IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. II (Jul.-Aug. 2016), PP 63-69
www.iosrjournals.org

A Structured and Layered Approach for a Modular Electronic Voting System: Defining the Security Service and the Network Access Layers

Emeka Reginald Nwogu[1] Chinedum E.Ihedigbo[2]
[1]*Michael Okpara University of Agriculture, Umudike*
[2]*Computer Science Department Michael Okpara University of Agriculture, Umudike*

Abstract: *This is the second part of the series of works that attempt to solve the problem of non-modularity in electronic voting systems. The work analyzed the second layer (Security Service layer) of our proposed structured and layered model. The Security Service layer was split into two sub-layers, namely; the Security control &application and the Security infrastructure sub-layers. A complete definition, description and detailed analysis of these sub-layers together with the components and modules that sit in the sub-layers were done. The work identified the Voter authentication module, the Device authentication system and the Information encryption module as the components/modules that are seen in the security control & application sub-layer, while the Token processing system and the Biometric security system were the identifiable components in the security infrastructure sub-layer.*

Keywords: *E voting, Electronic voting, Layer, Modular, Security Service*

I. Introduction

For an electronic voting system to be effective and reliable, security of the system should be taken very seriously. Adida (2006) explained the importance of security in electronic voting; he posited that systems used in electronic voting require a higher level of security than e-commerce systems. Thus e-commerce level of security will not be good enough for e-voting systems. Nwogu Emeka Reginald (2015) pointed out that there have been such issues as tampering with system's configuration in order to manipulate the election results together with threats posed by insiders (electoral officials). Kohno et al (2004) listed privacy issues and double voting problems as some of the major issues plaguing the deployment and use of the electronic voting system. In designing a modular electronic voting system, care is taken to ensure that the security of the system in the entire process is not traded off. Good security architecture will make it possible for electronic voting system engineers and maintenance technicians to scale up the system and even change components and modules of the system without any major challenge.

A well defined and structured security layer is also key to ensuring that the whole electronic voting system is well protected from the activities of fraudsters and desperate politicians who may want to manipulate the system through mischievous means to their own favour in an election. A good security layer definition and description will help in managing and maintaining the individual components of electronic voting security without haven to overhaul the whole security architecture.

Similarly, a well structured and defined network layer infrastructure is essential to a modular electronic voting system. Designers can adapt the electronic voting system network access layer to a technology that works in a particular place or country. While the use of VSAT architecture may prove the most viable and feasible Network Access infrastructure for some countries, the use of data service of the telecommunication system may be the choice technology in some others. There is also the choice of a fibre optic connection which would be a rather expensive implementation. Secondly, some other implementations may be a Virtual Private Network (VPN) connection, where the connection is set up specifically for the electronic voting system; others may as well be implemented on the public internet with strong security as in the case of the Estonian electronic voting system (Drew et al., 2014). This work is a continuation of the previous work that attempts to solve the problem of non-modularity in the electronic voting systems. It continues discussion on the analysis of an electronic voting system from a structured and layered perspective. The work defined in details, the modules and components that sit in Security Service layer of the proposed layered structure.

II. Background

Olivier Domy (2010) has defined layering as the segmenting of an information system into modular, interdependent layers; each layer is then minimally tied to the other layers to form the complete system. The available electronic voting technologies have not been layered. Consequently, they are not very modular.

Layering has been applied in almost all aspects of computer and information technology. It has been applied in computer networking with the creation of the TCP/IP model by the United States Department of Defense (DOD) in the 1970s and the subsequent creation of the Open System Interconnection (OSI) model by the International Organization for Standardization (ISO) in 1984 (Todd Lammle, 2009). The introduction of layering has greatly improved modularity and compatibility in computer networking. Manufacturers can decide which domain of the networking equipment production they want to contribute in. Recall that we had listed the Application, the Security Service and the Network Access layers as the three layers of our proposed layered system (Emeka Reginald Nwogu and Chinedum E. Ihedigbo, 2016). We had also discussed the Application layer extensively in the first part of this series. This second part discusses in details the Security Service layer.

