



Compression internet access methods of Universities in Turkey

Mirsat Yeşiltepe *, Mathematical Engineering, Yıldız Technical University, Davutpasa Campus, Istanbul, Turkey.

İrem Yılmaz, Mathematical Engineering, Yıldız Technical University, Davutpasa Campus, Istanbul, Turkey.

Muhammet Kurulay, Mathematical Engineering, Yıldız Technical University, Davutpasa Campus, Istanbul, Turkey.

Suggested Citation:

Yeşiltepe, M., Yılmaz, İ. & Kurulay, M. (2015). Compression internet access methods of Universities in Turkey. *Global Journal of Computer Sciences*. 5(2), 68-73.

Received 12 July, 2015; revised 18 August, 2015; accepted 26 September, 2015.

Selection and peer review under responsibility of. Prof. Dr. Doğan İbrahim, Near East University, Cyprus.

©2015 SciencePark Research, Organization & Counseling. All rights reserved.

Abstract

Which enables a user to specific conditions required by the relevant system that lets users connect to determine if the user is defined is the concept of authentication [1]. The authentication uses is very wide[2][3]. One of these is the use of accessing internet. Only certain users can use the generated web service objective in this area it is. The aim of this study was to compare students and staff in universities in Turkey internet access methods. The data were generated by contacting the university. In this way, universities can not work on which of the authentication methods they use to access the Internet, the use of which for the main purpose of the method of talking about the advantages and disadvantages of the university is to find out better.

Keywords: active directory, authentication, kerberos, XML

*ADDRESS FOR CORRESPONDENCE: **Mirsat Yeşiltepe**, Mathematical Engineering, Yıldız Technical University, Davutpasa Campus, Istanbul, Turkey. E-mail address: mirsaty@yildiz.edu.tr

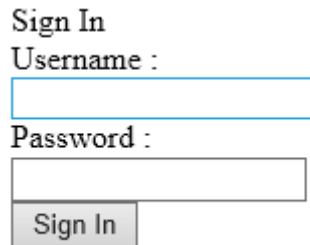
1. Authentications

Authentication which means verification of defined information in the system in order to performing certain operations and introducing user itself to the system. Firstly, user's credential is checked. If credential matches then process is completed and the user is authorized to access.

Credential is in order to verification of identity there is a requirement that includes interaction with trusted third party every time. Principals have to carry proof of their identity which is in the form of credentials with the aim of reducing that interaction [4].

2. Form Authentication

Form authentication is the whole process that takes credential informations and compares them with user information which are held database, XML, web.config or Active Directory through an entry form provided by an application. Standards html form fields are used to get the username and password values from the server [5]. Server validates the credential and then session is created. When the user clicks "log off" or the server logs the user off, the session will be invalidate. When the user is logged again, the prior session will be re-valid [6].



Sign In
Username :

Password :

Fig 1. Form Authentication Example

3. Windows Authentication

Windows authentication is the default authentication system for ASP.NET. The security of user computer is very important. When the user log in system once, the value of username and password wont requested again therefore machine should not leaved open. There is four way to windows authentication.



Fig 2. Windows Authentication Example

3.1. Anonymous Authentication

IIS allows any user.

3.2. Basic Authentication

Access with username and password values that are sending via network.

3.3. Digest Authentication

Same as basic authentication, but the credentials are encrypted. System works in the Active Directory structure. Secret information is not directly sent to opposite side via the communication line. After transferring various algorithms determined by client and servers, it is sent to opposite side. If value sent by the client and value calculated by server are equal, it means that user has entered true username and password. Authentication is made by this way without offering username-password window. This method is open to attack type which is called replay-attack. This can be prevented by the use of SSL.

3.3.1. Active Directory

Active Directory is an improved system for managing network resources. Directory is an information resources contains informations about objects. Information about files and folders is kept with creating directory. Active Directory objects particularly represent network resources including users, groups, computers and printers. Users want to find and use these objects. System administrators also want to manage these objects. Active Directory is a system that is developed for meeting both requirements.

3.3.1.1. Advantages of Directory Service

Centralized Administration: Through Active Directory, management can be done as center from single point without importance of distance and location of resources and users.

Multimaster Domain Controller (DC): Each DC has a feature that can receive the master server role. Features of opened a DC can be modified from another DC and this change can be updated to the other DC computer.

Scalability: According to the domain structure, Active Directory can be enlarged as desired. It can contain millions of objects in a domain.

3.4. Integrated Windows Authentication

Relies on Kerberos technology, with strong credential encryption [7].

3.4.1. Kerberos Technology

Kerberos Technology is an authentication protocol that uses a trusted third party arbitrator. Arbitrator is key distribution center (KDC). KDC produces random keys for servers and software systems. User enters username and password in client. Client applicates one way hash algorithm in user's password. This is secret key of client. The client sends username and domain information to authentication server. Authentication server checks whether the client is in its database. Secret key is encrypted as special ticket called Ticket-Granting Ticket (TGT) to send it back. The client receives the encrypted TGT involving key. If the client know and succesly solves, it can offer ticket to Ticket Granting Server (TGS) by encrypting with adding session key. Then, TGT publishes a new ticket that provides the use of a specific system or service.

