Improved E-Banking System With Advanced Encryption Standards And Security Models

Sharaaf N. A., Haamid M.N., Samarawickrama S.S., Gunawardhane C.N., Kuragala K.R.S.C.B, Dhishan Dhammearatchi

Abstract: Emerging new Technologies and large scale businesses have made this world, a global village. Many business organizations provide online services targeting global consumer bases. Transaction in international scale has been enabled by banks all around the world through E-banking in order to supply the needs of above business organizations. E-banking serves lots of benefits to both customers of banks and banks itself. It adds value to customer's satisfaction with better service quality and enables banks to gain a competitive advantage over other competitors. Online banking need to possess high level security in order to provide safe, consistent, and robust online environment which guarantees secure data transmission and identity of both bank and customer. Lack of security may lead to less trust or hard to trust attitude towards online banking. Although customers are attracted by online banking convenience, they seem largely in concern about identity theft and phishing. Analysis of many research papers on e-banking security models and their respective advantages and disadvantages have been discussed in literature review. Username, password, E-banking dongles, fractal images, biometric scans and advanced encryption standards are some of the suggested solutions for E-banking security. This study focuses on the security beyond above mechanisms. This paper ensures security of online banking at three levels. At client side, using internet dongle integrated with finger print scanning technology, at banking sever side and data transmission level. This model also includes username, password and advanced encryption for further security. Complete description on the model has been discussed in methodology section. Future works on this topic and Conclusion are covered in separate sections.

Index Terms: E-banking, Phishing, Fractal image, Biometric Scans, Encryption, Finger Prints, Server Side

1 INTRODUCTION

Information Technology and Internet Networks have shown a tremendous development over past decades, which led to effective Electronic Commerce (E-commerce) activities at global level. Major goals of E-commerce are rapid and flexible information exchange and improved customer services to earn more trust. Banking industry provide E-commerce services through Electronic banking or online banking. Online banking offers value added services and convenience to its customers. It also allows customers to make financial transactions through the website of respective bank. Opening bank accounts, issuing credit cards, paying and getting loans and debts, facilitating online shopping and online bill payments through bank accounts are most common services offered by online banking sites. On the whole these systems enable customers to access their account, obtain information on the financial products, transfer money and utilize other offerings of banks. Online banking provides countless advantages for both banking industry and its users. It enables the customers to make huge transactions worth several millions or simple transactions worth few rupees in matter of seconds without visiting the bank physically. Thus customers have no need to wait in long queues to retrieve bank services. Online banking is ease of access and time serving. From banks perspective, saving can be made from reducing staff remuneration, branch office, and Automatic Teller Machine (ATM) and Electronic Funds Transfer at Point of Sale (EFTPOS) transaction maintenance budgets. Providing banking services with the necessary security from a remote location through the internet is a challenging process in banking sector. Probability of attacks increase with the advancement of online banking services. Billions of financial data transaction is conducted online every day. Thus not achieving a perception of security will have the wider effect of reducing customers' trust in internet banking as well as the bank. Skilled criminal hackers' carryout bank cyber-crime attacks everyday by manipulating the banks' online information system. Ensuring perfect security in online banking is hard to achieve target with rational client Personal Computer (PCs), which are not designed for secure internet commercial transaction. Many researches have reported that criminal attacks on internet banking have become more complex, particularly with the development of key logger software. Man-in the middle attacks is common attack of above type. This raises a strong argument about the effectiveness of the system that rely on trusting the client. Therefore, there is a need to ensure client, banking server and the path from client to banking sever are properly secured with security algorithms. Current internet banking models focus on identification rather than fraud prevention. Consequently, there is a need to develop a suitable system for E-banking security which enables needed security and solves the flaws identified in the current internet banking system. This research work suggests an E-banking security model to solve major problems encountered in current internet banking system. This model consists of E-banking dongle with finger print scanner to ensure true client and advanced encryption mechanism for financial data transmission. This paper is organized as follows: section 2, literature review on similar researches on E-banking security, Section 3, discussion on methodology and implementation of new security model, Section 4, Conclusion and Section 5, Future works.