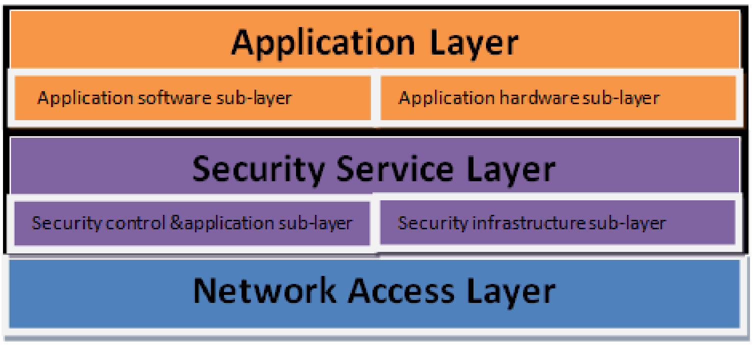
Application Layer
Application software sub-layer
Application hardware sub-layer
Security Service Layer
Security control &application sub-layer
Security infrastructure sub-layer
Network Access Layer

Fig 1: Complete layer model for the electronic voting system
Source: Emeka Reginald Nwogu and Chinedum E. Ihedigbo (2016)

Table 1 lists the different layers of the proposed architecture.

Table 1: Layers, sub-layers and components/modules of the electronic voting layered model
Source: Emeka Reginald Nwogu and Chinedum E. Ihedigbo (2016)

S/no	LAYER	SUB-LAYER	COMPONENTS/MODULES
1	**Application**	**Application software**	Client side module Tallying server module Voter information database module Election module
		Application physical	Client voting terminal Election server machine Voter database server machine
2	**Security service layer**	**Security control & algorithm**	Voter authentication module Device authentication system Information encryption module
		Security infrastructure	Token processing system Biometric security system
3	**Network Access Layer**		

III. The Security Service Layer

The security service layer is logically the second layer of the layered model. It is a logical second layer because the activity flow does not go chronogically from the Application layer down to the Security Service layer and then the Network Access. The activities flow horizontally severally between the Application and Security Service layers and sometimes the Network Access layer. This is a form of parallelism. This layer is divided into Security Control & Algorithm and Security Infrastructure sub-layers.

3.1 Security Control & Algorithm

3.1.1 Voter authentication module

The voter authentication module is concerned with the ways by which a prospective voter is authenticated with the voting system. It is the first to be called up by the client-side module at the voting terminal during a voter/system interaction. It controls the token processing system and the biometric security system, calling them up one after the other. The voter authentication is multi-factor which can be either two-factor or three-factor voter authentication. The standard is two-factor authentication for fast, ergonomic and secure voting experience. However, manufacturers and designers can also design systems with three-factor authentication based on the needs and specification of the voting system owners. Two-factor authentication is a security process where the user provides two means of identification, one of which is usually a physical token;such as a smartcard and the other usually something memorized such as security code or something one is, such as biometric information (Margaret Rouse, 2010).

Similarly, (Frogtalk technology news) defined three-factor authentication as security processes that require individuals to provide something they know such as security code or PIN, something they have such as token or smartcard and something they are such as biometric information. The voter authentication module is an important module in electronic voting. It authenticates prospective voters before they can complete the voting exercise. For a voter to be authenticated, voter authentication module first calls up the token processing system which reads and processes the voters'smartcard. The smartcard information is processed by the card processing server computer which checks for the validity of the card and returns the "voter information" if the card is valid or "voter not found information" if the card is invalid. Once the smartcard is confirmed valid, the voter authentication server opens a session with the voter information database where the voter information is pulled. Once the voter information is returned at the voting terminal, the voter authentication module calls up the biometric security system which prompts the voter to supply their biometric information. Similarly, for three-factor authentication, the voter authentication module would require the voter to supply a PIN once the smart card is read before calling up the biometric security system. This module is a software based module which runs on top of the client side module. It could be implemented with any object oriented third generation programming language.

3.1.2 Device authentication system

The device authentication system deals with the way the client voting terminal is authenticated with the servers. This ensures that only authorized voting terminals access the election server and voter database server machines; thus no cloned device can access the servers if good device authentication service is in place (Emeka Nwogu, 2014). In addition to this, the device authentication system ensures the security of the communication channel, making it impossible for any other device to transmit packets to the server. A number of technologies and architectures are available for implementing device authentication. Some implementation may require the two communicating devices to authenticate themselves without requiring a third party. This implementation usually would require the two communicating devices to share a secret, key or keys that are known to the two devices only. An example of such technology that requires no third party is Challenge Handshake Authentication Protocol (CHAP) which is specified in RFC 1994 (Wikipedia). Some other implementations may require a third party infrastructure to authenticate the communicating devices. This implementation would normally require a trusted certificate or ticket granted by the third party in order to authenticate the devices for communication to begin between them. Examples of technologies in this category are Public Key Infrastructure (PKI), Kerberos, Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+).

