IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 5, Ser. 1 (Sept. – Oct. 2024), PP 01-07
www.iosrjournals.org

Cyber Insecurity For Internet Banking

Mohammad Shohel Rana, Md. Majidul Islam,
Southeast University, School Of Science And Engineering, Department Of Computer Science And Engineering,

Abstract
Internet banking has become a crucial aspect of modern financial transactions, enabling customers to access their account information and perform various transactions from anywhere. Ensuring the security of these transactions is one of utmost importance, and this is where authentication protocols come into play. One such protocol is Kerberos, which is widely used for secure authentication in many applications, including internet banking. In this paper we discuss the basic operations and functionalities of Kerberos while pinpointing the advantages of using Kerberos as an authentication protocol in internet banking. We also discuss the security features of using Kerberos, including its use of encrypted tickets and its ability to prevent replay attacks.

Index Terms- Internet Banking, Cyber Security, Authentication, Kerberos, Multi factor authentication server, Replay attack.

Date of Submission: 26-08-2024 Date of Acceptance: 06-09-2024

I. INTRODUCTION

The widespread use of internet banking has increased the need for secure authentication protocols that can ensure the most common threat in our country is to phishing the victim's important information such as user credentials and an attacker can verify anything using that information. This is not only an issue for internet baking in Bangladesh. But it is the biggest issue in Bangladesh. Only Fake authentication is responsible for huge amounts of cyber-attack. But still maximum attack and loss occurs for weak authentication

The banking sector has been one of the primary targets of cyber-attacks, as financial information is highly valuable to attackers. The use of internet banking services has become increasingly popular, but this has also created new security challenges. To address these challenges, financial institutions must implement robust security solutions that can protect customer information and prevent unauthorized access to sensitive data.

In the context of internet banking, Kerberos provides a secure method for authenticating users and ensuring that sensitive financial transactions are protected against unauthorized access to reach a solution. One of the most widely used protocols for secure authentication is Kerberos, which was developed by the Massachusetts Institute of Technology (MIT) in the 1980s. Kerberos is a robust and scalable authentication protocol that provides secure authentication by encrypting user credentials and tickets exchanged between the client, the authentication server, and the target service In recent years, the banking industry has experienced an increasing number of cyber-attacks, leading to significant losses for financial institutions and customers alike.

II. Literature Review:

Our analysis is directly related to the literature on the diffusion of technology and innovation (Bass 1969, Davis 1989, Davis et al. 1989, Rogers 1995, Zhu et al. 2003, Zhu and Kraemer 2005), and more specifically to research related to the adoption of self-service technology (Meuter et al. 2000, Curran et al. 2003) and especially the adoption of online banking (Chang 2002, Tan and Teo 2000, Lee and Lee 2001, Lee et al. 2003, Lichtenstein and Williamson 2006).

Adoption of Internet Banking

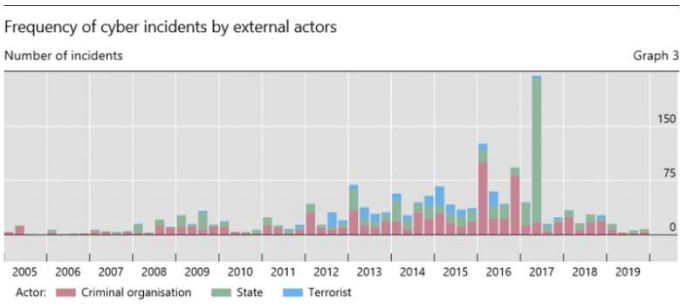
Studies have shown that the adoption of internet banking has increased significantly in recent years. This is due to a combination of factors, including the increasing availability of internet access, the growing need for convenience and accessibility, and the perception of internet banking as a more secure and efficient way to manage financial transactions. In addition, the introduction of mobile banking has made internet banking even more accessible, allowing consumers to manage their financial transactions from anywhere, at any time.

