying IBC within a Grid system.

1 Introduction

Continual improvements to computing power, storage capacity, and network bandwidth are permitting computing technologies of previously unheard sophistication. Nevertheless, there remain increasing demands for more computational power and resources and Grid computing has been proposed as a mechanism to provide such demands. In order to realise the Grid vision, a sound and effective security architecture is of the utmost importance, and there are many complications due to the interoperable, heterogenous, scalable, and dynamic qualities of a Grid deployment.

Independently of Grid computing, a variant of traditional public key technologies called Identity-based Cryptography (IBC) has recently received considerable attention. In [4] Shamir introduced identity-based cryptosystems in which the public key can be generated from a publicly identifiable information such as a person's e-mail address. The corresponding private key is generated and maintained by a Private Key Generator (PKG) (or Trusted Authority). More recently, work by Boneh and Franklin [1] on identity-based encryption has inspired much new research in the field. The potential of IBC to provide more immediate flexibility to entities in a security infrastructure may well match the qualities demanded by Grid computing. In particular, the properties of IBC that allow generation of keying information on the fly offers a good opportunity to consider IBC as an alternative approach to Grid security.

* The full paper is available at http://www.isg.rhul.ac.uk/∼hwlim/.

M. Bubak et al. (Eds.): ICCS 2004, LNCS 3036, pp. 474–477, 2004.

2 Alternative Approach to GRID Security

The Globus Toolkit (GT)[1], in its latest 3.0 version, is currently the most popular open source software toolkit for building GRID systems. The security services provided by the GT rely upon a security architecture called Grid Security Infrastructure (GSI), which is based on PKI and Transport Layer Security (TLS) communication protocol. The focus is primarily on authentication (including cross-domain), message protection, and single sign-on and identity delegation through proxy credentials [3]. The major components are as follows.

Virtual Organisation (VO). A dynamic collection of users and resources that potentially span multiple administrative domains and governed by a set of defined sharing rules.

User. A subscriber to a GRID. The user can belong to a VO or multiple VOs and he may share part or all of his local resource to other users.

Resource. This comprises from any sharable resource including hardware and software. A user can be a resource to other users if he could offer part or all of his local resource.

Community Authorization Service (CAS). Each VO has its own CAS to maintain a set of policies and communicate those policies to the resources.

Community Policy. A local database that stores policies imposed on each user of a VO.

Grid Certificate Authority (CA). An independent, trusted and potentially shared CA for a VO. It certifies and signs certificates for the VO members.

PKI is an authentication enabling technology and it is widely used in the GT. Using a combination of secret key and public key cryptography, it enables a number of other security services including data confidentiality, data integrity, and key management. Within the GT, when a user (say Alice) wishes to send a job request to a resource (Resource X), she needs to authenticate herself to her CAS Server. The CAS Server establishes Alice's identity and rights using a local policy database maintained at Community Policy. It then issues Alice a signed policy assertion containing her identity and rights. Alice sends the policy assertion and her certificate to Resource X. Resource X authenticates Alice and verifies her VO membership. It also enforces VO's policies stated in the assertion and local policies in regard with VO and Alice herself. Once these are done, Alice is authorized to use Resource X.

The identity token used in GRID is provided through an X.509 public key certificate. It contains a public key, a subject name in the form of a distinguished name (DN), and a validity period that is signed by a Grid CA [6]. Each entity's public key can be transmitted in a X.509 certificate as part of a TLS connection handshake. Upon completion of a handshake protocol which includes key exchange messages from both parties, the parties can begin to transfer data securely over the established communication channel. In GRID, a private/public key pair is usually generated by each individual (user/resource). Should a user

[1] The Globus Toolkit, `http://www-unix.globus.org/toolkit/`

realise or suspect that his private key has been compromised, then the holder himself is held accountable for the notification of the exposed key to the Grid CA in order to have his certificate revoked as soon as possible.