The most important thing is that the devices (voting terminals and servers) must be authenticated before they can communicate. The authentication system should also be a separate system that can be changed or upgraded without affecting conspicuously, the other functionalities, modules and components of the entire system. Designers are at liberty to choose any device authentication technology during their design implementation but this should be specifically a function of customer specifications and needs.Device authentication system also prevents against denial of service attacks, which are attacks that deny legitimate users access to essential services on servers by making these services unavailable to these users (Emeka Nwogu and McChester Odoh, 2015). Such denial of service attacks are perpetrated by zombie computers that have been compromised by an attacker's computer (Gunasekhar et al., 2014).

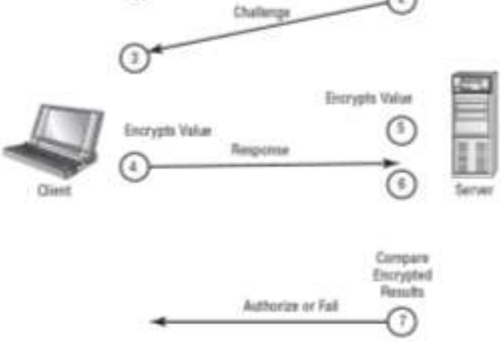

***Fig 2:** CHAP authentication process*
Source: Todd Lammle (2009)

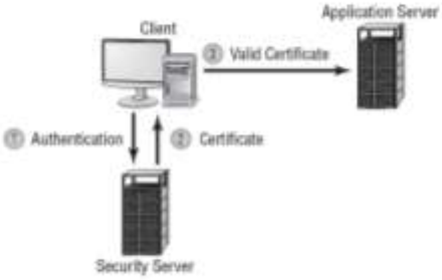

Fig 3: *Kerberos authentication process*
Source: Todd Lammle (2009)

3.1.3 information encryption module

The essence of the information encryption module is for the system to transmit secure information (ballots) from the voting terminals to the election server. It is concerned with making sure the electronic voting information (packets) travelling on the network from the voting terminal to the electronic server and vice versa is/are not intercepted by unscrupulous individuals.

Qingxiong et al. (2008) and Hyoungshick et al. (2012) discussed information security requirements. Security of the transmitted information is very important as this would ensure the election is not manipulated by unscrupulous politicians who want to win at all cost or corrupt electoral officials who aid and abet these unscrupulous politicians. Also, efficient securely transmitted ballots ensure the activities of black hat hackers who may want to cause national embarrassment or manipulate the electoral process and results to the advantage of some people are reduced to an insignificant minimum or possibly prevented. Internet Policy Institute (2001) listed a number of requirements including security requirements an electronic voting system should satisfy. The most important point here is that the ballot encryption module should be an integral module that can be changed without affecting the operation of the whole system. The easiest way to achieve ballot encryption is by cryptography. This may be symmetric or asymmetric keys cryptography. Ayushi (2010) discussed symmetric and asymmetric keys cryptography.