Use of Kerberos prevents the transmission as plain text in network of passwords. Kerberos system facilitates the preservation and management of username and password information. In addition, it eliminates obligation to keeping the server of password information.

4. Comparasion of Form Authentication and Windows Authentication

Unlike windows authentication, form authentication allows for adding other providers. For example, accounts such as google, linkedin, live-id can be tied in with other accounts[8]. Form authentication will be a great choice when you are administrating your own authentication process by using a back-end database and a custom page. [9]. However, Windows authentication is useful for case that you create a web application for a limited number of user with Windows account. Furthermore, while identifying users without creating a custom page is possible at windows authentication, identifying users with a custom database provided by forms authentication. In addition, exactly one user can log in from one computer in the windows authentication. For different user, settings have to be rebuilt. Username is valid for all sites in use of windows authentication. However, in the form authentication, different users can connect from the same computer without any setting requirements.

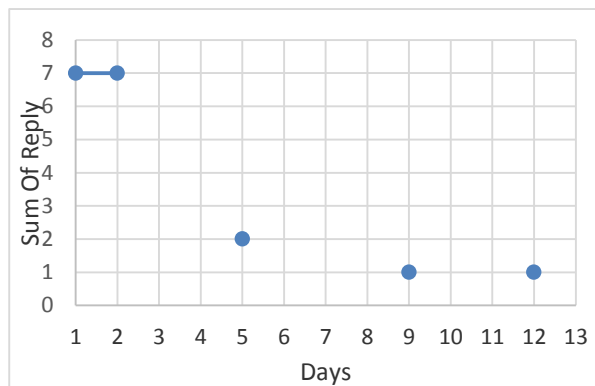
5. Testing

In this study, test procedure is asking the univercities in the list [10] with their formal e-mail adresses about staff and students of the universities how they access to the Internet in the Univercities which are in Turkey. Choosing one of the options from the relevant forms authentication or Windows authentication is requested. A question hasn't been asked about authorization because it was out of scope. Starting testing date is 01/10/2015 and finishing testing date is 19/10/2015.

Table 1. Classify Responses

Personel		Student	
Windows Authentication	Forms Authentication	Windows Authentication	Forms Authentication
15	7	14	8

Table 2. Frequency Of Responses



6. Conclusion

The result of the data discussed in table 1 and table 2 are as follows. Most responses weren't received from the university. Nearly %13 univercities send response. Some universities could not share this information in accordance with the scope of privacy. There had been delivery problem with some universities' email addresses, so no answer could be obtained from them. Thus, output of the study examined from small piece of data. But it can be give a view of whole data. Universities have no much difference the user class when they want to access Internet. So they use to authenticate to the staff have used the same for the students. Answers from the university is gradually decreased after the first few days, while the first and second day are many. Windows authentication is more used by Univercities than the other one. They wanted to use advantage of Windows authentication for ready infrastructure. Form authentication is more needed to prepare the infrastructure however when it is prepared it will have more advantages. Only one univercity have the opportunity that choosing windows authentication or forms authentication that can be best situation. If it is imposibble with some conditions, forms authentication must be choosen. Since the device which you access the internet can be use with another person, you must prepare the infrastructure again.

References

- [1]Bellare, M., & Rogaway, P. (1994, January). Entity authentication and key distribution. In *Advances in Cryptology—CRYPTO'93* (pp. 232-249). Springer Berlin Heidelberg.
- [2]Aziz, A., & Diffie, W. (1994). Privacy and authentication for wireless local area networks. *Personal Communications, IEEE*, 1(1), 25-31.
- [3]Bao, S. D., Zhang, Y. T., & Shen, L. F. (2005). Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. In *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the* (pp. 2455-2458). IEEE.
- [4]Tipton, H. F., & Krause, M. (2007). *Information security management handbook*. (6th ed.). Boca Raton, FL: 33487-2742
- [5]Ersoy, M. E. (2005). *ASP.NET güvenlik II form tabanlı güvenlik* [Security in ASP.NET II form based security]. Retrieved from: <http://www.csharspnedir.com/articles/read/?id=514>
- [6]What is the difference between basic auth and form based auth. (2012). Retrieved from: <http://kb.globalscape.com/KnowledgebaseArticle10691.aspx>
- [7]Windows authentication vs forms authentication. (2012). Retrieved from: <http://stackoverflow.com/questions/9443888/windows-authentication-vs-forms-authentication>
- [8] Difference between claim based authentication and classic windows authentication. (2014). Retrieved from: <http://sharepoint.stackexchange.com/questions/93018/difference-between-claim-based-authentication-and-classic-windows-authentication>

Yeşiltepe, M., Yılmaz, İ. & Kurulay, M. (2015). Compression internet access methods of Univercities in Turkey. *Global Journal of Computer Sciences*. 5(2), 68-73.

- [9]Yadav, A. (2013). *Windows authentication dot net security part 2*. Retrieved from:
<http://resources.infosecinstitute.com/windows-authentication-dot-net-security-part-2/>
- [10] Retrieved from: <http://www.yok.gov.tr/web/guest/universitelerimiz>