2 BACKGROUND STUDY

In the current decade E –banking is growing very vastly over the world. Frauds in E-Banking transaction is a very big deal all over the world. There are many researches and studies going on to reduce E-Banking frauds and make way to a better banking transaction to the consumers. Thus, there are many technical and theoretical solutions have been proposed in many region of the world. When research team went through among the research papers the team found some solutions and ideas as follows, Use of username and password is a common and traditional way that helps to protect every transaction from the banking frauds as well as hackers. When a consumer needs to make a transaction, he/she should verify his/her identity with the use of username and password [1][3]. Researcher Hameed U Khan has proposed a technique which will maximize the security level of the transaction. The research paper contains that use of Secret picture/ Iris pattern will enhance the security level of the E – Banking transaction. It includes one-time passwords to verify the consumer whether he/she is the correct person or not. The user must enter the one-time password message and send it back to the server to begin the transaction [1]. Research claims a new technique called Three-level Security Implementation to provide a safe and reliable E-Banking solution. The Three-level Security Implementation contains 3 main areas such as security module, network module and control module. The security module includes another 3 kinds of separate modules such as user authentication module which will include a bio metric scan (Finger Print) and security pin verification to connect with the banking server. These details of the consumer will be encrypted and send to the Kerberos server. Consumer must use a separate dongle to communicate with the banking server. Once the details of the consumer received the server will check the encrypted details and mac-address of the e-banking dongle. When the verification is successfully completed the Kerberos server will allow the consumer to communicate with the banking server with the use of Transaction data security module [2]. K. Thamizhchelvi and G. Geetha have come up with an idea called Message Authentication Image (MAI) Algorithm saying that it will be a unique way to provide a safe transaction. The approach says that when the user enters his/her user name to start a transaction the server will generate and send a pass mark image to the particular consumer. If that image matches with the consumer's one, then server will allow the consumer to enter his password. The consumer needs to send his fractal image to the server. When both fractal image and password matches the server will allow the particular consumer to begin the transaction. The pass mark image is used to verify that the consumer is communication with the correct server and the fractal image is used to verify that the server is communicating with the correct user [3]. Kovach S.et.al shows a fraud detection system suggested for online banking that is based on local & global behavior in this research paper. Fraud detection contains in identifying such unofficial activity once the fraud prevention has failed. Among the methods used by fraudsters, "phishing". One is differential approach. What happens in there is the account usage design are monitored and related with the history of its usage, which presents the users normal performance. The second method is Global Analysis Approach. This is based on three expectations. First on is expected that each device is used for online banking has a single identification. The second assumption is based on the fact that the probability of a transaction being a fraud growth with the number of accounts accessed by the same source that requested the present transaction. The third assumption comes from the fact that the only way to know that a fraud has been committed is when the customer reports it. Authors of this research paper used "The Dempster's Rule" to come up with a resolution for this online banking fraud issue. The impression behind this research paper is approach comes from the fact that fraud doubt in a transaction growth with the number of accounts accessed from some bases [4]. Chen H.et.al defined the current online banking matters in this research paper. First one is people detect a lack of attention and research concentrating on security problems relevant to the clients' side of online banking system. The second problematic is there are many security goods used in online banking system. In this research paper author shows how testers may perform online banking security testing. Security technologies comprise algorithms, protocols, standards and mechanisms. Security testing can be performing both black-box and white-box testing to reveal possible software risks and potential deeds. This conformance testing is a form of black-box testing. Compliance testing has two main aspects. Most methods to security testing treat the implementation under test (IUT) as a black-box. Writers have planned a general procedure for building a compliance testing system for security [5]. Rocha B. C.et.al aims to evaluate the use of methods of decision trees, in conjunction with the management model CRISP-DM to assistance in the prevention of bank fraud. This research paper shields the field of artificial intelligence. The research paper is concentrated on discussing how these trees are able to support in the decision making method of identifying frauds by the analysts of information concerning bank transaction. The technique of study is called Decision Trees which discussed in in this paper and it is applied within a management model of data mining called CRISP-DM. CRISP-DM is The Cross Industry Standards Process for Data Mining. Business understanding's independent is to detect fraud from a fraud history log. After the execution of the model, the evaluation should check if those losses were reduced. Also that the business understanding phase risk assessment and the project plan must be developed with the next steps for executing the CRISP-DM process. What happens in the second phase is, the initial data should have collected and a description of this data must be produced, as well as a confirmation of its excellence. This is where the fraud history of the bank is synthesized with the mandatory attributes such as time of the fraud, the number of frauds and fraud types. Third phase is preparing data for use in the algorithms of decision trees. It is the phase to find calculated fields, incorporated external database, perform a good data cleaning and classify the attributes as inappropriate, categorical and numerical [6]. This research paper aims to improve the models adopted in online banking systems are based on several layers of security consist of multi mechanisms solutions and which aim at protecting the online banking applications and the user's data in the whole process, such as: existence of a public key infrastructure (PKI) and a certificate authority (CA) and which represents a trusted third-party who signs the certificates attesting to their validity. One-time password (OTP) tokens use of changing passwords dynamically which can be used only once. Device registers is to use hardware fingerprint technology with secret documents by user ID. It is use for pre-registered device only ,Completely automated public turning test tell computers and humans apart (CAPTCHA) model has been implemented to prevent automated scripts (Bots) from jamming registration or login page and this method requires the user and the legitimacy of the scrambled image into its automated robots to deal with it is difficult to input information .model of Short message service (SMS) is sending a set of characters to the user in order to have authorize ,process the transaction through the online banking system and Biometric authentication technology model is automated method to distinguish the customers through their biological characteristics, traits such as fingerprints, finger vein patterns, retina, and voice recognition. [7]. This research paper differs from other research papers because it is use for initial framework for governing the information security banking system. The framework is categorized into three levels which are strategic level, tactical, operational level, and technical level. Strategic Level framework includes the concepts of metrics and measurement to identify the effectiveness current information security governance program. This level refers to board of directors and senior executive management. Tactical