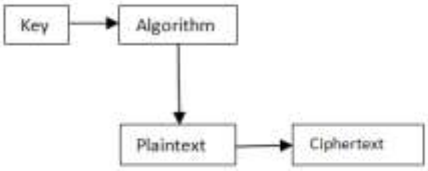

Fig 4: The encryption process

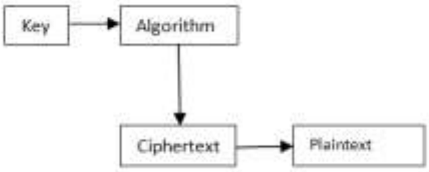

Fig 5: The decryption process

A number of symmetric and asymmetric keys cryptographic technologies are available for the implementation of this module. Some of the available technologies are Triple Data Encryption Standard, Blowfish, Diffie-Hellman, El Gamal, RSA and Elliptic Curve Cryptosystem. There has also been a suggestion of a ballot encryption technology that can allow the tallying of encrypted votes before decrypting the tallied votes as a group to reveal the result. Proponents of this school of thought Treball Final de Carrera (2014) and Sansar Choinyambuu (2009) argue that the technology increases the speed of result delivery as time is saved from tallying encrypted ballots as a group and later decrypting the tallied grouped ballots rather than decrypting the ballots individually before tallying. This is called homomorphism and can be seen in the Paillier Cryptosystem. An encryption technology is said to be homomorphic if given E(x) and E(y), one can obtain E(x ¬ y) without decrypting x; y for some operation ¬. (Sansar Choinyambuu, 2009). For homomorphic addition of plaintext, the product of two ciphertexts when decrypted will give the sum of their corresponding individual plaintexts as shown below.

$D\,(E(m_1,r_1).\,E(m_2,r_2) \bmod n^2) = m_1 + m_2 \bmod n.$

Similarly, the product of a ciphertext and a plaintext raising g when decrypted will give the sum of the corresponding individual plaintexts.

$D\,(E(m_1,r_1).\,g^{m_2} \bmod n^2) = m_1 + m_2 \bmod n.$

Also, for homomorphic multiplication of plaintext, an encrypted plaintext that has been raised to the power of another plaintext when decrypted will give the product of the two plaintexts as shown below.

$D\,(E(m_1,r_1)^{m_2} \bmod n^2) = m1\ m2 \bmod n$

Similarly, $D\,(E(m_2,r_2)^{m_1} \bmod n^2) = m1\ m2 \bmod n.$

3.2 Security Infrastructure

3.2.1 Token processing system

This system is responsible for the processing of the token (voter's card). It is the first to be called up by the voter authentication module. When token authentication is completed during voter authentication, control is transferred to the biometric security system. In authentication, a token refers to a small hardware device that the owner carries to authorize access to a network service (Margaret Rouse, 2005). This device may be in the form of a smartcard or a dongle.

The card reader reads data from the token (voter's card). The token provides the first level of authentication for the user. There are different technologies for coding voter information on a voter's card. Some of the technologies are barcode, magnetic stripe (swipe card) and smartcard technologies. While barcode and magnetic strip cards have been available for years, smartcard technology has gradually taken over the card technology industry.The smartcard is typically a type of chip card. It is usually a plastic card that contains an embedded computer chip, either a memory or microprocessor type that stores and transacts data Cardlogix corporation, 2010). The smartcard information is coded in the silicon chip on the smartcard. The various types of smartcards include contact cards (most common), contactless cards and the multi component cards. The Card Acceptance Device (Card Reader) is used to communicate with the smartcard. It reads the information on the smartcard and sends the information to a server computer for processing. The server computer extracts the card information together with the voter identification parameter(s). The voter identification parameter is subsequently used to query the voter information database in order to reveal the complete voter information. Once this is done, the voter authentication module now transfers control to the biometric security system for voter authentication to continue.

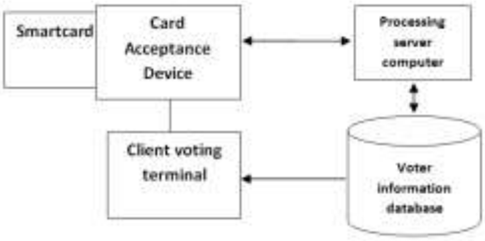

Fig 6: Macro-model of the token processing activity

3.2.2 Biometric security system

Anil et al. (2004) defined biometric systems as pattern recognition systems that function by acquiring biometric data from an individual, extracting a feature set from the acquired data, and thereafter, comparing this feature set against the template set stored in the database. biometric identifiers on the other hand are the distinctive, measurable characteristics used to label and describe individuals Jain Anil K. and Ross Arun (2008). The identifiers are often categorized as physiological versus behavioral characteristics (Jain Anil K. and Ross Arun, 2008). The typical biometric security system is used to add another level of security to voter authentication, making impersonation of voters somehow impossible. The voter authentication module calls up the biometric security system as the second level of authentication after the token processing has be completed successfully. According to Anil et al. (2004) a typical biometric security system would comprise the following modules;

1. The biometric sensor module (scanner or camera)
2. The Feature extraction module (processes the acquired sample to extract the minutiae from the sample)
3. The matcher module (compares the sample against the stored templates to generate matching scores).
4. System database module (used by the biometric system to store the biometric templates of the enrolled users).

