Network Security, Administration and Management:

Advancing Technology and Practice

Dulal Chandra Kar
Texas A&M University–Corpus Christi, USA

Mahbubur Rahman Syed
Minnesota State University, Mankato, USA

Information Science
REFERENCE

Senior Editorial Director: Kristin Klinger
Director of Book Publications: Julia Mosemann
Editorial Director: Lindsay Johnston
Acquisitions Editor: Erika Carter
Development Editor: Joel Gamon
Production Editor: Sean Woznicki
Typesetters: Natalie Pronio, Jennifer Romanchak, Milan Vracarich Jr
Print Coordinator: Jamie Snavely
Cover Design: Nick Newcomer

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com/reference

Library of Congress Cataloging-in-Publication Data
Network security, administration and management: advancing technology and practice / Dulal Chandra Kar and Mahbubur Rahman Syed, editors.
p. cm.
Includes bibliographical references and index.
Summary: “This book identifies the latest technological solutions, practices and principles on network security while exposing possible security threats and vulnerabilities of contemporary software, hardware, and networked systems”-- Provided by publisher.
ISBN 978-1-60960-777-7 (hardcover) -- ISBN 978-1-60960-778-4 (ebook) -- ISBN 978-1-60960-779-1 (print & perpetual access) 1. Computer networks--Management. 2. Computer networks--Security measures. I. Kar, Dulal Chandra, 1960- II. Syed, Mahbubur Rahman, 1952-
TK5105.5.N466724 2011
005.8--dc22
2011010430

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 3
Security Issues for Multi-Domain Resource Reservation

Christos Bouras
Research Academic Computer Technology Institute (CTI) & University of Patras, Greece

Kostas Stamos
Research Academic Computer Technology Institute (CTI) & University of Patras, Greece

ABSTRACT

In this chapter, we deal with the issue of security regarding components that are responsible for provisioning multi-domain network services, either automatically or through some form of administrator interaction. It is evident that a malicious compromise of such a component would have far-reaching implications for the stability of the network. Furthermore, trust between cooperating domains is a delicate issue, and each partner in the multi-domain federation has to have some guarantees that peers in the service are not going to be security compromised. We enumerate some of the related dangers and propose ways to limit the attack surface, reduce the intrusion possibilities, and guarantee the quick resolution of any successful violations.

The issue of security is studied in two main parts: Inter-domain security, for the communication between domains and the successful negotiation of resource reservations, and intra-domain security, for the internal communications within a domain for the initiation of a resource reservation and its actual realization in the network devices. Resource reservation is studied both on the level of IP services based on Differentiated Services architectures, and on the level of dynamic circuit reservation based on Layer 2 technologies.

The chapter is completed with a case study on the authentication and authorization framework designed in the context of a Pan-European network resource reservation service, in the Geant academic and research network.

DOI: 10.4018/978-1-60960-777-7.ch003

INTRODUCTION

A specific example of automated network administration for resource provisioning is the Bandwidth Broker entity, which is the component responsible for providing QoS within a network domain and negotiating the realization of a service across peering domains. The Bandwidth Broker manages the resources within the specific domain by controlling the network load and by accepting or rejecting bandwidth requests. In this context, resources refer to bandwidth and queue allocation at the network elements in order to achieve better performance in terms of throughput, delay, jitter, packet loss and reordering. A user within the domain that is willing to use an amount of the network resources between two nodes, has to send a request to the Bandwidth Broker. The decision to accept or reject a request is made by the admission control module. In the case that the requested resource is managed by multiple domains, the Bandwidth Broker is also responsible for the inter-domain communication with Bandwidth Brokers of adjacent domains. This procedure requires communication between adjacent Bandwidth Brokers and also a special agreement between the domains. Several such automated systems have been proposed and implemented (Bouras et al. 2007, Campanella et al. 2006, Shigeo Urushidani et al. 2008). In this chapter, our focus is on the security aspects in the context of Bandwidth Broker interdomain and intradomain communication, on the past work that has been done in this area and on the theoretical challenges and proposed solutions.

In addition, several efforts have been made for the automated multi-domain provisioning of circuit services at layers below the IP layer. One such extensive effort has been taken over by the Geant pan-european research and academic network, using the name AutoBAHN (Automated Bandwidth Allocation across Heterogeneous Networks). In the framework of this activity, it has specified and is developing a Bandwidth on Demand (BoD) service intended to operate in a multi-domain environment using heterogeneous transmission technologies. The AutoBAHN system aims at providing a guaranteed capacity, connection-oriented service between two end points. In this context resources refer to the provisioning of the circuits themselves. The reservation of network resources by an end-user, an application or middleware software is automated to a large extent, as the AutoBAHN system, in cooperation with localized provisioning systems that may be available in various participating domains, takes care of the interdomain communication and orchestration of the pathfinding, resource checking, scheduling and low-level network configuration procedures. A user submits a reservation through a GUI while applications and middleware utilize a related API. The AutoBAHN service supports multi-domain point-to-point connectivity with symmetric capacity and paths. It is also capable of handling advance reservations and of providing protection to the service. In our discussion, a domain refers to an administrative entity that is responsible for the management of a set of network elements. A single domain may contain multiple technological domains, but in terms of authority and authentication, it is considered as a single entity.