III. SECURED AUTHENTICATION PROTOCOL FOR SECURED BANKING

To combat this growing threat, the banking sector must take advantage of robust security solutions that can protect sensitive information and prevent unauthorized access to customer accounts. This paper aims to examine the role of the Kerberos protocol in enhancing the security of internet banking services.

The banking sector has been one of the primary targets of cyber-attacks, as financial information is highly valuable to attackers. The use of internet banking services has become increasingly popular, but this has also created new security challenges. To address these challenges, financial institutions must implement robust security solutions that can protect customer information and prevent unauthorized access to sensitive data

This graph representing the cyber-attack frequency in recent years which is really alarming



Source: https://www.suerf.org/policynotes/18421/cyber-risk-in-the-financial-sector

A. Kerberos Overview

Kerberos is a network authentication protocol that was developed in the 1980s at MIT. It is widely used to provide secure authentication on computer networks, including the internet. The key advantage of Kerberos is that it eliminates the need for users to send their passwords over the network in clear text. Instead, Kerberos uses a combination of encryption and tickets to authenticate users and authorize access to resources.

B. Use of Kerberos in Banking Security

Kerberos provides several security benefits, including the use of encrypted tickets and the prevention of replay attacks. In a replay attack, an attacker intercepts a valid authentication message and resends it to the authentication server, potentially gaining unauthorized access to the target service. Kerberos prevents replay attacks by using a time-limited ticket that becomes invalid after a certain period of time. Also, it confirms Three level security which is better than two factor authentication.

C. WHY KERBEROS?

Kerberos is an essential component of internet banking security and is critical in ensuring the security and privacy of sensitive financial transactions. By providing secure authentication and encryption, Kerberos helps to prevent unauthorized access and protect sensitive information from being intercepted.

Kerberos operates on the principle of a trusted third-party, known as a Key Distribution Center (KDC), which is responsible for issuing tickets to clients and servers that need to communicate with each other. These tickets, which contain encrypted information about the client and server, are used to establish secure connections and prevent unauthorized access.

One of the key benefits of using Kerberos in internet banking is that it allows for single sign-on (SSO) functionality. This means that users only need to authenticate themselves once to access multiple banking services, rather than having to enter their credentials multiple times. This reduces the risk of password-related security breaches and enhances the overall user experience. In addition to providing SSO, Kerberos also helps to prevent network-level attacks such as man-in-the-middle (MITM) attacks, by encrypting all communication between the client and server. This ensures that sensitive information, such as bank account numbers and passwords, cannot be intercepted and read by unauthorized individuals.

IV. CURRENT INTERNET BANKING SECURITY DEFECTS AND WAY TO OVERCOME THE ISSUE

ISSUE FINDINGS:

Phishing scams: These are fraudulent emails or websites that appear to be from a legitimate bank or financial institution, tricking customers into revealing their login credentials and other sensitive information.

Malware attacks: Malicious software can infect a customer's computer, allowing attackers to steal login credentials and other sensitive information.

Man-in-the-middle attacks: In this type of attack, an attacker intercepts communications between a customer and their bank, allowing them to steal sensitive information.

Unsecured Wi-Fi networks: Using unsecured Wi-Fi networks to access internet banking can put a customer's sensitive information at risk, as it can be intercepted by attackers.

It's important for customers to be vigilant and take steps to protect themselves when using internet banking, such as using secure connections and being wary of emails and websites that ask for sensitive information.

How To Overcome Security Issue Of Internet Banking
Precautions That Bank Can Take To Prevent Cyber Attack

1. **Multi factor authentication**: Banks can require customers to use multi-factor authentication, such as a password and a one-time code sent to their phone, to log into their accounts.
2. **Secure connections:** Banks can ensure that all internet banking transactions are performed over secure connections, such as SSL or TLS, to prevent man-in-the-middle attacks.
3. **Regular software updates:** Banks should regularly update their software and systems to patch any known vulnerabilities and protect against the latest threats.
4. **Employee training:** Banks can train their employees on how to recognize and respond to cyber attacks, as well as implement policies and procedures to prevent attacks.
5. **Network security:** Banks can implement firewalls, intrusion detection and prevention systems, and other security measures to protect their networks and systems from attacks.
6. **Monitoring and logging:** Banks can monitor their systems for unusual activity and log all transactions for auditing and investigative purposes.
7. **Incident response plan:** Banks should have a comprehensive incident response plan in place to quickly respond to and recover from a cyber-attack.