Level framework, monitoring, compliance, and auditing are also proposed as key components to manage the information security program. Tactical and operational level refers to senior managers and operation managers. Technical Level involves the technical and physical mechanisms implemented to secure an IT environment. When implementing security governance framework technology controls applicable to the organization’s environment and identified risks must be implemented [8]. This paper described solution options are SMS challenge code, Image verification, Dynamic Security Skins (DSS), PKI based software solution and PKI based hardware token. SMS challenge code is the user enters his account name into the spoofed web site, the attacker uses the received username, logs on to the real service and initiates the submission of the one-time password through SMS. One system that promises good user acceptance uses the user's registered mobile phone to receive an activation code. The user enters this challenge code into the browser and proves thus that he has access to the correct mobile phone. Image verification is user has already authenticated to the service a “Device ID” sent along with username. PKI based software solution & PKI based hardware token is using a PIN code on the external device’s keypad unlocks the key vault in the smartcard. A signed Java applet downloaded from the bank’s web site communicates with the card reader on one side and with the bank on the other. This applet authenticates itself against the card reader [9]. As a result of data Ahsanul Haque, Ahmad Zaki Hj Ismail and Abu Hayat Daraza have come up with a new trusted online data transferring system as mechanism of Encryption. Through encryption methodology perception of information security and increase consumer confident and trust. Encryption is ensuring that the data transferred is only understood by the sender and the receiver [10]. Shahriar Mohammadi Sanaz Abedi research paper expresses that by the combination of two common mechanisms, PKI (Public Key Infrastructure**)** and biometric, a higher level of security can be achieved that resolves the key management problem. The functionality of e-banking divided into three levels areas. The first level includes information systems that only offer openly existing information and their main purpose is marketing. Level 2 are systems that allow the transmission of sensitive evidence to their users. In conclusion, level 3 has the most advanced systems that simplify electronic funds transfer and other financial transactions. In PKI security architecture that has been presented to provide an increased level of confidence for customer. PKI refers to the use of a public and private key pair for authenticating and proof of contented. The public key cryptography procedures two pairs of mathematically linked cryptographic keys. If one key is used to encrypt the message, then simply the associated key can decrypt that message. Public keys are kept in digital certificates beside with other appropriate information. Since the certificate is publicly available, preventing access. In paper P. Subsorna and S. Limwiriyakul Automatic introduce timeout feature for inactivity of logging page for a time period. And secured the data by encrypting method. And used username and password as common and traditional way to authentication [11] [12]. Customers from an online bank can manage their accounts with their own electronic devices as long as an Internet connection is available. Most of them are used several kind of security system as well as registration and login phase method. Password security is using advanced system like one-time password, grid authority card, (QR) code, Biometric systems, Security questions and E-token etc. Some of security issue it can be a happened like that Phishing, Internet scams, Malware, Virus. [13] Private data may result in consequence such as identity stealing, as well as theft of assets. Therefore, security is very important of banking transaction. This study indicates that Internet banking allows customer to conduct transaction at any time and thus it reduces the number of physical visit to a bank and it has reduced the cost per transaction.so now a day if transaction complete must be an internet connection any time. [14] The banking industry as well as way people interact with financial institution and one another financially. Security infrastructure being applied at the banking institutions to secure their databases and servers. For any non-personal transaction, the bank has to verify the identification of the end-user, and hence in an online environment has to trust some form of digital identity to know its customer. Then can login to system using password throughout some external hardware. There is a significant need for standardization in the security mechanism used by banks. [13] Then, online banking facilities give users the flexibility to undertake their banking at a time that best suits them and also saves time but it also presents various security threats. [15]

