

WEB-SERVICES ARCHITECTURE FOR PERVASIVE COMPUTING ENVIRONMENT

N. A. Malik and A. Tomlinson

Information Security Group, Royal Holloway, University of London, Egham, Surrey, UK.

Corresponding Author: Nazir.Malik@rhul.ac.uk

ABSTRACT

With the ever increasing shift towards pervasive computing to provide better services to the user based on the user's context and location of the user, there is a need for the development of secure architecture for ubiquitous computing. The paper reviews few existing security architectures and then proposes web-services architecture for pervasive computing. A number of solutions have been proposed in the literature including open source protocols to implement the security in pervasive environment. However, most of the proposed architectures rely on the intermediate servers to securely transfer data and communication between end user. This might be a suitable in certain scenarios but the broad range of users is not comfortable to accept and deploy such solutions. End-to-end secure communication between users is a key for the communication protocol to be considered for deployment by broad range of users. The paper presents a web services architecture for pervasive computing environment using open standards to implement a secure architecture.

Keywords: Web services; SAML; Pervasive Computing; Web Services Security; Authentication Assertions;

INTRODUCTION

The ability of smart devices and smart applications to identify current operating conditions or context and adapt their behavior on the basis of the context is termed as context awareness. With the fast pace development of new computing paradigms, the vision of ubiquitous / pervasive computing is becoming a reality into our daily lives. The implementation of context awareness in context-aware computing is a vast concept that encompasses all possible parameters identifying a particular situation. The applications and frameworks are being defined to identify context and relevant parameters limited by their scope. As its an emerging technology, a number of challenges in context aware computing paradigm exist which need to be addressed to make pervasive computing a reality. Due to heterogeneous nature of the pervasive computing and ubiquity of communication devices, service adaptation is required during run time (Malik *et al.*, 2007). The entities involved in a context setting include the persons, the objects and the computing resources present in the environment (Dey *et al.*, 1999). Humans being a very complex architecture are quite successful at conveying their thoughts to each other in an implicit natural way. This is because humans communicate through rich languages as well as gestures and expressions. Modern ubiquitous computer systems lack an automatic mechanism of inferring information like humans do. By improving the ability of computers to gather context and infer it, the richness of communication in human-computer interaction increases that results in a more powerful and more useful

computational environment.

To realize the development and deployment of pervasive devices, the design of secure pervasive architecture encompassing security in all aspects is paramount. The final realization of pervasive environment, in which each device communicates with other device seamlessly without user intervention, non-intrusive authentication and encryption mechanism, needs a considerable amount of time because of various standards and protocols being implemented in wireless devices. The limitation of bandwidth, memory and processing powers of mobile devices pose another challenge for implementing authentication and encryption mechanism in each mobile device.

This paper is in continuation to our work for developing a secure pervasive environment in an enterprise network. A number of solutions have been proposed in the literature including open source protocols to implement the security in pervasive environment. However, most of the proposed architectures rely on the intermediate servers to securely transfer data and communication between end user. This might be a suitable in certain scenarios but the broad range of users is not comfortable to accept and deploy such solutions. End-to-end secure communication between users is a key for the communication protocol to be considered for deployment by broad range of users.

RELATED RESEARCH

A security by contract architecture (SxC) is proposed by (Dragoni *et al.*, 2007), based on the mobile contract which a

mobile download carries with itself. It proposes layered security architecture for pervasive services and discusses the threat and mitigation services for corresponding threats and interaction modalities for security services layer. Another approach to address the problem of security in personal network is proposed in (Jehangir *et al.*, 2006). The solution is tailored based on the needs of constrained devices and wireless communication. It focuses on the pair-wise keys for secure cluster formation and group keys for intra cluster communication. It uses the group authentication for increased efficiency and security agents to authenticate the devices in the system.

In case of context sensitive environment, the concepts needs to be more tailored to the devices which communicate and update themselves. In pervasive environment, the security framework needs to be context-sensitive also (Pigeot *et al.*, 2007). It proposes a modular security environment integrated with PerSE architecture which enables a user to define privacy and security policy in pervasive environment. The modular approach provides security and privacy at different levels i.e. message filter and resource access filter.

