Concerns Regarding Service Authorization by IP address using eduroam

Luzuko Tekeni, Kerry-Lynn Thomson and Reinhardt A. Botha
School of Information and Communication Technology
Nelson Mandela Metropolitan University
P.0.BOX 77000, Port Elizabeth 6031
E-mail: {Luzuko.Tekeni, Kerry-Lynn.Thomson, ReinhardtA.Botha}@nmmu.ac.za

***Abstract*—eduroam is a secure WLAN roaming service between academic and research institutions around the globe. It allows users from participating institutions secure Internet access at any other participating visited institution using their home credentials. The authentication credentials are verified by the home institution, while authorization is done by the visited institution. The user receives an IP address in the range of the visited institution, and accesses the Internet through the firewall and proxy servers of the visited institution. However, access granted to services that authorize via an IP address of the visited institution may include access to services that are not allowed at the home institution, due to legal agreements. This paper looks at typical legal agreements with service providers and explores the risks and countermeasures that need to be considered when using eduroam.**

***Index Terms*—eduroam, Authorization, IP-Based, Service Level Agreement**

I. Introduction

In the current generation, the number of users who connect to the Internet using mobile devices has increased significantly [1]. Most mobile users would like to get connectivity everywhere, including at home and at educational institutions. The TERENA (Trans European Research and Education Network Association) proposed a service for WLAN roaming between educational institutions and research networks [2]. This WLAN roaming service is called eduroam (EDUcation ROAMing). eduroam is a secure WLAN roaming service between academic and research institutions around the globe [3]. It provides users (researchers, teachers and students) with secure Internet access at any eduroam participating visited institution using their home credentials with minimal administrative overhead [4]. Institutions see eduroam as very beneficial, as the exchange of students and academic staff members between institutions is very common. These students and academic staff members can use their home institution credentials. In eduroam, the authentication credentials are verified by the home institution, while authorization is done by the visited institution [5]. The student or academic staff member receives an IP address in the range of the visited institution, and accesses the Internet through the firewall and proxy servers of the visited institution. However, access granted to services that authorize via an IP address of the visited institution may include access to services that are not allowed at the home institution, due to legal agreements. This paper explores the risks involved and looks at legal agreements with service providers when an institution uses eduroam.

The rest of this paper is organized as follows. Section II looks at the background of the eduroam service. Section III provides an overview of the eduroam service as well as its components. Section IV looks at the IP-based authentication process and the underlying problems that can be encountered when roaming between academic institutions. Section V illustrates the example of a legal agreement between a client and a service provider and provides a brief description of a possible illegal case. Section VI provide a discussion of some possible risks, their impact and possible controls. Finally, section VII concludes the paper and serves as an introduction to future work.

II. The origin Of eduroam

The eduroam service started as an idea of combining a RADIUS-based infrastructure with IEEE 802.1x protocol for roaming Internet access across institutions in Europe [6]. The actual eduroam service started in 2003 within TERENA's Task Force on Mobility, TF-Mobility [7]. During that time many institutions showed an interest in eduroam by joining. Those institutions were from the Netherlands, Finland, Croatia, United Kingdom, Portugal and Germany [8]. Gradually, other NRENs (National Research and Education Networks) in Europe began joining what was then named eduroam [1]. In December 2004, Australia became involved and was the first non-European country to join eduroam [9]. According to the eduroam website, eduroam "is now available in 68 territories worldwide" [10], but is only available at certain locations within those countries, as long as their NRENs have signed the eduroam Compliance Statement [11]

III. eduroam Service and Components

The eduroam infrastructure is based on hierarchically organized RADIUS proxy servers [12] and the IEEE 802.1x protocol [4]. This initiative makes use of three levels of RADIUS proxy servers, namely: Top-level server (Confederation), National-level server (Federation) and Institutional-level server (Edge) [3]. The Top-level server

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

acts as the bridge between National-level servers for global communication, while the National-level server is responsible for connecting institutions within the country. Every institution wanting to join eduroam connects to its National-level server and deploys a dedicated server for eduroam.

Figure 1 shows a user who wants to connect to eduroam at `institution_A` (visited institution), whose home institution is B (home institution). In this case, the users supplicant software contacts the Access Point (AP) using 802.1x with EAP (Extensible Authentication Protocol) protocol.