3 METHODOLOGY

The proposed system consists three main phases in order to accomplish E-banking security. They are, Client verification phase, Server verification phase, Secured data transmission phase. Advanced Encryption mechanisms are used at each and every phases of the proposed system to ensure advanced security. Public and private keys of Client, Authentication server and Banking server are used for this purpose. Phases of this model are further described in the following section.

3.1 Client Verification Phase

Client verification phase is one of the important phase in E-banking security as many frauds related to E- banking happen due to impersonalized intruders. This phase ensures that, Original user is requesting for E- banking services. This is implemented using MAC address of banking dongle, Finger print information of particular user, private username and one-time password. Initial request for E-banking operation is send with the MAC address of E-banking dongle of particular user. Further operations are carried out only if the MAC address is valid. Next the finger print of the user is checked for validation. If the result is positive, the system prompts username. For correctly entered username, one-time password is issued through SMS and client verification process comes to an end.

3.2 Server Verification Phase

Server verification phase ensures that the client is accessing an original E-banking site. This is implemented by validating the finger print at clients’ end. Finger prints of valid users are stored in the database of the banking server. This finger print information is send to the valid client request. The E-banking dongle application allows further E-banking process only if both the finger print information matches with each other. This finger print validation verifies originality of both parties at a time (i.e. only the original banking site will be able to send finger print of original client).

3.3 Secured Data Transmission Phase

This phase ensures that the E-banking service operations are carried out securely between client's end and server end. This is implemented with the use of temporary session keys for encryption and decryption of transaction information. Session keys are issued at the end of client and server verification processes. Session key is encrypted with public key of client and private key of E-banking server and issued to the client. Session key is encrypted using private key of E-banking server to ensure that the session key is issued by original E-banking site and encrypted using public key of client to ensure that the session key is decrypted only by original client. Session keys get expired either, if no transaction is recorded within 10 minutes of initiation or if user request session termination.

3.4 New System Overall Process

The following section describes how the proposed online banking security model works. The process of connecting client to the server, transaction information exchange and connection termination are being explained in a step by step by manner below.

1. Once the intended user inserts the banking dongle which has internet connectivity and finger print scanner technology, dongle automatically sends a request to the authentication server.
2. Authentication server checks the MAC address of requesting dongle for client verification, if it is a valid client, Authentication server sends a request to Banking server for the finger print of particular user.
3. Banking server sends the finger print of respective user, after encrypting it with Banking servers' private key and public key of Authentication server.
4. This finger print is decrypted with suitable keys at Authentication servers' end, again encrypted with Authentication servers' private key and forwarded to Client.
5. Preliminary server verification is conducted at clients' end by matching the received finger print with the users' finger print scanned at the movement of inserting dongle.
6. If the result is positive, the dongle application prompts username of the user and sends the retrieved information to the authentication server after encrypting it with the public key of Authentication server.
7. If the username is valid password text box is enabled and one-time password is send to the user through SMS.
8. When authentication server confirms the identity, session key for further data transmission which is encrypted with private key of Authentication server and public key of respective user is send to the user.
9. Both banking server and client device uses this session key to encrypt and decrypt transaction information.
10. Session key get expired if there aren't any transactions observed within 10 minutes of session initiation.
11. Once the user request to terminate the operation, session key get expired and dongle application get closed after notifying the user.
12. User ejects the dongle from their client device.