Implementing these and other security measures can help banks to reduce the risk of cyber attacks and protect their customers' sensitive information.

How To Implement Those Precautions In Internet Banking:

To implement those precautions, we are proposing to use Kerberos as a multi-factor authentication protocol

1. Kerberos will Work as Multifactor authentication protocol

Kerberos is a widely used network authentication protocol that provides secure authentication for users and systems. In terms of multi-factor authentication, Kerberos provides two key factors: something the user knows (i.e., a password) and something the user possesses (i.e., a cryptographic token). Here's how multi-factor authentication works in Kerberos:

1. The user enters their username and password, which is encrypted and sent to the Kerberos authentication server.
2. The authentication server verifies the user's credentials and, if they are valid, generates a unique cryptographic token (often called a "ticket") for that user.
3. The authentication server sends the ticket to the user, who then uses it to request access to a network resource (such as a file server).
4. The network resource sends a request to the authentication server to validate the ticket, which the authentication server does by checking the encrypted information contained within the ticket.
5. If the ticket is valid, the authentication server sends a message to the network resource granting access to the user.

This process provides a secure form of multi-factor authentication because the user must possess both their password and the unique cryptographic token in order to access the network resource. The use of encryption and unique tokens helps to prevent attackers from intercepting or forging authentication information, providing a higher level of security for the network and its users.

Kerberos will ensure Secured Network connection:

Kerberos is designed to provide secure network authentication by using encryption and mutual authentication between users and network resources. Here's how it helps to ensure a secured network:

Encryption: Kerberos uses strong encryption algorithms to encrypt all authentication information, including passwords and tickets, helping to prevent attackers from intercepting or forging authentication information.

Mutual authentication: Kerberos uses mutual authentication, meaning that both the user and the network resource must prove their identity to each other before access is granted. This helps to prevent attackers from impersonating either the user or the network resource.

Centralized authentication: Kerberos uses a centralized authentication server to manage and verify user credentials, making it more difficult for attackers to compromise individual systems or accounts.

Time-stamped tickets: Tickets generated by the Kerberos authentication server are time-stamped, which helps to prevent replay attacks by requiring that tickets be used within a specified time window.

Single sign-on: Kerberos can provide single sign-on functionality, allowing users to authenticate once and gain access to multiple network resources without having to re-enter their credentials.

By using these and other security measures, Kerberos helps to ensure a more secure network environment, reducing the risk of unauthorized access and other security incidents.

Kerberos Implementation In Internet Banking And Proposed Model

Kerberos can be implemented in internet banking to provide secure authentication for online transactions. Here are the general steps to implement Kerberos in internet banking:

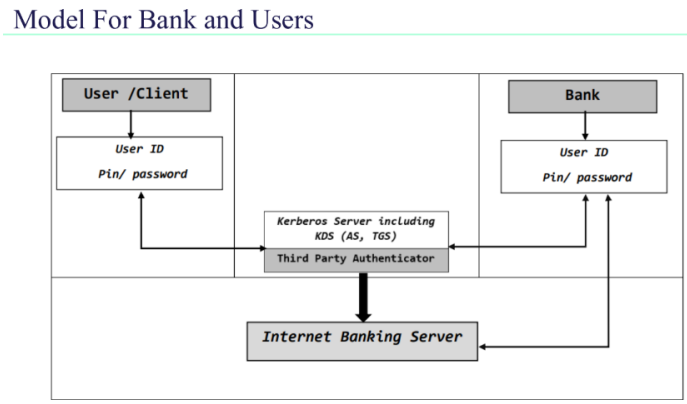


Fig. 1 Modules interaction for the proposed system

1. Set up a Kerberos authentication server: *This server will manage user accounts and issue tickets to users who need to access the internet banking system.*
2. Integrate the internet banking system with the Kerberos authentication server: *The internet banking system must be able to request and validate tickets issued by the Kerberos authentication server.*
3. Require multi-factor authentication for internet banking transactions: *Users must provide both their username and password, as well as a Kerberos ticket, to access the internet banking system.*
4. Encrypt all transactions: *All transactions between the user and the internet banking system should be encrypted to protect sensitive information from being intercepted or altered.*
5. Monitor and log all transactions: *Banks should regularly monitor the internet banking system for unusual activity and log all transactions for auditing and investigative purposes.*

By implementing these steps, banks can use Kerberos to provide secure authentication for internet banking transactions, reducing the risk of unauthorized access and other security incidents.

It's important to note that implementing Kerberos in internet banking can be complex and requires careful planning and testing. Banks should work with experienced security professionals to ensure a secure and successful implementation.

Kerberos Working Principles

Kerberos works with few steps these are

1. User authentication: The user enters their username and password, which are encrypted and sent to the Kerberos authentication server. The authentication server verifies the user's credentials and generates a unique, encrypted ticket for the user.
2. Ticket request: The user uses the ticket to request access to the internet banking system. The ticket is encrypted and contains information that proves the user's identity to the system.
3. Ticket validation: The internet banking system contacts the Kerberos authentication server to validate the ticket. The authentication server verifies that the ticket is authentic and has not been altered or used before.
4. Ticket granting: If the ticket is valid, the Kerberos authentication server sends a message to the internet banking system granting access to the user. The internet banking system uses the information in the ticket to identify the user and allow them to access their account.
5. Encrypted communication: All communication between the user, the internet banking system, and the Kerberos authentication server is encrypted to protect sensitive information from being intercepted or altered.

Session management: The internet banking system and the Kerberos authentication server manage the user's session, monitoring for unusual activity and logging all transactions for auditing and investigative purposes.

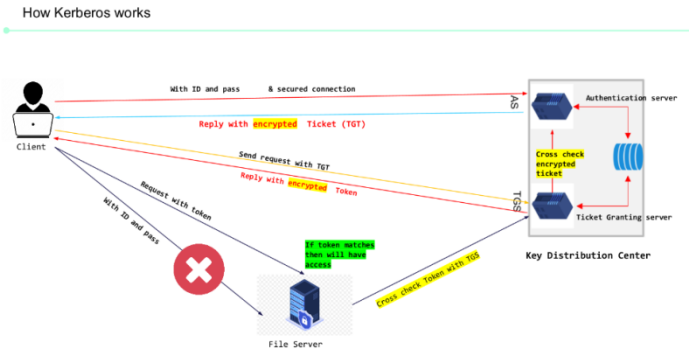


Fig. 2 Kerberos authentication process illustration

By following these steps, the Kerberos protocol in internet banking provides secure authentication for online transactions, reducing the risk of unauthorized access and other security incidents.

V. LIMITATIONS OF INTERNET BANKING

THE LIMITATIONS OF INTERNET BANKING FROM A USER PERSPECTIVE INCLUDE

Technical Issues: Technical issues, such as slow connection speeds or website downtime, can negatively impact the user experience of internet banking. This can result in frustration and a loss of confidence in the security of the system.

Security Concerns: The fear of online fraud and cyberattacks is a major concern for many users of internet banking. This fear can lead to a lack of trust in the system and discourage users from using internet banking.

Limited Functionality: Internet banking may not provide users with access to all the features and services available through traditional banking methods. For example, some users may prefer to have the option to visit a physical branch or speak with a customer service representative in person.

Accessibility: Not everyone has access to the internet or a reliable internet connection, which can limit the adoption of internet banking. In addition, older or technologically challenged individuals may struggle to use internet banking, further limiting its accessibility.