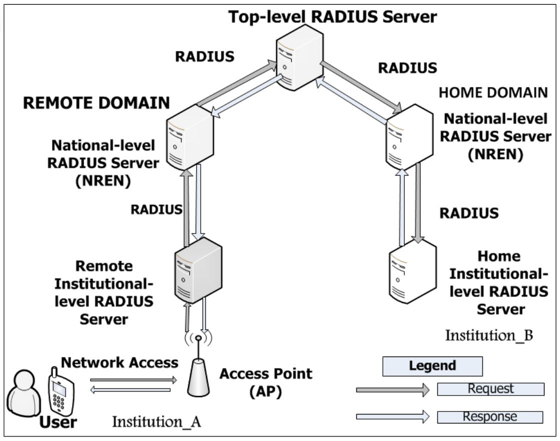


Fig. 1: eduroam infrastructure

The EAP protocol provides integrity and confidentiality to protect the transportation of user credentials throughout the hierarchy of RADIUS servers [13]. Then the AP contacts its local RADIUS server for authentication. The RADIUS server examines the realm part of the username, since it is not a local realm, then proxies the request through the hierarchy of RADIUS servers until `institution_B` is reached. `Institution_B` RADIUS server decapsulates the EAP massage and verifies the users credentials. It can either accept or deny the request by proxying the results in the reverse order using the same path. The AP at `institution_A` informs the user about the outcomes (accept or deny) and the connection is established (if the response is accept).

IV. IP-Based Authorization Process

Some services, such as digital libraries, at universities use an IP address to authorize users. This presents a potential problem when using eduroam. Figure 2 shows home and visited institutions and their service provider. In this example, before a user can be given any kind of access, the IP-based process for authentication and authorization must take place first. The user then roams between the two institutions using his or her home institutional credentials.

When the user reaches the visited institution and connects to eduroam, the following happens:

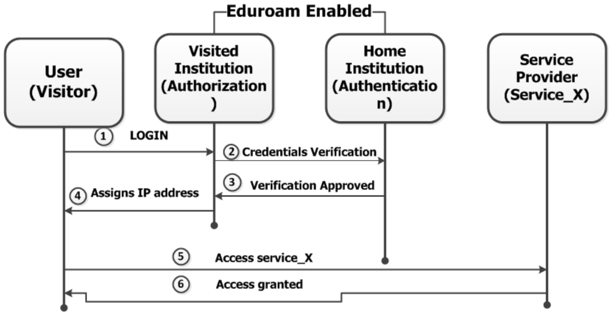

Eduroam Enabled
User (Visitor)
Visited Institution (Authorization)
Home Institution (Authenticatio n)
Service Provider (Service_X)
1 LOGIN
2 Credentials Verification
3 Verification Approved
4 Assigns IP address
5 Access service_X
6 Access granted

Fig. 2: IP-based process

1) The user tries to login at the visited institution using his or her home credentials.
2) The visited institution examines the realm part of the username and sees that the user belongs to the home institution, and then sends the user credentials through the hierarchy of RADIUS servers for authentication (verification) to the home institution.
3) The home institution decapsulates the message and verifies the users credentials, it can either accept or deny the request by sending back the response to the visited institution.
4) The visited institution receives the response and grants internet access if the results are positive (accepted), and assigns an IP address to the user.
5) The user accesses the service provider's resource (`service_X`) using the assigned visited institutional IP address.
6) The service provider verifies the validity of the IP address and gives permission to the user based on the provided IP address (visited institutional IP address).

This would result in an unauthorized user gaining access to certain services of the visited institution.

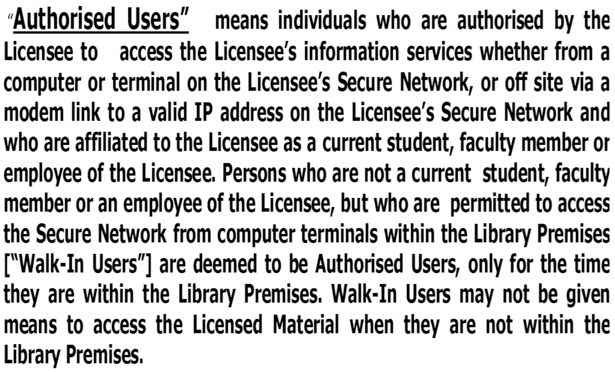
V. Case Description

This section is divide into two subsections, the first subsection looks at the legal agreement example which was extracted between the Nelson Mandela Metropolitan University (NMMU) and the Emerald Licence Agreement, and the second subsection explores illegal case based on the example provided in subsection V-A.