The overall architecture of the AutoBAHN system, its goal and the network mechanisms it employs are thoroughly presented in Campanella et al. (2006). The core of the system is comprised of the following main modules: Inter-domain Manager (IDM), Domain Manager (DM), Technology Proxy, Reservation Request Handling, User access module, AAI module, Inter-domain Pathfinder, Intra-domain Pathfinder and Topology Abstraction module. This chapter highlights the architecture of the AAI system (Authentication and Authorization Infrastructure) of the AutoBAHN platform, for the purposes of a detailed case study that has wider applicability.

BACKGROUND

Dealing with sensitive information such as the network resources management has to increase the awareness of possible security problems. The Public Key Infrastructure model (PKI) has been developed in order to deal with a number of possible attacks and protect against security, privacy and authentication violations. It is generally understood as the set of policies and software that regulate or manipulate the use of certificates and of public and private keys. Asymmetric encryption is a basic component of the architecture, which is based on a public key that can be disclosed to anyone, and a private key that is known only to its holder.

Our discussion intends to identify the ways with which the resource provisioning system implementation can be guarded against the various types of attack. In general, network attacks can be summarized in the following broad categories:

- Integrity attacks: The attacker tries to compromise the correctness, timeliness, authenticity or quality of the information exchanged.
- Confidentiality attacks: The attacker tries to disclose sensitive information that should normally only be accessible for authenticated parties.
- Availability attacks: The attacker tries to make the service unavailable to legitimate users.

Furthermore, a robust implementation also has to be capable of recovering from situations that do not pose a direct security threat, but can nonetheless compromise the operation of the system. Such cases are:

- Equipment / software malfunction: One or more of the communicating peer modules do not operate as expected and, for whatever reason, produce invalid, unexpected or simply erroneous results.
- Users' misbehavior: Users that do not follow the rules that have been mutually agreed upon, by for example violating the SLAs and attempting to increase their network resource usage at the expense of other users. These users have to be identified and disciplined according to the policies that have been set in place for each case.

There are the following aspects of security that relate to possible users' misbehaviour:

- Non-repudiation: The intent here is to make it impossible for the user to credibly deny having performed an action, for example by refusing to acknowledge that that he/she is the sender of an exchanged message.
- Authentication: The intent is to only allow legitimate users to have access to the resource reservation service. The access may be used to perform any service-related activity, such as reservation request, reservation query, reservation administration and management, etc.
- Authorization: The intent is to differentiate between the actions that legitimate users are allowed to perform. This means that authentication is a prerequisite for authorization, but authorization goes a step further by restricting the level of access a user may have to the service.

WS-Security Standards

A multi-domain resource reservation infrastructure such as Bandwidth Brokers rely on the communication between multiple and often remote components. Communication over the HTTP protocol using XML messages following the SOAP standard have been a very popular way of constructing such multi-domain services, where

interoperability and automated machine interaction is a primary objective. It is therefore important to also consider the implications of securing message exchanges through the WS-Security standards (WS-Security, 2010).

An alternative to Web Services Security in this context is also the usage of Transport Layer Security in order to exchange messages over HTTPS. This approach however, does not provide true end to end security, which is guaranteed by WS-Security from the moment an XML message is constructed to the point it is parsed. However, some researchers have also criticized aspects of WS-Security for possible exploitation weaknesses (Gruschka et al., 2009).