User Error: User error, such as misusing the system or making incorrect transactions, can result in financial loss or other negative consequences. This can lead to a lack of confidence in the system and discourage users from using internet banking.

In conclusion, while internet banking provides a convenient and accessible way to manage financial transactions, it is important to consider the limitations from a user perspective. Addressing these limitations, through measures such as enhanced security protocols and user education, can improve the user experience of internet banking and increase its adoption.

VI. Limitations Of Kerberos As Internet Banking Authentication Protocol

Kerberos is a widely used authentication protocol in the field of internet banking security, but it also has some limitations:

Complex Configuration: Kerberos requires a complex and time-consuming setup process, including the creation of a Kerberos server, authentication database, and authentication client. This can make it challenging for organizations to implement and maintain.

Single Sign-On Limitations: Kerberos is designed for single sign-on meaning that a user only needs to enter their credentials once to access multiple resources. However, this feature can also be a limitation, as users may forget or lose access to their SSO credentials.

Dependence on Network Connectivity: Kerberos requires a stable and secure network connection to function properly, which can be a challenge for organizations with distributed or remote users.

Limited Support for Mobile Devices: Mobile devices may not support the Kerberos protocol or may require additional software or configuration to use it, which can limit its adoption in mobile banking environments.

Security Risks: Although Kerberos provides strong security measures, it is not immune to security risks, such as the risk of man-in-the-middle attacks, replay attacks, and password guessing attacks.

In conclusion, while Kerberos provides a robust authentication solution for internet banking security, it also has some limitations that organizations must consider when deciding whether to use it. Other authentication methods, such as biometrics or multi-factor authentication, may also be used in combination with or as an alternative to Kerberos to provide a more secure and user-friendly experience.

To prevent the Internet Banking cyber-attack only Kerberos will not be enough because it has some limitations

VII. Precaution That User Should Follow To Prevent Cyber Attack For Internet Banking

Users of internet banking can take several precautions to prevent cyber-attacks:

Strong Passwords: Users should choose strong and unique passwords and avoid using easily guessable information, such as their name or birthdate. They should also regularly change their passwords to prevent unauthorized access.

Two-Factor Authentication: Using two-factor authentication, such as a one-time code sent to a mobile device, can provide an additional layer of security to the user's account.

Avoid Public Wi-Fi: Users should avoid accessing their internet banking account on public Wi-Fi networks, as these networks are often unsecured and vulnerable to cyberattacks.

Keep Software Up-to-Date: Users should regularly update their device's operating system, antivirus software, and internet browser to ensure they have the latest security updates and patches.

Watch for Phishing Scams: Users should be cautious of emails, text messages, or phone calls that ask for personal information, as these can be phishing scams designed to steal sensitive information.

Verify the Bank's Website: Users should only log in to their internet banking account through the bank's official website, and be cautious of websites that look similar but may not be legitimate.

Monitor Accounts Regularly: Users should regularly check their account activity and monitor for any suspicious transactions or activity.

By following these precautions, users of internet banking can help protect themselves from cyber attacks and ensure the security of their personal and financial information. Additionally, they can also educate themselves on the latest cybersecurity best practices and be vigilant for signs of potential threats.

VIII. Conclusion

Kerberos is a crucial tool for improving the security of internet banking services. By using encryption and tickets to authenticate users and protect transactions, Kerberos helps to ensure that sensitive financial information remains confidential and secure. Financial institutions must take advantage of this and other robust security solutions to enhance their cyber security posture and protect their customers from the growing threat of cyber-attacks.

Appendix

Kerberos is a widely used security protocol in internet banking, providing a means of authentication and authorization for users. In this appendix, we will provide a brief overview of the Kerberos protocol and its use in internet banking.

Kerberos is a network authentication protocol that uses tickets to securely identify users and authorize access to resources. The protocol operates on a trusted third-party principle, with a central authentication server (AS) acting as the trusted third-party.