A. Legal Agreements

The increase and growth of the Internet and online services has forced organizations to outsource certain online services such as online databases [14]. When an organization outsources a particular online database service, a contract between the organization and the service provider is signed. This contract is called a Service Level Agreement (SLA) [15]. "SLA is a contract between a user and a provider of a service specifying the conditions under which a service may be used" [16]. Three of the Service Level Agreements were reviewed and all of them state a similar definition but one is used as an example below in figure 3. This was extracted from the

Consortium License Agreement between the Nelson Mandela Metropolitan University (NMMU) and the Emerald Licence Agreement.



"**Authorised Users"** means individuals who are authorised by the Licensee to access the Licensee's information services whether from a computer or terminal on the Licensee's Secure Network, or off site via a modem link to a valid IP address on the Licensee's Secure Network and who are affiliated to the Licensee as a current student, faculty member or employee of the Licensee. Persons who are not a current student, faculty member or an employee of the Licensee, but who are permitted to access the Secure Network from computer terminals within the Library Premises ["Walk-In Users"] are deemed to be Authorised Users, only for the time they are within the Library Premises. Walk-In Users may not be given means to access the Licensed Material when they are not within the Library Premises.

Fig. 3: Service level agreement

The main concept that needs to be highlighted in figure 3 is the "Walk-In Users" (visitors). According to figure 3 above, walk-In Users are only able to access Licensed Material from computer terminals within the Library premises. In other words the users must be within the physical premises of the Library, but this SLA is too antiquated because most users are using their mobile devices to access the wireless. This statement specified on the SLA needs to be reviewed by the authorities. eduroam users from another institution could breach the SLA if they accessed the Licensed Material from their own devices not on the Library Premises. The next section looks at this situation in more details of breaching the SLA through the introduction of eduroam.

B. *Illegal Access*

An illegal case can be defined as one of the two agreed entities breaking the agreement and this is often referred to as breaching the SLA [17]. In many cases the SLA is viewed from the service providers perspective. In other words, a breach would be constituted if the service provider cannot provide the level of service agreed upon for the customer to meet its goals [18]. Before eduroam, if a user visited a particular institution, he or she would be given a guest account. This would make the visitor known on the physical premises.

eduroam is advantageous in that it reduces the amount of work to be done by network administrators, allows easy and secure Internet access at any place around the globe. However many risks also came along especially to services that authorize via an IP address. The main focus of this paper is the concern of breaching the SLA to library services that authorize via an IP address when eduroam is implemented. Figure 4 below shows a situation when a user is at home institution using eduroam.

When the user accesses eduroam at the home institution and tries to access a service which the institution does not have access to, the following happens:

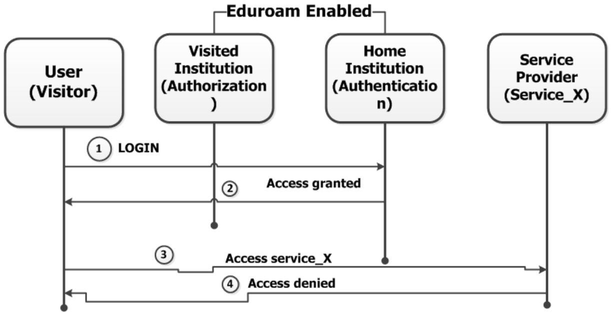

Eduroam Enabled
User (Visitor)
Visited Institution (Authorization)
Home Institution (Authenticatio n)
Service Provider (Service_X)
1 LOGIN
2 Access granted
3 Access service_X
4 Access denied

Fig. 4: eduroam access at home institution

1) The user tries to login at the home institution using his or her credentials and the EAP message is carried to the home server.
2) The home institutional server decapsulates the message and verifies the users credentials, sees that the user is the home user, assigns an IP address and grants Internet access.
3) The user accesses the service provider's resource (`service_X`) using the assigned IP address.
4) The service provider verifies the validity of the IP address and discovers that the received IP address has no subscription to access the service then denies access to the user.

If the user does not have access to `service_X` at home (home institution) but when visiting a particular institution that has subscription to the same service, the user is able to access that service without requesting authorization to it. Section V-A in figure 3 clearly states that "Walk-In Users"(visitors) are deemed to be authorized users only if they are using computer terminals or workstations within the Library Premises, meaning their presence is noticed. But the current eduroam infrastructure is lacking proper authorization mechanisms to those IP services and tracking of eduroam users.