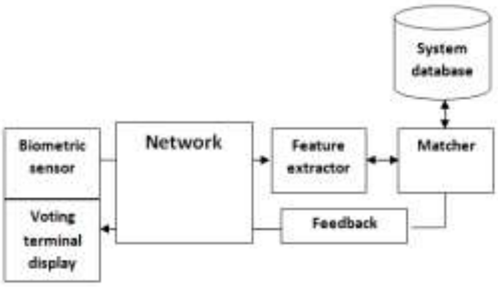

Fig 7: Macro-model of the biometric security system

During voter registration, biometric enrolment is done by every registered individual. In enrolment, a new user supplies their biometric information to the biometric system for storage in the system database. Subsequently, for authentication, a prospective voter supplies their biometric information to the biometric sensor which captures and transmits the captured biometric information to the feature extractor. The feature extractor extracts the minutiae from the biometric information and sends it to the matcher. The matcher pulls the stored template in the system database and matches the supplied biometric information (query) against the template. The matcher returns a match score representing the degree of similarity between the template and the query. The authentication succeeds if the degree of similarity reaches the threshold value. If not, authentication is denied.

All biometric information exchange in the biometric security system still has to go through the information encryption module. The biometric sensor module is attached to the voting terminal while the other module may reside at the server side of the electronic voting system network.

IV. Network Access Layer

The network access layer is the third and the last layer of the proposed layer structure. It is concerned with the transmission of voting information between remote sites in the electronic voting network. The remote sites may be the voting terminals and the election server, the election server and the tallying server or the election server and the voter database machine. The Network Access layer describes the set of protocols that guide voting information transmission together with the physical architecture of the electronic voting network.

The TCP/IP model developed in the 1970s by the United States Department of Defense grouped network protocols into four abstraction layers. All the implementations in the Network Access Layer of our proposed layered model map well on the second through the fourth layers of the TCP/IP model. The Application and the Security Service layers of our proposed model also map well on the Application layer of the TCP/IP model. Figure 8 gives a diagrammatic representation of the mapping between the TCP/IP model and our proposed layered architecture model.

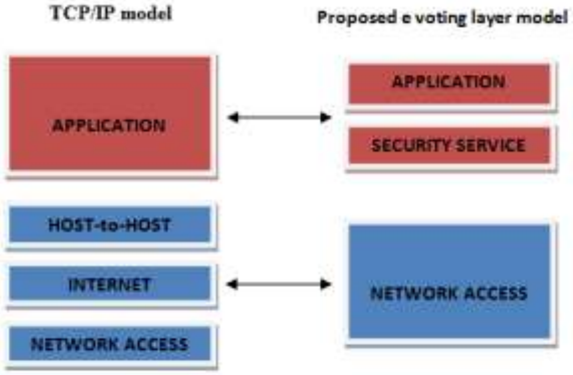

Fig 8: Associating the TCP/IP model with the proposed e voting layer model

Once the voting process leaves the Application and Security Service layers of our proposed model, control is transferred to the Network Access layer of the model. At the receiving station, the Network Access layer also receives the packet and passes it onto the Application and Security Service layers for further processing.

V. Conclusion

The security Service layer as discussed in this work is important in the electronic voting system. If it is well defined and structured, protecting the system against activities of hackers and election fraudsters becomes a lot easier. This work has discussed in details, the Security Service layer of our proposed model. We have listed the different sub-layers of the security service layer to include the Security Control & Algorithm and Security Infrastructure and have also discussed the components and modules that make up this layer. The work has made it possible to integrate security infrastructure from different vendors and with different technologies into the electronic voting system, ultimately resulting in a better, scalable and modular system.

References

[1]. Adida, B. (2006), Advances in Cryptographic Voting Systems. Electrical Engineering, Massachusetts Institute of Technology. Retrieved March 10, 2016 from https://dspace.mit.edu/handle/1721.1/38302

[2]. Anil K. Jain, Arun Ross and Salil Prabhakar (2004), An Introduction to Biometric Recognition, *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.*

[3]. Ayushi (2010), A Symmetric Key Cryptographic Algorithm, *International Journal of Computer Applications (0975-8887) Volume 1 – No. 15*

[4]. Cardlogix corporation (2010), Smartcard Basics. Retrieved March 17, 2016 from http://www.smartcardbasics.com/smart-card-overview.html

[5]. Drew Springall et al. (2014), Security Analysis of the Estonian Internet Voting System University of Michigan, Ann Arbor, MI, U.S.A., Open Rights Group, U.K.