Despite the importance of PKI, there is an increased research focus on IBC. The main stimulus for this trend is the problem of managing certificates and their associated keys using PKI (refer to the full paper for further description). In the full paper we explore whether IBC may be used to alleviate similar problem in a GRID environment and perhaps provide other advantages. To illustrate the properties of IBC, suppose Alice, through an IBC-based system, wants to send an encrypted message to Bob using an identity-based cryptosystem. Alice does not need to verify the authenticity of Bob's public key (by retrieving Bob's public key certificate). Instead Alice simply encrypts the message with an identifying public key, e.g. '`bob@xyz.com`'. Clearly, Alice needs to know the public parameters or system parameters of Bob's PKG. If Bob does not already possess the corresponding private key, he has to obtain it from his PKG. If the PKG is satisfied that Bob is the legitimate receiver of the message, the PKG uses a master key to generate the private key that matches Bob's public key string. The major technical difference between IBC and PKI is the binding between the public/private keys and the individual. This is achieved by using certificates in PKI. For IBC, the public key is bound to the transmitted data while the binding between the private key and the individual is managed by the PKG [2].

To see how IBC could be applied in a GRID environment, we presume that Alice and Bob both belong to the same VO. When Alice wishes to communicate securely with Bob, in principle she could simply encrypt the message with public key string:

'`Bob's DN` $\|$ `timestamp`'.

She neither needs Bob's public key certificate nor verifies his identity as the authentication task has been indirectly transferred to the PKG. Note that Bob needs to authenticate himself to the PKG before he receives the appropriate corresponding private key. In addition, one can add more granularity to impose restrictions on the receiving party. For instance, if Alice wants to ensure that her job request can be read by Resource X only and no other resource, she can in principle encrypt her job descriptions and the associated policy assertion with public key string that includes Resource X's role:

'`Resource X's DN` $\|$ `role` $\|$ `timestamp`'.

The potential shown by IBC in generating public key instantly without performing certificate lookup and verification offers the flexibility that closely matches the dynamic qualities of the entities within the GRID environment as they join and leave the VO. However, IBC-based cryptography also has a drawback since each entity needs an authenticated and secure channel with the PKG when retrieving his private key. Thus IBC is a relatively new technology in comparison with PKI and the full implications have yet to be considered in its application to a GRID system. However, some first steps are taking place and

we note that Stading [5] has recently developed an IBC-based key management mechanism for use within a distributed system.

3 Conclusions

The development of GRID computing is one of today's most important technical problems and the security issues within a GRID deployment are numerous and complicated. Current implementations rely heavily on traditional PKI as a way of supporting many security services. In the full paper we explore the potential benefits of IBC within a GRID infrastructure and we suggest that IBC might have the right properties to provide an alternative security solution for GRID systems. However, true possibilities of integrating identity-based mechanisms within a GRID infrastructure will become clearer with more research. Nevertheless, this interaction could be promising, and the inherent qualities of IBC appear to closely match the demands of a dynamic environment like GRID where the availability of new or current resources can change swiftly over time.

References

1. D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In J. Kilian, editor, Proceedings of Advances in Cryptology - CRYPTO 2001, pages 213-229. Springer-Verlag LNCS 2139, 2001.
2. K.G. Paterson and G. Price. A Comparison between Traditional Public Key Infrastructures and Identity-Based Cryptography. Information Security Technical Report, 8(3):57-72, 2003.
3. L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke. A Community Authorization Service for Group Collaboration. In Proceedings of the 3rd IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'02), pages 50-59, June 2002.
4. A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, Proceedings of Advances in Cryptology - CRYPTO '84, pages 47-53. Springer-Verlag LNCS 196, 1984.
5. T. Stading. Secure Communication in a Distributed System Using Identity Based Encryption. In Proceedings of 3rd IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2003), pages 414-420, May 2003.
6. M.R. Thompson, D. Olson, R. Cowles, S. Mullen, and M. Helm. CA-based Trust Model for Grid Authentication and Identity Delegation. Global Grid Forum (GGF) Grid Certificate Policy Working Group, June 2003. Available at http://www.gridforum.org/documents/GFD/GFD-I.17.pdf, last accessed in November 2003.