VI. Discussion

eduroam is a new service that has been recently integrated to the existing networks in academic institutions and research networks in many countries around the world. Academic institutions and research networks have policies in place that govern how the access to the Internet services can be granted, now that eduroam is implemented possible risks arises. The subsections below take a closer look at the identified risks, the impact that they might have and as well as some possible controls that could be used.

A. *Possible Risks*

According to [19] [20], risk can be defined as the possibility of an undesired outcome or the absence of the desired outcome to a service. It "is a future event that may or may not occur" [19]. For this paper we explore the risks from different perspectives: the Users, Service Providers, and Libraries at universities. Each of these risk perspectives are described below:

Users: when users visit a particular institution, they could have access to services that they normally do not have when they are at their home institution. These users can be regarded as happy users because they have access to services that they are not subscribed to, but the users from the visited institution to the home institution could be faced with the challenge of not having access to services that they normally do when they are at their home institution, these type of users can be regarded as unhappy users. In this case, the situation can be seen as “unfair” to some of the users while others are enjoying the benefits of accessing services that are not available at home.

Service Providers: The service providers are the ones that are responsible to provide a particular service to the users. In this context, the service providers could find themselves in a position of losing their income when the users are accessing the service. In other words the user might visit the institution just to access the service that is unavailable while he or she is at home, on the other hand the user might unsubscribe to a particular service intentionally because he or she knows that the service is available to the neighbours and could just go and visit to access it, in this way the service provider might find themselves faced with a big challenge if the situation is not controlled.

Libraries: Many libraries at universities use an IP address to authorize users. This presents a potential risk when using eduroam. The eduroam user is given an IP address when visiting a particular institution which gives him or her access to services that are normally unavailable at home. This would result in an unauthorized user gaining access to certain services of the visited institution and the visited institution might find themselves breaching the SLA if these users access the Licensed Material from their own devices not on the Library Premises as stated on the license agreement in figure 3 above. Libraries therefore run a risk of being held legally liable.

Libraries also do not want to subscribe to unused (and therefore unnecessary) services. So if at `institution_X`, the librarian staff members are capturing their online database usage for the purpose of terminating the contract if an online database is not being used. Visitors accessing these databases through eduroam may lead to incorrect statistics captured. This could lead to the library not terminating the use of an online database. At first this risk may seem neglible, but it is worth remembering that services in this category (possible cancellation) is already little used-even a small number of visitors accessing could multiply the number of accesses thereby rendering the service in the expensive but needed category. There is no tracking of users and their activities in the current eduroam infrastructure and therefore it is impossible to assess the extent of visitor user access.

B. Impact

The impact helps to identify the probability of the risk, how vulnerable is the service to the identified risk and whether the immediate actions are needed or not. For each of the identified risks above, their impact is analyzed below.

Users: The impact on users could be positive or negative, depending on the specific circumstances. To understand this statement consider the South African Academic landscape. Table 1 below shows a comparison of digital libraries available at selected South African Universities and Research Institutes. Note that for brevity only a selected of the digital libraries at each institution is shown. As this is illustrative the names of institutions are not used. Selected institutions participate in eduroam in South Africa.

Comparison of eduroam Institutions			
Digital Libraries	Unit1	Unit2	Unit3
Access Engineering	No	Yes	Yes
Access Pharmacy	No	No	Yes
AccessScience	No	Yes	Yes
ACM	Yes	Yes	No
African Journals	Yes	No	No
Biomed Central	Yes	No	Yes
Emerald	No	Yes	Yes
IEEE Xplore	Yes	Yes	Yes
ISI Web of Knowledge	No	No	Yes
LexisNexis Academic	No	No	Yes
Sabinet	Yes	Yes	Yes
SAGE	Yes	Yes	Yes
ScienceDirect	Yes	Yes	Yes

TABLE I: Comparison of digital libraries at institutions

Based on the results shown in table 1, the risk varies depending on the institution that the user is visiting. For example, if the user visits the Unit1 from Unit3, that user can access the ACM database whereas at Unit3 he or she does not have access to the ACM database. While users from Unit1 will be very happy with the situation (as they have more access), users from Unit1 visiting Unit3 will be less happy as they do not have access to the database that he or she usually has when he or she is at the home institution.