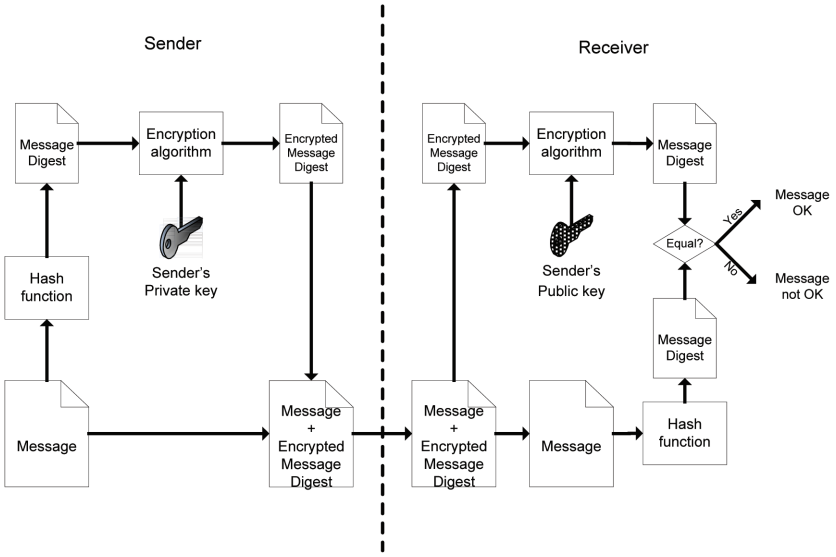
The purpose of WS-Security is to specify how technologies such as XML-Signature, XML-Encryption and SAML can be used for securing SOAP messages.

XML-Signature is the way to provide data integrity through the utilization of digital signatures. A digital signature is used in the context of asymmetric encryption, where the communicating parties own their secret private key and have announced the corresponding public keys. A sender can then produce, using a hashing algorithm, a digest of the exchanged message, and then encrypt the digest using its own private key. The encrypted digest is called a digital signature, and the receiver of the message can decrypt the digest (using the sender's public key), be certain that only the specified sender may have produced the encrypted digest (since he is the only one holding the corresponding private key), and re-run the hashing algorithm in order to compare it with the decrypted digest and make sure that the exchanged message has not been tampered with. Figure 1 illustrates the digital signature concept as used in modern cryptography.

The purpose of XML Signature is to assure data integrity and it can also be considered in the context of authentication and non-repudiation. The WS-Security standard specifies how XML Signature can be used to bind the identity of a sender to a SOAP message.

XML-Encryption defines how the contents of an XML message should be encrypted using cryptography in order to convert plaintext into ciphertext. XML-Encryption is usually used in combination with XML-Signature, such as in a

Figure 1. Digital signature concept



combination known as Sign-Encrypt-Sign, where the plaintext document is first signed, and then the signature is encrypted, along with the plaintext. Finally, the ciphertext is signed again in order to ensure that it can not be changed, either intentionally or by accident, without being noticed.

The Secure Assertion Markup Language (SAML) is a specification that aims at enabling portable trust, by specifying assertions using XML. These assertions are used for providing authentication of single persons or applications between multiple different domains, without requiring a central authentication registry, which often introduces problems of scalability, management and confidentiality.

SECURITY APPROACHES FOR DIFFERENTIATED SERVICES

The SIBBS protocol (Simple Inter-domain Bandwidth Broker Signaling) is proposed by the Internet2 community in order to implement the inter-domain communications of resource reservation between the Bandwidth Brokers. It exchanges two pairs of messages for QoS configuration purposes, the Resource Allocation Request (RAR) / Resource Allocation Answer (RAA) messages to request for a service, and the CANCEL / ACK messages to terminate the requested service. The transmitted information is sensitive and therefore has to be protected against possible security compromises. In Lee et al. (2004), the authors outline the main security threats that inter-domain Bandwidth Broker communication has to protect against, and explain how the Public Key Infrastructure (PKI) can be integrated in order to produce a secure SIBBS implementation.

In Bouras et al. (2008), an efficient algorithm for the Bandwidth Broker's admission control module has been proposed, with the intent of achieving satisfactory utilization of the network resources without heavily impacting the Bandwidth Broker's performance. In Bouras et al. (2005) the architecture has been extended so that it can support a distributed Bandwidth Broker architecture as illustrated in Figure 2. In the case of a distributed Bandwidth Broker operation, the messages exchanged between the remotely positioned Bandwidth Broker modules have also to be secured, since in that case there is also a fair amount of intra-domain Bandwidth Broker communication that exchanges sensitive information related to the management of the network resources in the domain managed by the Bandwidth Broker.

The security for messages exchanged between the Bandwidth Broker components and messages directed to the Policy Enforcement Points (PEPs) can be enforced using the PKI model with lightweight certificates that do not have a large impact on the communication overhead imposed on the network.

