University of Manchester

E-infrastructure Security: Levels of Assurance (ES-LoA)

Ning Zhang, Stephen Pickles

A. Introduction

Supporting secure and dynamic resource (including data, knowledge, and services) sharing and collaborations across institutional boundaries, i.e. the concept of Virtual Organisations (VOs), is an essential part of achieving the vision of an e-Infrastructure[1]. Robust electronic authentication (e-authentication) capable of reliably identifying remote users (human beings or software components) with a certain level of assurance in authentication strength is an important pre-requisite to facilitate effective user authorisation and fine-grained access control to distributed services and resources in the VO environment.

Resources provided in this e-world usually have varying levels of sensitivity. For example, e-catalogue services typically have a lower sensitivity level than subscribed e-resources such as e-journals and e-learning materials, whereas e-journals are less sensitive than exam papers that should only be accessible to staff members who are responsible for setting and moderating the exams. Similarly, raw patient data sets uploaded into a central repository for anonymisation processing are much more sensitive than the processed data sets that have private and sensitive information being taken away from them. Clearly, there should be a minimum agreed level of trust between a user and his/her home institution and between the home institution and the service provider for the granting of, and access to, resources with varying levels of sensitivity. A determining factor in this trust level derivation is the strength, or LoA, of the underlying authentication systems used. In other words, to provide a fine-grained access control to resources, there is a need to link access privileges to the authentication LoA derived based upon the method/token used to identify the user and the underlying access management systems used by the home institution.

We propose to organise a preliminary discussion on the definition and application of authentication assurance levels in achieving fine-grained access control in Grid/VO environments, and to establish consensus across the Grid communities on how different levels of assurance are established, and how different levels of assurance are assigned to various types of resources.

B. Related on-going work

The FAME-PERMIS (Flexible Access Middleware Extensions to PERMIS) [FAME] hosted in the University of Manchester is most relevant to this proposal. The FAME-PERMIS project, collaboratively undertaken with Prof David Chadwick [PERMIS] from the University of Kent, is the first such effort to develop middleware extensions to link LoA to authorisation decision making.

The FAME-PERMIS project addresses the very fact that different authentication methods, tokens, and protocols provide different levels of authentication assurance by implementing the LoA definition recommended by NIST [NIST]. For instance, IP address-based authentication and authorisation services would grant the access privilege to anybody who has access to a machine with a correct IP address. Authentication via username/password establishes the identity of a user through proving the knowledge of an authorised username/password pair. A smart-card based authentication method authenticates a user provided that the user possesses a hard cryptographic token and also can demonstrate the knowledge of a secret (or a PIN) used to lock/unlock this token. Clearly, the IP-based authentication method provides the weakest, whereas the smart card based method provides the strongest level of authentication assurance among the three methods. FAME-PERMIS has envisaged that service providers should be able to enforce varying levels of access control to resource/data with varying levels of sensitivity depending on the level of authentication assurance, i.e. LoA.

For this vision, the FAME-PERMIS project team has made several achievements so far [ChinA/B, ZhanA/B]. Firstly, the FAME-PERMIS middleware extensions have been developed, which consist of two major software components, FAME and PERMIS, linked through the Shibboleth infrastructure and protocols. FAME is an extension to the Shibboleth Identity Provider (IdP). It supports the use of a variety of authentication methods, calculates a LoA based upon the authentication method/token used in an authentication instance, and feeds this LoA along with the user's other attributes to Shibboleth targets. PERMIS, the authorisation decision engine deployed at a Shibboleth target, has now been extended to include LoA in its decision making process. In this way, an authorisation decision is now

[1] http://www.hm-treasury.gov.uk/media/95846/spend04_sciencedoc_1_0907.pdf

made based on the following tuple, (*Subject, Target, Action, LoA*), rather than the traditional (*Subject, Target, Action*) attributes.

Secondly, it has been recognized in the GridSite user community that the missing piece for GridSite users is a way of representing the quality of the authentication, and expressing requirements about that in GACL or XACML policies. Based upon these observations, and in order to make the project outcome more profitable to the GridSite user community, the FAME-PERMIS project team is also working on applying our LoA approach to, and implementing it in, the GridSite policy engine. This will implicitly add Shibboleth support to the existing website and portal systems built on GridSite's security framework.

In addition, the CLEF-Services project, providing "joined up" information solutions for clinical care and clinical and bio-science research in cancer, is a user partner of the FAME-PERMIS project.