3.5 System Module Interaction

Fig. 1 below gives a diagrammatic picture of the system module interaction and data transfer.

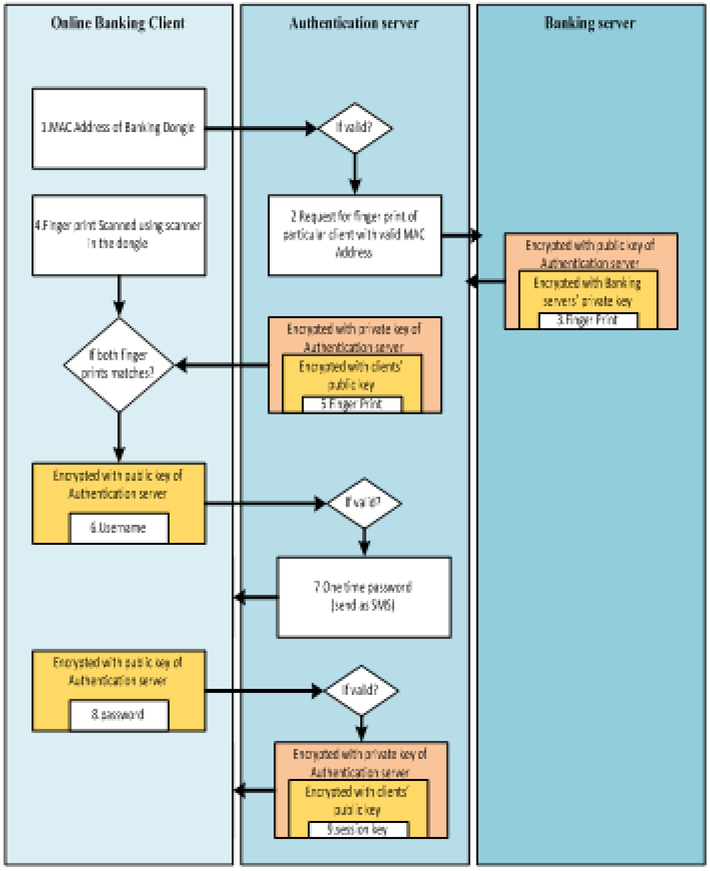

Online Banking Client
Authentication server
Banking server
1.MAC Address of Banking Dongle
If valid?
2.Request for finger print of particular client with valid MAC Address
Encrypted with public key of Authentication server
Encrypted with Banking servers' private key
3.Finger Print
4.Finger print Scanned using scanner in the dongle
Encrypted with private key of Authentication server
Encrypted with clients' public key
5.Finger Print
If both finger prints matches?
Encrypted with public key of Authentication server
6.Username
If valid?
7.One time password (send as SMS)
Encrypted with public key of Authentication server
8.password
If valid?
Encrypted with private key of Authentication server
Encrypted with clients' public key
9.session key

Fig. 1. *System Module Interaction*

3.6 System Authentication Protocol

An authentication protocol is a type of computer communication protocol or cryptographic protocol which is used to transfer authentication information between client and server. This protocol is essential for secure communication between the nodes in a network. There are two main types of authentication protocols, they are, Authentication protocols developed for PPP and AAA architecture protocols (Authentication, Authorization, Accounting). This proposed system uses AAA Architecture protocol as Authentication protocol. This is a complex protocol which is used in larger networks for authorization, authentication and accounting purposes.

1. Authentication: Refers to who is allowed to gain access to the network (In this original clients of online banking). Clients are required to prove their identity.
2. Authorization: Refers to what the client is allowed to do or what services the client access to.
3. Accounting: Refers to keeping track of what the client did and what services were used. This is necessary for security auditing purposes of banks. Accounting uses start and stop of the messages to keep track of when a service was started and when it was terminated.

Terminal Access Control Access Control Server (TACACS+), Remote Authentication Dial-In User Service (RADIUS) and DIAMETER are the servers which utilizes the above Authentication protocol.