Inter-Domain Security

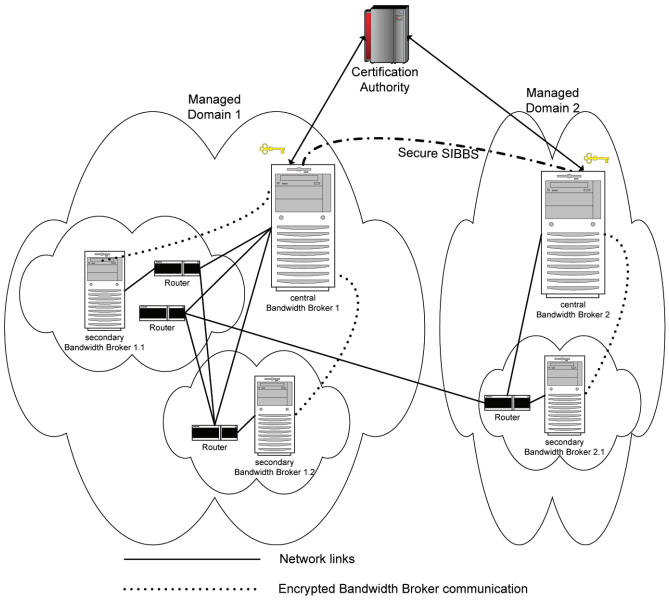
Inter-domain security deals with the communications between Bandwidth Brokers that manage neighbouring domains. The effort on this area has concentrated on securing protocols such as the SIBBS protocol (Qbone, 2002, Sander, 2000), that deal with the Bandwidth Broker communication across domains.

A common certification authority or a common hierarchy of trust enables the signing of exchanged messages and their validation at the receiving end according to the digital certificates issued by the certification authority. Furthermore, the issue of authorization of user actions and requests (dealing with what level of access a user originating from a specific domain is allowed to have in the overall multi-domain service) can be dealt with the utilization of portable trust approaches such as the utilization of SAML.

Intra-Domain Security

Intra-domain security has to deal with the communication between the Policy Decision Point

Figure 2. Security-enhanced distributed architecture



(PDP) that is the Bandwidth Broker, and the Policy Enforcement Points (PEPs) that are typically the network routers that are appropriately configured in order to enforce the Bandwidth Broker's decisions. Also, in the case of a distributed Bandwidth Broker implementation, a large amount of sensitive internal Bandwidth Broker information is likely to be transmitted over the network and is therefore, vulnerable if not properly protected. The overall internal design of the service determines the amount of intradomain information exchanged. For example, several approaches utilize multiple distributed components that coordinate in order to produce admission decisions. Distributed approaches gain in scalability, but introduce complexity, may not achieve optimal results and introduce increased level of information exchange. Their security requirements are therefore also more widespread. In any case, the actual configuration of network devices upon the execution of an accepted user reservation requires access to low level network functionality, which makes network administrators nervous. Therefore, a layered and modular approach is usually more successful, where domain may re-use already existing, tested and trusted components for network configuration, with a limited and well-defined interface towards the multi-domain provisioning service components.

CASE STUDY: POLICIES FOR AAI IN GEANT

The European project GN3 (GEANT, 2010) encompasses a range of research activities to advance both networking and user services in Europe. Central to this project, is the goal of providing high-quality services from one end user to another over multiple interconnected networks. GEANT has deployed services in two main areas: The provisioning of L3 QoS based on Differentiated Services (DiffServ) architecture, and the provisioning of Bandwidth on Demand (BoD) based on dynamic allocation of L2 circuits. The activity that has specified and prototyped a Bandwidth on Demand service intended to operate in a multi-domain environment using heterogeneous

transmission technologies is called AutoBAHN, while the activity that has developed a L3 QoS provisioning framework is called AMPS.

In this section we describe the design decisions and implementation conclusion from the activities related to authentication and authorization for users of the service. After a user has been authenticated using the edugain infrastructure (Edugain, 2010) and is able to submit a resource reservation request, an authorization procedure takes place that determines, according to the specified policies, whether this specific user should be able to reserve resources. This decision is taken in every domain along the reservation path, based on user attributes that have to be transmitted with the reservation request and mapped to the policies implemented by each domain.

The AAI infrastructure is therefore comprised of three main areas, which are described in detail below: User authentication, trusted communications between modules and multi-domain user authorization.