Service Providers: Service providers will view this as a risk since it has a potential impact on their business. To some extent service providers are depending on the honesty of their clients that they provide the service to. If an authorization issues exist at the client side, the service provider is at risk. The situation needs to be controlled by the clients because if the service provider sets an SLA, there is no assurance that the clients will enforce the SLA effectively.

Libraries at Universities: Universities have thousands of users to manage, potentially including several visitors. Keeping track of registered users and visitors could be challenging in this environment. The advantages of eduroam infrastructure undoubtedly exceeds the possibility of misuse. This situation does not affect the institutions only, even the service providers are included, their service could be misused by the visitors because they know they are not paying for it, but maintaining access records on individual level rather than institutional level is certainly more costly.

C. Possible Controls

Even though a high-level analysis of risk involved may not identify major risk it is worth noting that possible controls may already exist to address this situation. While the situation needs to be further analysed, two ways are highlighted here.

One possible way of controlling the risks as described in subsection VI-A and their impact described in subsection VI-B, involves the use of a Virtual Private Network (VPN) tunnel. A VPN provides a complete data privacy and integrity for users who access the network from outside their Intranet in a secure manner [21]. For instance, by enabling VPN between the user and the home institution, a secure tunnel will be established. This will help to improve the IP-based level of security. In other words, adding another layer of security in the IP-based authorization process. Figure 5 shows how a VPN tunnel between the user and the service provider in eduroam network can address the risk of a user not having access to services when visiting institutions without access to the required service. However, this only address the risk from the perspective of a user not having access to something that he or she normally have and others. Refer to figure 2 for step one to three and step five to six for their descriptions; the fourth step improves the IP address that is normally assigned by the visited institution to access a service. Meaning the user will now make use of the tunnel being established to allow one-to-one communication rather than consulting the visited institution as it can be seen in figure 2. The benefits that the unauthorized user was enjoying will now be controlled by the tunnel.

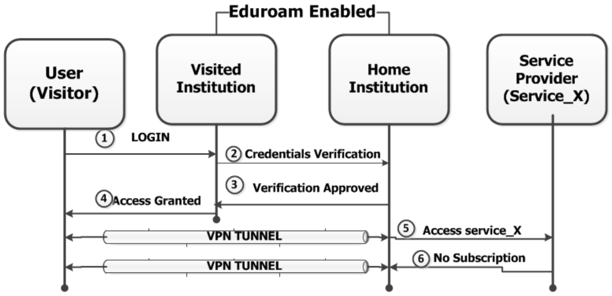


Fig. 5: VPN tunnel in eduroam

Since the issue here is really that of a users identity to be used across institutions, solutions may exist in the federated identity management space. A possible solution may be to introduce technologies such as Shibboleth, which will act as an intermediate third party between the home institution and the service provider on behalf of the visited institution as shown in figure 6 [22]. Figure 6 shows a high-level view of how Shibboleth could be used in eduroam.

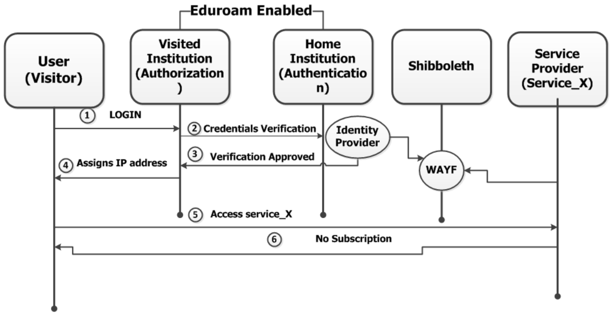


Fig. 6: Shibboleth in eduroam

A Where Are You From (WAYF) database will be used to identify the user and once that it is done, the service provider will be able to access the users attributes from the Attribute Authority (AA) at the user's home institution. The AA is the database that stores the attributes of the user located at the home institution under the supervision of the Identity Provider(IdP). Shibboleth will be able to identify services that are allowed at the home institution for the user, using SAML (Security Assertion Markup Language) [23] query request/response messages. This will, however, require service to evaluate SAML attributed to do authorization.

VII. Conclusion

This paper, discussed the origin of the eduroam service and its components. The eduroam initiative has proven to be more secure and scalable [7] by making use of a hierarchically organised RADIUS servers and IEEE 802.1x protocol with EAP protocol. eduroam is being used in many countries with many benefits and advantages. However, this paper argues that authorization can be a problem for services that do IP-based authorization. We analysed an example of an SLA between the NMMU and Emerald Licence Agreement to revealed that eduroam authorization potentially allows us to breach the SLA with some digital libraries (or other services) that authorize via an IP. The paper discussed possible risks and their impact. Finally some possible controls were mentioned. Future research will investigate possible solutions in more details. This will contribute towards securing services that authorize via an IP address in the eduroam service. While it may be argued that the risk is neglible, eduroam is growing, as more and more institutions and NRENs and their constituents are joining in. It may therefore be prudent to address this issue before the scale of eduroam turns a molehill into a mountain.