3.7 System Hardware Components

1. Authentication Server

This proposed model uses TACACS+ server as Authentication server. Authentication, Authorization and Accounting functions are performed separately in TACACS+ server. This gives the administrator more flexibility when designing AAA policy. This server uses client server model and able to run in either Universal Network Information Exchange (UNIX) or Network Terminal (NT). TACACS+ uses the most reliable connection oriented Transmission Control Protocol/Internet Protocol (TCP/IP) protocol. Although port number 49 is the default port for this server, it can be configured to listen any other ports as needed. A shared secret key is used by the server (Session key) to provide encryption for transaction data transmission between Banking server and client machine. While traditional clients are forced to use static passwords to verify their identity, TACACS+ allows to use one time passwords and other mechanisms. TACACS+ encrypts entire payload when communicating. Thus, makes it difficult to decipher communication information between client and the server. Hash function MD5 is used for basic encryptions inside the server. TACACS+ configuration contains two parts. They are creating user profiles in the serves’ database and setting up the client to communicate the server. Offering multiprotocol support is another advantage of TACACS+. TACACS+ has been selected due to many reasons. Secure and uninterrupted flow of transaction information is an essential factor in online banking security. This is enable by the use of TCP/IP protocols in TACACS+ server. TACACS+ supports major verification models of the proposed system such as one time passwords, advanced encryption standards and shared secret keys etc. Another issue arises when configuring access lists to the online banking clients who access the banking server from remote location with dynamically created IP addresses when they dial into the network. TACACS+ solves that issue using “Virtual Profile” mechanism. Here access lists are tailored to specific users and then applied dynamically when the client connects to the network. A virtual interface gets created when user dials into the system and it dynamically get removed when user disconnects from the network.

2. Internet Banking Dongle with Finger Print Scanner

E-banking dongles are proposed in the system as they are cheap and easy to use consumer devices. E-banking dongle provides end to end connectivity established between Internet banking site and dongle. Finger print scanners are integrated to the dongles so that finger print of the user are captured and encrypted at the time of connection itself. In this way possibilities of sniffing the finger print at application level using malwares and Trojans are eliminated.

4 Conclusion

The combination of finger prints biometric scan and the image verification can offer more secure mechanism for security. Connecting the biometric scanning dongle to the server, automatically check with the both mac add of the dongle and username password of the account are matching. Moreover, image verification done by the user, to identify the image that provided by the relevant bank. This is due to the fact to prevent unknown authentication loggings. In addition, banking system using a PKI to secure the sender and receiver account details. All the logging details will be sent to authentication server. Finally,” Improved E-banking System with Advanced Encryption Standards and security Models” progress between e-banking systems should be developed more and implemented in order to provide security awareness such as money transferring risks and threats logging information to all existing and potential internet banking customers.

5 Future works

The major drawback of the proposed research is used for device connected internet dongle integrated with finger print scanning technology. With the use of a higher performance dongle it might be possible to connect with the Bluetooth in that login devices.

Acknowledgment

Authors are very much thankful to Sri Lanka Institute of Information Technology for doing research work in Computer Networking as well as all the authors whom team have referred in this research paper. Authors are also thankful to Mr. Dhishan Dhammearatchi for his constant support and encouragement for conducting research work in Computer Networks Design and Implementation.

References

[1] H. Ullah Khan, "E-Banking: Online Transaction and Security Measures", Research Journal of Applied Sciences, Engineering and Technology, vol. 07, no. 19, pp. 1-8, 2014[online]. Available at: http://maxwellsci.com/jp/abstract.php?jid=RJASET&no=428&abs=14 [Accessed 28 Jul. 2016].

[2] E. R.Nwogu, "Improving the security of the Internet Banking System Using Three-Level Security Implementation", International Journal of Computer Science and Information Technology and Security, vol. 04, no. 06, pp. 1-10, 2014[online]. Available at: http://ijcsits.org/papers/vol4no62014/7vol4no6.pdf [Accessed 28 Jul. 2016].