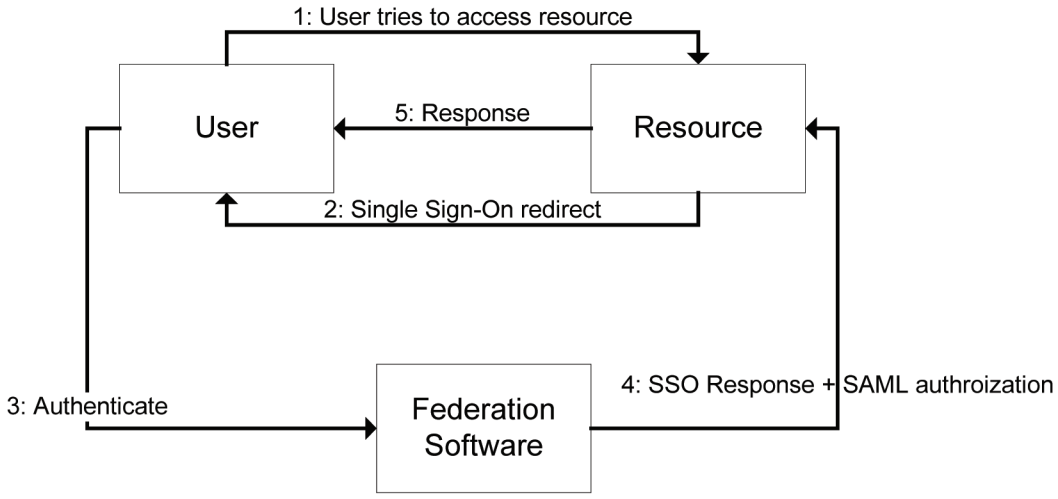
User Authentication

When a user wants to make a reservation in a resource, eduGAIN SSO (Single Sign-On) infrastructure will be used for authentication and authorization purposes as illustrated in Figure 3.

In principle, when a user tries to make a reservation directly, the resource redirects the user to the Single Sign-On service of his/her federation. Then the user is authenticated through the federation software which sends the SSO response and SAML 2.0 authorization back to the resource. The response contains both authentication and authorization information as SAML 2.0 attributes. Finally, the resource checks the SSO response and SAML 2.0 attributes and responds to the user appropriately about his reservation request. The proposed attributes transmitted are the following:

- Name/Email: A unique id of the user wanting to make a reservation. This could be either the name or the email of the user, or a combination of both.
- Organization: The organization/domain/federation of which the user is a member.
- Project Membership: This attribute should contain a specified value (e.g. AUTOBAHN) that demonstrates that this user is an authorized AutoBAHN user.
- Project Role: This attribute offers granularity in terms of the subset of available

Figure 3. Message flow when a human user wants to make a reservation



actions that the user is allowed to perform, and can contain values such as Administrator, Developer, User, etc.

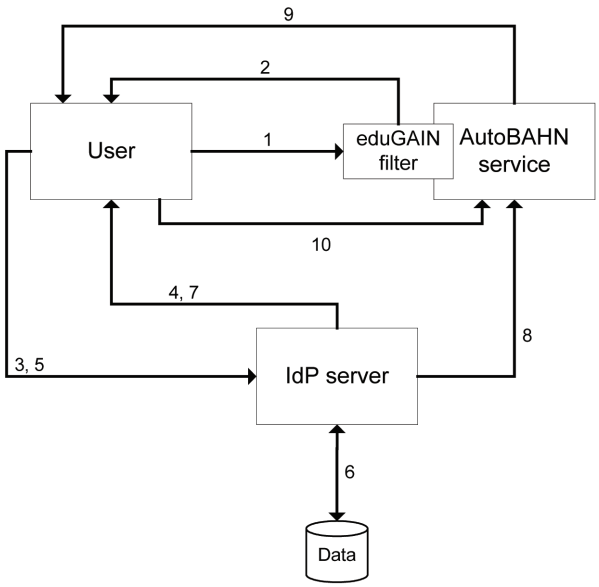
The procedure takes place in the following steps as shown in Figure 4:

1. The user (through a web browser) tries to access the AutoBAHN service (the web-based User Interface) of the starting point of the required reservation.
2. The eduGAIN filter intercepts the request and sends to the web browser an http redirection to an Identity Provider (IdP). In order for this redirection to take place, eduGAIN has implemented a WFAYF (Which Federation Are You From) service, which allows the user to select the appropriate IdP for further processing.
3. The user's web browser sends an http request to the IdP server.
4. The IdP server sends to the web browser a page to authenticate the user.
5. The user sends his credentials (login and password, certificate, etc) to the IdP server.
6. The IdP authenticates the user using the credentials and the local database (such as LDAP). The user attributes concerning AutoBAHN are also retrieved.
7. The IdP server redirects the web browser to the AutoBAHN service.
8. The local AAI also sends the autoBAHN attributes to the IDM. The IDM stores these attributes.
9. The IDM sends the BoD request page.
10. The user fills in the page and sends it to the IDM. From then on, the reservation request procedure is initiated by the IDM.

Trusted Communications Between AutoBAHN Modules

In principle, when the client module wants to communicate with another module (the resource), it sends its request to the required resource along with its X.509 certificate through its eduGAIN filter as shown in Figure 5. The eduGAIN filter of the resource authenticates the client by validating its certificate. The certificate contains identification

Figure 4. AutoBAHN Single-Sign On authentication procedure



information that allows the resource to authenticate only designated clients.

Below is presented the detailed procedure in the context of the AutoBAHN system for the trusted communication between AutoBAHN modules.