References

[1] K. Wierenga and L. Florio, "Eduroam: past, present and future," *Computational methods in science and technology*, vol. 11, no. 2, pp. 169–173, 2005.

[2] I. Yamaguchi, T. Suzuki, H. Goto, and H. Sone, "Centralized authentication system for location privacy protection and low operational cost of large scale wlan roaming," in *Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on*. IEEE, 2010, pp. 297–299.

[3] K. Wierenga, S. Winter, R. Arends, R. Poortinga, J. R. DFN, D. Simonsen, M. Sova, and M. S. DFN, "Deliverable dj5. 1.4: Inter-nren roaming architecture: Description and development items," *GN2 JRA5, GÉANT*, vol. 2, 2006.

[4] M. Milinović, J. R. DFN, S. Winter, and L. Florio, "Deliverable ds5. 1.1: eduroam service definition and implementation plan," 2008.

[5] Ó. Cánovas, A. F. Gómez-Skarmeta, G. López, and M. Sánchez, "Deploying authorisation mechanisms for federated services in eduroam (dame)," *Internet Research*, vol. 17, no. 5, pp. 479–494, 2007.

[6] TERENA. (2012) eduroam celebrates a decade of providing secure roaming internet access for users. [Online]. Available: http://www.terena.org/news/fullstory.php?news_id=3162

[7] Eduroam. (n.d) About eduroam. [Online]. Available: https://www.eduroam.org/index.php?p=about

[8] D. Olesen. (2003) Terena annual report 2003. [Online]. Available: http://www.terena.org/publications/files/terena_final_2003.pdf

[9] TERENA. (2004) Eduroam goes global. [Online]. Available: http://www.terena.org/news/archive/2004/newsflash163.pdf

[10] Eduroam. (n.d) Where can i eduroam? [Online]. Available: https://www.eduroam.org/index.php?p=where

[11] TERENA. (2011) eduroam compliance statement. [Online]. Available: https://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf

[12] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (radius)," 2000.

[13] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz *et al.*, "Extensible authentication protocol (eap)," RFC 3748, June, Tech. Rep., 2004.

[14] J. Huai, "Design service level agreements in outsourcing contracts," in *Management and Service Science (MASS), 2010 International Conference on*. IEEE, 2010, pp. 1–4.

[15] R. Schutz, S. McLaughlin, T. Daeleman, M. Luoma, M. Peuhkuri, P. Carlen, and J. Haines, "Protected core networking (pcn): Pcn qos and sla definition," in *Military Communications and Information Systems Conference (MCC), 2013*. IEEE, 2013, pp. 1–9.

[16] T. Sandholm, "Service level agreement requirements of an accounting-driven computational grid," *Royal Institute of Technology, Stockholm, Sweden, Tech. Rep. TRITA-NA-0533*, 2005.

[17] Z.-Z. Yau, "Design of sla management framework with case," 2005.

[18] A. Aleem and C. R. Sprott, "Let me in the cloud: analysis of the benefit and risk assessment of cloud platform," *Journal of Financial Crime*, vol. 20, no. 1, pp. 6–24, 2012.

[19] E. S. Chia, "Risk assessment framework for project management," in *Engineering Management Conference, 2006 IEEE International*, Sept 2006, pp. 376–379.

[20] P. Smith and G. Merritt, "Proactive risk management: Controlling uncertainty in product development. 2002."

[21] S. Rangarajan, A. Takkallapalli, S. Mukherjee, S. Paul, and S. Miller, "Adaptive vpn: Tradeoff between security levels and value-added services in virtual private networks," *Bell Labs Technical Journal*, vol. 8, no. 4, pp. 93–113, 2004.

[22] M. Erdos and S. Cantor, "Shibboleth architecture draft v05," *Internet2/MACE, May*, vol. 2, 2002.

[23] S. Cantor, I. J. Kemp, N. R. Philpott, and E. Maler, "Assertions and protocols for the oasis security assertion markup language," *OASIS Standard (March 2005)*, 2005.