[3] K. Thamizhchelvy and G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm", International Conference on Computing Sciences, pp. 1-5, 2012[online]. Available at: https://www.eecis.udel.edu/~wwang/cisc849/E-Banking%20Security%20Mitigating%20Online%20Threats%20Using%20Message%20Authentication.pdf [Accessed 28 Jul. 2016].

[4] Kovach S. and Vicente Ruggiero, "Online Banking Fraud Detection Based on Local and Global Behavior", The Fifth International Conference on Digital Society, pp. 1-6, 2011[online]. Available at: https://www.researchgate.net/publication/228616927_Online_Banking_Fraud_Detection_Based_on_Local_and_Global_Behavior [Accessed 16 Aug. 2016].

[5] Chen H. and Corriveau J "Security Testing and Compliance for Online Banking in Real-World", Proceedings of the International Multi Conference of Engineers and Computer Scientists, vol. 1, pp. 1-5, 2009 [online]. Available at: http://www.iaeng.org/publication/IMECS2009/IMECS2009_pp1039-1043.pdf [Accessed 14 Aug. 2016].

[6] D.S. Coming and O.G. Staadt, "Velocity-Aligned Discrete Oriented Polytopes for Dynamic Collision Detection," IEEE Trans. Visualization and Computer Graphics, vol. 14, no. 1, pp. 1-12, Jan/Feb 2008, doi:10.1109/TVCG.2007.70405. (IEEE Transactions)

[7] Khrais, Laith. "Highlighting The Vulnerabilities of Online Banking System". The Journal of Internet Banking and Commerce 2015 (2015): n. pag. Web. [online]. Available at: http://www.icommercecentral.com/open-access/highlighting-the-vulnerabilities-of-online-banking-system.php?aid=61518 [Accessed 08 Sep. 2016].

[8] Ula, Munirul, Zuraini Ismail, and Zailani Sidek. "A Framework for The Governance of Information Security in Banking System". JIACS (2011): 1-12[online]. Web. Available at: http://ibimapublishing.com/articles/JIACS/2016/726196/726196.pdf [Accessed 08 Sep. 2016].

[9] Das, Soumyajit and Dr. Pranam Dhar. "Technological Security Aspects for Internet Banking". PARIPEX 3.6 (2012): 110-115. Web.

[10] A Haque, A zaki, "Issues of E-Banking Transaction: An Empirical Investigation On Malaysian Customers Perception". Connection.ebscohost.com. N.p., 2016. Web. Available at: http://irep.iium.edu.my/8061/1/Issues_of_E-banking_transaction_An_empirical_investigation_on_Malaysian_customers_perception.pdf [Accessed: 14 Sept. 2016.]

[11] Mohammadi, Shahriar and Sanaz Abedi. "ECC-Based Biometric Signature: A New Approach in Electronic Banking Security". 2008 International Symposium on Electronic Commerce and Security (2008): n. pag. Web. Available at: https://www.eecis.udel.edu/~wwang/cisc849/AshrafBah-Pres1-Paper2.pdf [Accessed: 14 Sept. 2016.]

[12] Subsorn, P. and S. Limwiriyakul. "A Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective". Procedia Engineering 32 (2012): 260-272. Web. Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1024&context=icr [Accessed 14 Sept. 2016.]

[13] S. Pakojwar and D. Uke, "Security in Online Banking Services – A Comparative Study", International Journal of Innovative Research in Science, Engineering and Technology, vol. 3, 2014[online]. Available at: http://www.ijirset.com/upload/2014/october/79_Security.pdf [Accessed 14 Sep. 2016].

[14] R. Kaur Jassal and R. Kumar Sehgal, "Online Banking Security Flaws", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, 2013[online]. Available at: http://www.ijarcsse.com/docs/papers/Volume_3/8_August2013/V3I2-0257.pdf [Accessed 14 Sep. 2016].

[15] J. Choubey and B. Choubey, "Secure User Authentication in Internet Banking: A Qualitative Survey", International Journal of Innovation, Management and Technology, vol. 4, 2013[online]. Available at: http://www.ijimt.org/papers/391-D0493.pdf [Accessed 14 Sep. 2016].