1. The AutoBAHN module that wants to communicate (client) must have a certificate, so no interaction for credentials is needed. The X.509 certificate is issued by a Certificate Authority (CA) subordinated to one of the eduGAIN roots of trust.
2. The client module sends its request and the certificate to the resource.
3. The resource module performs trust validation by checking that the whole trust path of the certificate correctly resolves to the root(s) of trust defined by eduGAIN.
4. The resource checks that the client module is allowed to access it.
5. The resource provides the requested answer to the client module.

In the case of AutoBAHN, the support for eduGAIN means that the dedicated eduGAIN trust fabric (composed of a hierarchy of Certification Authorities) can be used in order to make the trusted communication between AutoBAHN modules possible.

Multi-Domain User Authorization

After a user has been authenticated and is able to submit a resource reservation request, an authorization procedure should take place that determines, according to the specified policies, whether this specific user should be able to reserve the resources. This decision has to be taken in every domain along the reservation path, based on user attributes that have to be transmitted with the reservation request and mapped to the policies implemented by each domain.

Figure 6 presents the detailed multi-domain authorization procedure in the context of the AutoBAHN system.

Steps 1-6 are the user authentication procedure. Steps 9-19 are the possible authorization procedure within the start domain of the reservation. When the reservation request has been authorized in its Home Domain and the IDM wants to propagate further down the selected reservation path, it has to send the request to the next domain. The attributes are sent in the same request. An eduGAIN module is planned to be used in order to concatenate these attributes in the AutoBAHN request (XML).

Upon arrival at the next domain, the possible authorization procedure is repeated there and at every subsequent domain.

Concerning the classification of users there are several different options:

- Each reservation made by an authenticated and authorized user is credited to the user individually.
- Each reservation made by an authenticated and authorized user is credited to the user's home domain, and counts against an

Figure 5. Message flow when an automated client wants to make a reservation

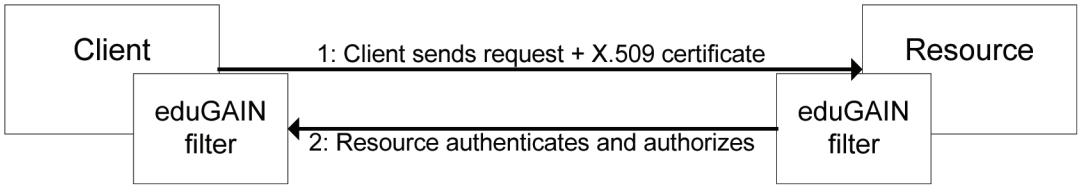
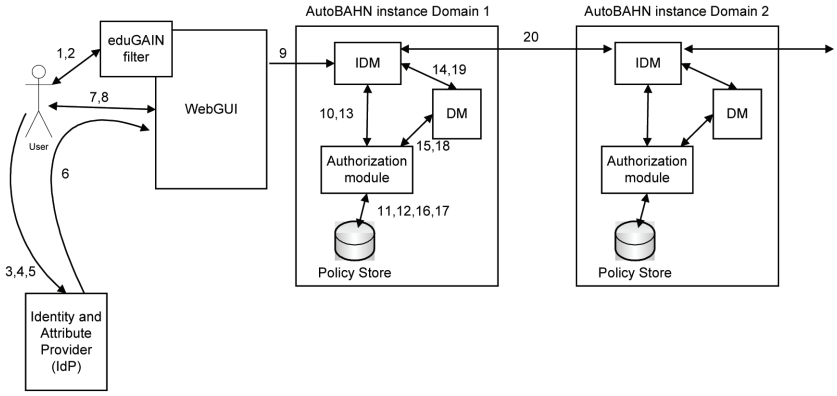


Figure 6. Multi-domain authorization procedure



aggregate limit for all users from the same domain.

- Each reservation made by an authenticated and authorized user is credited to the total number of reservations and counts against an aggregate limit for all AutoBAHN users.

It is possible that each domain chooses its own policy regarding the classification of users, or that over time policies change. The authorization procedure should therefore be able to handle all of the above possibilities.

Furthermore, some sort of granularity in terms of authorization flexibility is required, so that for example users can perform a subset of the available actions through the AutoBAHN management interface (e.g. monitor service, use service, and administrate service). The structure of the subset of allowable actions can also be defined by each domain.

FUTURE RESEARCH DIRECTIONS

Multi-domain authentication and authorization infrastructures pose a new and significant challenge as federated services are being developed and deployed. Deployments have to maintain their security objectives in a potentially unfriendly environment, while simultaneously being practical and effective in terms of user experience and convenience. The widespread deployment of multi-domain reservation services, such as in the case of Geant, is going to provide valuable insight in the large scale characteristics of such services. Furthermore, as multi-domain resource reservation services are moving from the experimental to the production phase, which is also the case for the Geant BoD service, the effectiveness of the AAI infrastructure in the face of actual security challenges is going to be assessed.