When a user wants to access a protected resource, they first request a ticket from the AS. The AS then verifies the user's identity and, if they are authorized, issues a ticket granting ticket (TGT) to the user. The user then uses the TGT to request a service ticket (ST) from the Ticket Granting Service (TGS). The ST contains information about the user and the requested resource, and is used by the user to access the protected resource.

In internet banking, Kerberos is used to provide secure authentication and authorization for users accessing online banking systems. The protocol helps to ensure that only authorized users are able to access sensitive financial information, reducing the risk of unauthorized access or theft of sensitive information.

However, there are several limitations to the use of Kerberos in internet banking. One of the biggest limitations is the complexity of the protocol, which can make it difficult for users to understand and use. In addition, Kerberos requires a well-configured and secure infrastructure to operate effectively, making it challenging to implement in environments with limited resources or technical expertise.

Another limitation is that Kerberos does not provide encryption for data transmission, meaning that sensitive information, such as account numbers and passwords, may be vulnerable to interception and theft during transmission. To address this, other security protocols, such as SSL/TLS, may be used in conjunction with Kerberos to provide encryption for data transmission.

In conclusion, while Kerberos has several limitations, it is widely used as a security protocol in internet banking due to its ability to provide secure authentication and authorization. However, it is important to carefully consider the limitations of the protocol and to implement appropriate measures, such as encryption, to ensure the security of sensitive financial information.

REFERENCES

[1] Martins, C., Oliveira, T. And Popovič, A., 2014. Understanding The Internet Banking Adoption: A Unified Theory Of Acceptance And Use Of Technology And Perceived Risk Application. International Journal Of Information Management, 34(1), Pp.1-13.

[2] Dhanalakshmi, R., Prabhu, C. And Chellappan, C., 2011. Detection Of Phishing Websites And Secure Transactions. Ijcns, 1(11), Pp.15-21

[3] Dodge, R.C., Carver, C. And Ferguson, A.J., 2007. Phishing For User Security Awareness. Computers & Security, 26(1), Pp.73-80.

[4] Gharaibeh, N., 2013. The Impact Of Customer Knowledge On The Security Of E-Banking. International Journal Of Computer Science And Security (Ijcss), 7(2), P.81.

[5] Council, F.F.I.E., 2005. Authentication In An Internet Banking Environment. Financial Institution Letter, Fil-103-2005. Washington, Dc: Federal Deposit Insurance Corp.(Fdic). Retrieved March, 18, P.2005.

[6] Internet Live Stats (2017), Accessed On January 8, 2017 From Http://Www.Internetlivestats.Com/

[7] Kesharwani, A. And Singh Bisht, S., 2012. The Impact Of Trust And Perceived Risk Internet Banking Adoption In Indiaan Extension Of Technology Acceptance Model. International Journal Of Bank Marketing, 30(4), Pp.303-322.

[8] Chen, C.J., 2016, July. User Adoption Decisions In Self-Service Technologies: A Study Of Internet Banking. In Advanced Applied Informatics (Iiai-Aai), 2016 5th Iiai International Congress On (Pp.1207-1208). Ieee.

[9] Saudi Arabian Monetary Agency (Sama) Annual Report (2016): Http://Www.Sama.Gov.Sa/En

[10] Baharat Poddar, Yashraj E., Neetu Chitkara, Abhinav Bansel, 2016. Productivity In Indian Banking. Boston Consulting Group, Aug, 16.

[11] State Bank Of Pakistan Annual Report (2015/2016):Http://Www.Sama.Gov.Sa/Enus/Economicreports/Pages/Annualreport.Aspx

[12] Matthew Johnson And Simon Moore, "A New Approach To E-Banking," In U´ L Far Erlingsson And Andrei Sabelfeld, Editors, Proc. 12th Nordic Workshop On Secure It Systems (Nordsec 2007), Pages 127–138. Retrieved. May 14, 2012 http://Www.Matthew.Ath.Cx/Publications/2007-Johnson