The services being provided in the pervasive environment needs the secure mechanism for access control also. Team-based access control (TMAC) proposes a RBAC for collaborative environments (Thomas, 1997). It addresses the issue of access control to the collection of users in specific roles to accomplish a specific task. In pervasive environment, the collaboration between the enterprise colleagues to achieve a single goal working as a team while maintaining the secure environment and privacy of personal data is also very important for effective implementation of the system. The use of security-relevant context to provide access control is proposed in (Covington *et al.*, 2002). It provides architecture for authentication service, access control and adaptable security system based on current context in the environment. An architecture is proposed based on current status in combination with ideological and security mechanisms in (Liu *et al.*, 2006). The inherent nature of the pervasive devices to communicate seamlessly with each other requires extensive code execution, which also needs to be considered and catered for. Hybrid method of code analysis and component composition techniques is described in (Llewellyn-Jones *et al.*, 2004).

WEB SERVICES SECURITY

We have chosen eXtensible Markup Language (XML) (Bray *et al.*, 2008) as standard for exchanging information between the devices in pervasive environment. XML provides a standard to describe, communicate and implement the web services architecture. In contrast to other programming languages which focus on processing and actions, XML focuses on contents and objects. XML is structured as self-describing way to represent data that is

totally independent of application, protocol, vocabulary, operating system, or even programming language. SOAP (Gudgin *et al.*, 2007) provides platform independent and also data independent service interfaces. SOAP transports XML from one computer to another via a number of standard transport protocols. SOAP itself is defined using XML, and it provides an extensible mechanism that allows one application to send an XML message to another. After defining the contents of a message in XML, SOAP moves the data from one place to another over the network. It allows the sender and receiver to support common data transfer protocol. Universal Description, Discovery and Integration (UDDI) provides a way to discover the provider and services being offered by those providers (Clement *et al.*, 2005). Web Services Description Language (WSDL) provides interfaces to Web Services. It is also an XML language that defines the set of operations that a service provides and the structure of their related SOAP messages. XML defines SOAP, UDDI and WSDL (Christensen *et al.*, 2001). The relative links between all these related technologies are shown in Fig. 1.

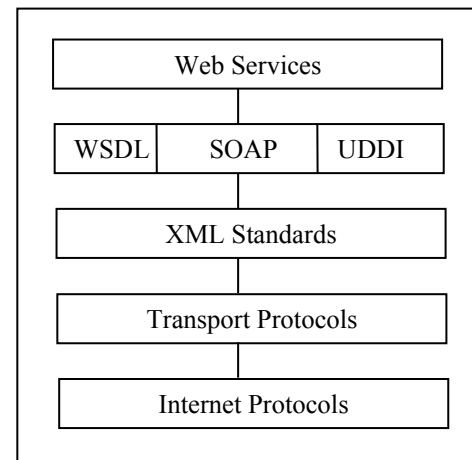


Fig. 1. Web Services Technologies

To provide security related mechanism using XML, we have chosen Security Assertion Markup Language (SAML) to communicate user authentication, authorization and attributes information. The underlying assumptions and reasons to choose these technologies are as follows:

- There exists a trusted Third Party in the system, which provides the corresponding SAML assertions to each individual user.
- SAML assertions are in the form of XML Schema so it's easy to implement in heterogeneous environment even. SAML assertions can also be useful for scalability of the system at later stage.
- SAML assertions provide the data about authentication, authorization and attributes.

- The assertion represents that the entity holding the assertion is recognized by the TTP for corresponding assertions e.g. the authentication assertion represents that the entity has been authenticated.
- The receiver of the SAML assertions checks whether the receiver trusts the TTP and thereby accepts the assertions as true or otherwise.
- SAML assertions can also work with XML signatures, XML encryption, HTTP, XMPP and SOAP specifications.
- The users are first registered with the TTP and TTP assigns them the SAML Assertions.
- SAML assertions can also be used by the applications which are not communicating using Web Services even.