CONCLUSION

Security for multi-domain resource reservation services is a subject that touches upon most of the building blocks of security: Confidentiality, integrity, non-repudiation, authentication, authorization, availability etc. It is a very important subject, as any security breach might have repercussions on the proper operation of the network and thus be a potential costly matter. In this chapter we have presented the security requirements and the proposed procedures for protecting against various types of attacks both for layer 3 services based on IETF Differentiated Services architectures, and for Bandwidth on Demand services exemplified by the Geant AutoBAHN service. Emerging multi-domain provisioning

services have a variety of security requirements, ranging from confidential exchange of information both within a single domain and between peering domains, to portable and scalable trust for user requests, and single point of authentication procedures. In this chapter we have shown how current research programmes such as Geant have dealt or are proposing to deal with these issues in actual production environments.

REFERENCES

Bouras, C., Haniotakis, V., Primpas, D., Stamos, K., & Varvitsiotis, A. (2007). *AMPS - ANStool: Interoperability of automated tools for the provisioning of QoS services.* TERENA Networking Conference 2007, Lyngby, Denmark, 21 - 24 May 2007.

Bouras, C., & Stamos, K. (2004). *An adaptive admission control algorithm for bandwidth brokers*. 3rd IEEE International Symposium on Network Computing and Applications (NCA04), Cambridge, MA, USA, August 30 - September 1 2004, (pp. 243–250).

Bouras, C., & Stamos, K. (2005). *Examining the benefits of a hybrid distributed architecture for bandwidth brokers*. The First IEEE International Workshop on Multimedia Systems and Networking (WMSN'05).

Campanella, M., Krzywania, R., Reijs, V., Sevasti, A., Stamos, K., Tziouvaras, C., & Wilson, D. (2006). *Bandwidth on demand services for European research and education networks.* 1st IEEE International Workshop on Bandwidth on Demand, 27 Nov 2006, San Francisco (USA).

Edugain. (2010). Retrieved from www.edugain.org

GEANT network. (2010). Retrieved from http://www.geant.net/

Gruschka, N., & Iacono, L.-L. (2009). *Vulnerable cloud: SOAP message security validation revisited.* 2009 IEEE International Conference on Web Services (pp. 625-631).

Lee, B., Woo, W.-K., Yeo, C.-K., Lim, T.-M., Lim, B.-H., He, Y., & Song, J. (2004). Secure communications between bandwidth brokers. *Operating Systems Review*, *38*(1), 43–57. doi:10.1145/974104.974109

QBone Signaling Design Team. (2002). *Final report*. Retrieved from http://qos.internet2.edu/wg/documents-informational/ 20020709-chimento-etal-qbone-signaling/

Sander, V. (2000). *The security environment of SIBBS*. Retrieved from http://qbone.internet2.edu/bb/SIBBS-SEC.doc

Urushidani, S., Fukuda, K., Ji, Y., Abe, S., Koibuchi, M., Nakamura, M., et al. Shiomoto, K. (2008). *Resource allocation and provision for bandwidth/networks on demand in SINET3.* IEEE Network Operations and Management Symposium Workshops, April 2008, Salvador da Bahia, Brazil.

WS-Security Specification. (2010). *Library specification*. Retrieved from http://www.ibm.com/developerworks/ library/specification/ws-secure/

ADDITIONAL READING

Abdalla, M., Boyen, X., Chevalier, C., & Pointcheval, D. (2009). Distributed Public-Key Cryptography from Weak Secrets, Public Key Cryptography - PKC 2009, LNCS 5443, pp. 139-159, Springer, Stanislaw Jarecki and Gene Tsudik (Eds.), March 2009.

Adams, C. (2003). Understanding PKI: Concepts, Standards, and Deployment Considerations, (2nd Edition), Addison-Wesley Professional, 2002m ISBN-13: 978-0672323911.

Barak, B., Canetti, R., Lindell, Y., Pass, R., & Rabin, T. (2005). Secure computation without authentication. In V. Shoup, editor, CRYPTO 2005, volume 3621 of LNCS, pages 361-377. Springer, Aug. 2005.

Bellare, M., Pointcheval, D., & Rogaway, P. (2000). Authenticated Key Exchange Secure Against Dictionary Attack, Advances in Cryptology - EUROCRYPT 2000, Lecture Notes in Computer Science, vol. 1807, pp. 139-155, B. Preneel, ed., Springer-Verlag, May 2000.

Bertino, E., Martino, L., Paci, F., & Squicciarini, A. (2009). *Security for Web Services and Service-Oriented Architectures, Springer*, *ISBN-13*, 978–3540877417.