Two further Manchester projects are of special relevance to LoA. "User-Friendly Authentication and Authorisation for Grid Environments" (EPSRC, shortly to commence) is focused on improving the usability of security in a Grid context, and is questioning the need for end-users to manage private keys. The JISC-funded SHEBANGS project (http://www.sve.man.ac.uk/Research/AtoZ/SHEBANGS) is providing access to the NGS for users who do not currently have credentials that can be understood by the currently deployed Grid middleware. It achieves this by utilising the emerging Shibboleth infrastructure, translating SAML based Shibboleth assertions into PKI, GSI and VOMS based Grid credentials. In both projects, the mechanisms for insulating the end-user from the PKI subtly alter the LoA, and it is important to understand the implications for service providers and their policies.

C. Questions for Discussions

LoA is defined as the strength of authentication required for a service provider to be assured that a resource access is only granted to users whose identities have been verified. It reflects the degree of confidence in an authentication process used to establish the identity of an entity (an individual or a software component) to whom the credential was issued, and the degree of confidence that the entity using the credential is indeed the entity that the credential was issued to. All the processes associated to the authentication process influence the LoA established. These include the process of identity proofing, the type of authentication *credential* (or *authenticator* or *token*) being used by the entity, and the authentication protocol/method used by the underlying authentication service. More importantly, LoA is also influenced by how credentials are managed. This includes the token technology that is used to store the credential, the manner in which a claimed identity is bound to an authentication credential, the life cycle management of the credential, whether the Credential Service Provider (CSP) has sufficient operating procedures, processes and policy frameworks to establish the required level of trust. Furthermore, the extent to which an authentication event is coupled to an authorisation event should also be taken into account when LoA is established.

There have been some notable national and international efforts and activities in defining the levels of assurance and specifying requirements for these levels. For example, LoA definitions have been specified by the UK government's Office of the e-Envoy in its document release - the e-Government Strategy Framework Policy and Guidelines [eEnv]. Influenced by the definitions published by the UK government, the US government's e-Authentication Initiative [eAuth] has defined a framework for determining the level of authentication assurance needed for e-government transactions. NIST (US National Institute of Standard and Technology) [NIST04/06] provides specific technical guidance on how to achieve that level of assurance. In this draft standard published by NIST, four levels of authentication assurance are defined. Other activities include the Australian eGovernment Evolution 2006 initiative [eGov] and the Electronic Authentication Partnership led by US industry [ePar].

Despite these efforts and activities, the definition and application of authentication LoA in the context of Grids and VO environments has not been examined. Are the existing definitions of LoA suited to Grid or VO environment? How to apply LoA to safeguard Grid services/resources? Are some onerous registration requirements or special condition stipulations due to perceived inadequacies in the strength of authentication? Are there any limitations in terms of user accessibility, scalability and interoperability?

References

[ChinA] Chin, J.; Parkins, M.; Zhang, N.; Nenadic, A.; and Brooke, J. M.; "GridFAME: Flexible Authentication Middleware Extension for Grids", the 2nd Workshop on Grid Computing & Applications (GCA 2005), May 2005, Biopolis, Singapore, pp. 17–26.

[ChinB] Chin, J.; Parkin, M.; Zhang, N.; Nenadic, A.; and Brooke, J. M.; "An Authentication Strength Linked Access Control Middleware for the Grid", SCS International Journal of Information Technology (SCS-IJIT), Vol. 11, No. 4, 2005.

[eAuth] http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf.

[eEnv] http://www.cabinetoffice.gov.uk/csia/documents/pdf/Assurance_V2._Sept_2002.pdf.

[eGov] http://www.iqpc.com.au/cgi-bin/templates/document.html?topic=592&event=9139&document=66543&slauID=5&

[ePart] http://www.eapartnership.org/.

[FAME] http://www.fame-permis.org/index.html.

[GridSite] Grid Security for the Web platforms for Grids; http://www.gridsite.org/.

[NIST04] W. E. Burr et al., DRAFT Recommendation for Electronic Authentication, NIST Special Publication 800-63, Jan. 2004.

[NIST06] William E. Burr, et al, DRAFT Recommendation for Electronic Authentication, NIST Special Publication 800-63 version 1.0.2, April 2006.

[PERMIS] http://www.permis.org/en/index.html.

[Shibboleth] http://shibboleth.internet2.edu/.

[ShiMMeR] Shibbolising MIMAS eResources' http://www.mimas.ac.uk/shibboleth/

[ZhanA] Zhang, N.; Yao, L.; Chin, J.; Shi, Q.; Nenadic, A.; and McNab, A.; Rector A.; and Goble, C.; "Plugging a Scalable Authentication Framework into Shibboleth", the 14th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE 2005), 13-15 June 2005, Linkoping, Sweden, pp. 271-276.

[ZhanB] N. Zhang, L. Yao, A. Nenadic, J. Chin, C. Goble, A. Rector, D. Chadwick, S. Otenko and Q. Shi; "Achieving Fine-grained Access Control in Virtual Organisations", to appear in Concurrency and Computation: Practice and Experience, published by John Wiley and Sons publisher.