APPENDIX

Figure 1: RADIUS vs. TACACS+

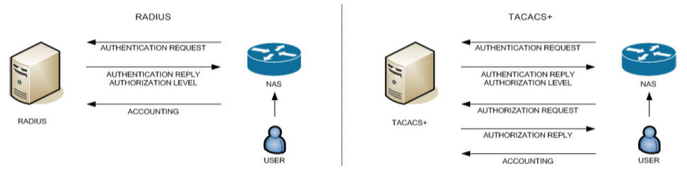
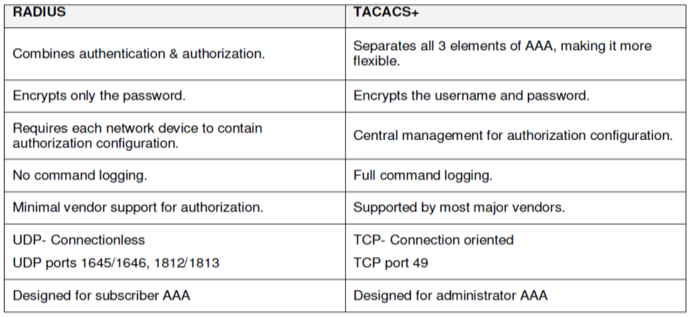


Table 1: RADIUS vs. TACACS+



RADIUS	TACACS+
Combines authentication & authorization.	Separates all 3 elements of AAA, making it more flexible.
Encrypts only the password.	Encrypts the username and password.
Requires each network device to contain authorization configuration.	Central management for authorization configuration.
No command logging.	Full command logging.
Minimal vendor support for authorization.	Supported by most major vendors.
UDP- Connectionless UDP ports 1645/1646, 1812/1813	TCP- Connection oriented TCP port 49
Designed for subscriber AAA	Designed for administrator AAA

Fig. 1. *TACACS+ vs RADIUS*

*(**Source:** http://51sec.weebly.com/blog/basic-cisco-tacacs-configuration-with-free-tacacs-software-for-windows-part-1)*

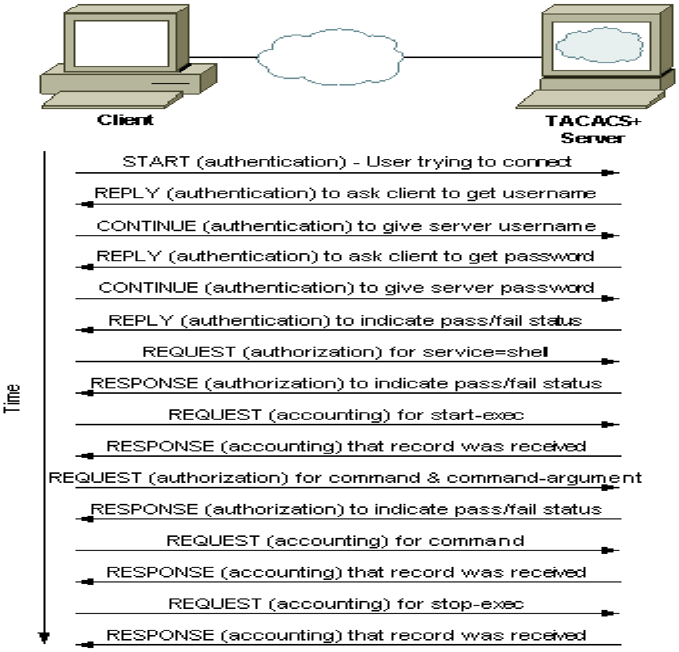

Client
TACACS+ Server
Time
START (authentication) - User trying to connect
REPLY (authentication) to ask client to get username
CONTINUE (authentication) to give server username
REPLY (authentication) to ask client to get password
CONTINUE (authentication) to give server password
REPLY (authentication) to indicate pass/fail status
REQUEST (authorization) for service=shell
RESPONSE (authorization) to indicate pass/fail status
REQUEST (accounting) for start-exec
RESPONSE (accounting) that record was received
REQUEST (authorization) for command & command-argument
RESPONSE (authorization) to indicate pass/fail status
REQUEST (accounting) for command
RESPONSE (accounting) that record was received
REQUEST (accounting) for stop-exec
RESPONSE (accounting) that record was received

Fig. 02. *TACACS+ Traffic Example*

*(**Source:**http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html)*