Blake, S., Black, D., Carlson, M., Davies, M., Wang, Z., & Weiss, W. (1998). An Architecture for Differentiated Services. *Internet RFC*, *2475*, 1998.

Caffrey, L. (EDT) & Okot-Uma, R. (2001). Trusted Services and Public Key Infrastructure (PKI), ISBN: 0850926602.

Chang, C. C., Hwang, K. F., & Lin, I. C. (2003). Security Enhancement for a Modified Authenticated Key Agreement Protocol. *International Journal of Computational and Numerical Analysis and Applications*, *3*(1), 1–7.

Dournaee, B. (2002). XML Security. *McGraw-Hill Osborne Media*, *ISBN-13*, 978–0072193992.

Fitzi, M., Gottesman, D., Hirt, M., Holenstein, T., & Smith, A. (2002). Detectable byzantine agreement secure against faulty majorities. In 21st ACM PODC, pages 118-126. ACM Press, July 2002.

Gennaro, R. & Lindell, (2003). Y. A framework for password-based authenticated key exchange. In E. Biham, editor, EURO-CRYPT 2003, volume 2656 of LNCS, pages 524-543. Springer, May 2003.

Gentry, C., MacKenzie, P., & Ramzan, Z. (2006). A Method for Making Password-Based Key Exchange Resilient to Server Compromise, Advances in Cryptology - CRYPTO 2006, pp. 142-159. Lecture Notes in Computer Science Volume 4117, Springer Berlin / Heidelberg September 24.

Grob, T. (2003). Security Analysis of the SAML Single Sign-On Browser/Artifact Profile.

Holtby, D., Kapron, B. M., & King, V. (2006). Lower bound for scalable Byzantine agreement. In E. Ruppert and D. Malkhi, editors, 25th ACM PODC, pages 285-291. ACM Press, July 2006.

Kanneganti, R., & Chodavarapu, P. (2008). SOA Security. *Manning Publications*, *ISBN-13*, 978–1932394689.

Katz, J., & Shin, J. S. (2005). Modeling insider attacks on group key-exchange protocols. In V. Atluri, C. Meadows, and A. Juels, editors, ACM CCS 05, pages 180-189. ACM Press, Nov. 2005.

Nichols, K., Jackobson, V., & Zhang, L. (1999). A Two-bit Differentiated Services Architecture for the Internet, lnternet RFC 2638, July 1999.

O'Neill, M. (2003). Web Services Security. *McGraw-Hill Osborne Media*, *ISBN-13*, 978–0072224719.

Panko, R. (2003) *Corporate Computer and Network Security, Prentice Hall*, *ISBN-13*, 978–0130384713.

Pfitzmann, B., & Waidner, M. (2002). Privacy in Browser-Based Attribute Exchange, In Proceeding of the ACM Workshop on Privacy in the Electronic Society.

Raina, K. (2003). *PKI Security Solutions for the Enterprise: Solving HIPAA, E-Paper Act, and Other Compliance Issues* (1st ed.). Wiley.

Rosenberg, J., & Remy, D. (2004). Securing Web Services with WS-Security: Demystifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption. *Sams*, *ISBN-13*, 978–0672326516.

Windley, P. J., & Media, O. (2005). *Digital Identity.*, *ISBN-13*, 978–0596008789.

Zhang, X., Park, J., & Sandhu, R. (1990). Schema Based XML Security: RBAC Approach, Machine Simulator, Third International Conference on Computer Assisted Learning

Zhang, Z., Duan, Z., & Hou, Y. (2001). On Scalable Design of Bandwidth Brokers", IEICE Transactions on Communications, Vol. E84-B, No.8, pp. 2011-2025, August 2001.

KEY TERMS AND DEFINITIONS

Authentication: The process of confirming that a principal (person or application) is the one that is claimed to be and has access to the provided service.

Authorization: The process of determining what operations a principal is allowed to perform.

Availability: The assurance that the service is up and running and can be accessed by its legitimate users.

Bandwidth Broker: As defined by the IETF, a Bandwidth Broker is an agent that has some knowledge of an organization's priorities and policies and allocates Quality of Service (QoS) resources with respect to those policies.

Bandwidth on Demand: The dynamic reservation of dedicated channels for data transport between varying locations with guaranteed levels of service.

Confidentiality: The assurance that exchanged information is available only to the parties that are intended to obtain it.

Integrity: The assurance that exchanged information has not been tampered with while on transit from the sender.

Non-Repudiation: The assurance that an action has been performed by a specific principal, who can not deny this action.

Quality of Service: The ability to guarantee a certain level of performance to a user, application or data flow.