PROPOSED ARCHITECTURE

The final implementation of pervasive environment involves the use of devices by average users and not only by researchers. The implementation of security schemes need to be transparent to the end user. A number of security technologies are already available on almost all layers of protocol stacks. The implementation and configuration of these schemes are already complex and the involvement of end user to configure and implement these schemes will make the pervasive environment vulnerable to a lot of security loop holes. A weak link in the environment might give a trust level to malicious user who can further use the resources as authorized user. Therefore, security schemes must be user friendly for deployment of security and building of trust.

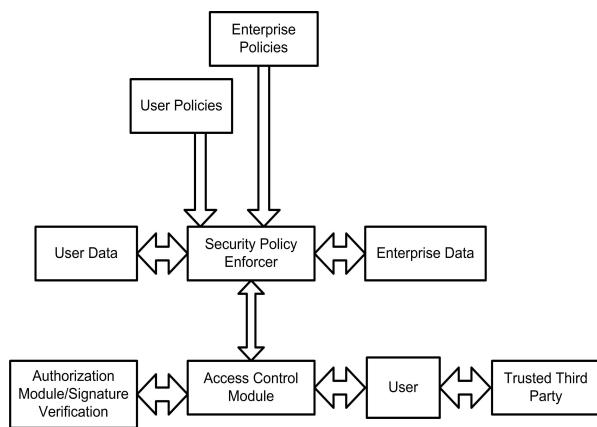


Fig. 2. Secure Pervasive Architecture

Registration and Assertions Module: Once a new user enters in the system, it needs to be registered with the Trusted Third Party (TTP) of the organization. Alternately,

the user may present his credentials from another TTP of his organization to get access tokens from the current TTP. In pervasive environment, the user can be part of multiple domains and if the user is having a trusted identity in one domain then his credentials may be used in any other domain which he is visiting. The concept of portable identity can be effectively utilized in the pervasive environment, where a user establishes a trusted identity in one domain by registering himself with a TTP and his credentials are available to be utilized to give him access rights in other domains. Once the user is registered with the TTP based on its present context or credentials from his parent organization. The user is assigned SAML assertions. The SAML assertions may contain Authentication, Authorization and Attributes of the user. The steps to register and give assertion are as follows:

- A new user enters the system with a new device.
- New device is registered with the TTP by registering user name, password and MAC address of the device.
- Attributes of the user are recorded to provide attribute assertion to the entities which require the confirmation of the authenticity of the user.
- Corresponding to authentication assertion and attribute assertions, authorization assertions are generated based on Enterprise's and user's policy at PDP (Policy Decision Point) and PEP (policy Enforcement Point).

Access Control Module: The function of the Access Control Module (ACM) is to check the authentication assertions before granting access to the user of the enterprise or user data. The SAML assertions are received by the ACM and it acknowledges the authentication credentials based on whether it trusts the TTP or not and thereby the assertions are regarded as true or false. Authentication assertions identify the user as the one who he claims to be. These credentials along with the attributes and authorization credentials are used to decide about the level of authorization assigned to the requesting user.

Authorization Module: After verifying the authentication credentials, ACM verifies the authorization data with Authorization Module to check the level of authorization based on authentication and attribute assertions provided by the requesting user. Authorization module grants the authorization levels depending upon the attributes of the user and its authentication level. The authorization assertions enable the user to perform specific actions in the visiting domain.

Security Policy Implementer: Security Policy Implementer (SPI) acts as Policy Enforcement Point (PEP) and Policy

Decision Point (PDP). After verifying the authentication credentials, ACM verifies the authorization data with Authorization Module to check the level of authorization based on authentication and attribute assertions provided by the requesting user. Authorization module grants the level of authorization based on authentication and attribute credentials.

If the SAML assertions are verified, ACM will approach the Security Policy Implementer. SPI builds dynamic security policies taking input from User Personal Privacy Policy and Enterprise Policy. Each user can define his personal privacy policy as to what amount of data; the user can share within enterprise or outside the enterprise. Enterprise security policy takes the priority over Personal Policy of the individual user in matters relating to Enterprise domain. The combination of User Policy and Enterprise Policy makes rules for SPI. Security Policy Enforcer allows the access to authorized data for which the user has been granted access by seeing his credentials and level of Trust. The following steps describe the overall functionality of the system:

- ACM receives the new contact's ID including SAML authentication assertions from the new contact.
- ACM verifies the SAML assertions of the new contact by checking whether it trusts the TTP.
 - If the user trusts the TTP, it will take the assertions as assurance of authentication of the user.
 - If the user doesn't trust the assertion provided by the TTP, it can refuse the connection with the incoming request.
- If the user trusts the TTP, it will check the attributes of the user by passing authentication assertions to the TTP.
- TTP will return the guaranteed correct attributes of the new user corresponding to the authentication assertions.
- ACM will pass on the authentication and authorization attributes to local authorization service. (An external SAML authorization service can also be used similar to SAML authentication service to check whether the user requesting particular service is authorized to perform specific operation or is eligible for particular service).
- Once the user is authorized by the SAML authorization service for the use of a particular service, it will allow the requesting user the authorized services.

CONCLUSION

Pervasive computing research field is still in its infancy and a lot of research efforts needs to be done to see the actual

implementation of real pervasive environment. A lot of focus is being given on the service discovery, context acquisition, context categorization and context modeling in context aware computing. Web services are used for integrating information sources from both inside and outside an enterprise. Web services are simpler, standards-based, and more loosely coupled technology for connecting data, systems, and organizations. Although security schemes are derived to be implemented in the pervasive environment but they are being implemented into already existing pervasive computing architectures. No generalized architecture exists in pervasive environment therefore schemes are implemented differently in each case. The paper presents a web services architecture for implementing security in pervasive environment using standard based technologies which are widely used and implemented.

REFERENCES

- Bray, T., J. Paoli, C. M. Sperberg-McQueen, E. Maler, F. Yergeau (2008). Extensible Markup Language (XML) version 1.0, Fifth Edition, W3C Recommendation.
- Christensen, E., F. Curbera, G. Meredith and S. Weerawarana (2001). Web Services Description Language (WSDL) version 1.1, 15 March 2001.
- Clement, L. A. Hatley, C. Riegen and T. Rogers (2005). Universal Description, Discovery and Integration (UDDI) Standard. February 2005.
- Covington, M. J., P. Fogla, Zhan, Z. and M. Ahamad (2002). A Context-Aware Security Architecture for Emerging Applications. In: Proceedings of 18th Annual Computer Security Applications Conference, Las Vegas, Nevada, USA. 249.
- Dey, A. K. and G. D. Abowd (1999). The Context Toolkit: Aiding the Development of Context-enabled Applications. In proceedings of Conference on Human Factors in Computing Systems, Pittsburgh, USA. 431-441.
- Dragoni, N., F. Massacci, C. Schaefer, T. Walter and E. Vetillard (2007). A Security by Contract Architecture for Pervasive Services. In proceedings of Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Istanbul, Turkey. 49-54.
- Gudgin, M., M. Hadley, N. Mendelsohn, J. Moreau, H. F. Nielson, A. Karmarkar, Y. Lafon (2007). SOAP version 1.2, W3C Recommendation.
- Jehangir, A. and S. M. Heemstra (2006). A Security Architecture for Personal Networks. In Third Annual International Conference on Mobile

and Ubiquitous Systems - Workshops, San Jose, California, USA. 1-8.

Liu, Y., F. Li (2006). PCA: A Reference Architecture for Pervasive Computing. In: Proceedings of 1st International Symposium on Pervasive Computing and Applications, Urumqi, China. 99-103.

Llewellyn-Jones, D., M. Merabti, Q. Shi and B. Askwith (2004). A security framework for executables in a ubiquitous computing environment. IEEE Global Telecommunications Conference, Dallas, Texas, USA . 4: 2158-2163.

Malik, N. A., U. Mahmud, and M. Y. Javed (2007). Future Challenges in Context Aware

Computing. In Proceedings of WWW/Internet 2007, Villa Real, Portugal. 2: 306-310.

Pigeot, C., Y. Gripay, M. Scuturici and . Pierson (2007). Context-Sensitive Security Framework for Pervasive Environments. In proceedings of Fourth European Conference on Universal Multiservice Networks, Toulouse, France. 391-400,

Thomas, R.K. 1997. Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments. In: Proceedings of the 2nd ACM workshop on Role-based access control, Fairfax, Virginia, USA. 13-19.