[6]. Emeka Nwogu and McChester Odoh (2015), Security Issues Analysis on Online Banking ImplementationsinNigeria, *International Journal of Computer Science and Telecommunications [Volume 6, Issue 1, January 2015] ISSN 2047-3338*

[7]. Emeka Reginald Nwogu and Chinedum E. Ihedigbo (2016), A Structured and Layered Approach for a modular Electronic Voting System: Defining the Application Layer. Article in press.

[8]. Frogtalk technology news, 3 "Factor authentication: why you need it to protect your business," Retrieved Aug 15, 2014 form http://www.ribbit.net/frogtalk/id/121/3-factor-authentication-why-you-need-it-to-protect-your-business

[9]. Hyoungshick Kim, Jun Ho Huh and Ross Anderson (2012), "On the security of internet banking in South Korea

[10]. Internet Policy Institute (March 2001), Report of the National Workshop on Internet Voting, USA. Retrieved February 16, 2016 from www.worldcat.org/.../report-of-the-national-workshop-on-internet-voting.../225360688

[11]. Jain A., Hong L. and Pankanti S. (2000). "Biometric Identification", *Communications of the ACM, 43(2), p. 91–98. DOI 10.1145/328236.328110*

[12]. Jain Anil K., Ross, Arun (2008). "Introduction to Biometrics", *A. Handbook of Biometrics Springer. pp. 1–22. ISBN 978-0-387-71040-2*

[13]. Kohno T., Stubblefield A., Rubin A.D., and Wallach D.S. (2004), Analysis of an Electronic Voting System,*" Security and Privacy. Proceedings. 2004 IEEE Symposium on , vol., no., pp. 27-40, 9-12 May 2004 doi:10.1109/SECPRI.2004.1301313.* Retrieved December 12, 2015 from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1301313&isnumber=28916

[14]. Margaret Rouse (2005), Security Token. Retrieved February 11, 2016 from http://searchsecurity.techtarget.com/definition/security-token,

[15]. Margaret Rouse (2005), Two Factor Authentication. Retrieved Oct 10, 2014 from http://www.searchsecurity.techtarget.com/definition/two-factor-authentication

[16]. Nwogu Emeka Reginald (2014), Improving the Security of the Internet Banking System Using Three-Level Security Implementation, *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 4, No.6, December 2014*

[17]. Nwogu Emeka Reginald (2015), Mobile, Secure E - Voting Architecture for the Nigerian Electoral System *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. II (Mar – Apr. 2015), PP 27-36*

[18]. Olivier Domy (2010), Layering or the Modular Approach to Information Systems. Orange Business Services. Retrieved March 30, 2016 from http://www.orange-business.com/en/blogs/connecting- technology/data-centers-virtualisation/layering-or-the-modular-approach-to-information-systems

[19]. Qingxiong Ma, Allen C. Johnston and J. Michael Pearson (2008), Information security management objectives and practices: a parsimonious framework, *Information Management & Computer Security Vol. 16 No. 3, 2008 pp. 251-270 q Emerald Group Publishing Limited 0968-5227*

[20]. Sansar Choinyambuu (2009) Homomorphic Tallying with Paillier Cryptosystem *HSR Hochschule für Technik Rapperswil*

[21]. Todd Lammle (2009). CompTIA Network+ Study Guide. Wiley Publishing, Inc., Indianapolis, Indiana, ISBN: 978-0-470-42747-7Okediran et al. (2011), A Framework for a Multifaceted Electronic

[22]. Treball Final de Carrera (2014), Design and Implementation of an Electronic Voting SYSTEM Based on Homomorphic Tallying of Votes, Universidad de Lleida

[23]. T.Gunasekhar, K.Thirupathi Rao, P.Saikiran, P.V.S Lakshmi (2014), A Survey on Denial of Service Attacks, *International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2373-2376,*

[24]. Wikipedia,Challenge-Handshake Authentication Protocol Retrieved February 15, 2016 from https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol