A critical review of mechanisms of Protocols Using Shared Key Cryptography based on BGJKMY Protocols

Bushra K.Hilal
Department of Computer information systems , College of Computer Science and information technology /University of Al- Qadisiyah
Bushra.k.h@qu.edu.iq

Abstract:

Shared key cryptography protocols are critical in ensuring secure communication over insecure networks. They rely on a single secret key for the encryption and decryption of data. The Bird Gopal Herzberg Janson Kutten Molva Yung protocols (BGJKMY) are a set of security protocols that use a combination of cryptographic techniques, including public-key encryption and shared-key cryptography, to establish secure communication channels. This paper presents an overview of the BGJKMY protocols and their design principles. These protocols use multiple rounds of challenge-response exchanges to prevent replay attacks and require mutual authentication before communication can begin. BGJKMY protocols enable secure communication, even when the communication channel is not entirely secure. For instance, third-party interceptors cannot decrypt messages without the private key since public keys can be exchanged and used to encrypt messages without a pre-existing shared secret.

Keywords: cryptography, BGJKMY protocols, public-key.

مراجعة نقدية لآليات البروتوكولات التي تستخدم تشفير المفتاح المشترك بناءً على بروتوكولاتBGJKMY

بشرى كامل هلال
قسم نظم المعلومات الحاسوبية كلية علوم الحاسوب وتكنولوجيا المعلومات /جامعة القادسية
Bushra.k.h@qu.edu.iq

ملخص:

تعد بروتوكولات تشفير المفاتيح المشتركة ضرورية لضمان الاتصال الآمن عبر الشبكات غير الآمنة. يعتمدون على مفتاح سري واحد لتشفير البيانات وفك تشفيرها. تعد بروتوكولات Bird Gopal Herzberg Janson Kutten Molva Yung (BGJKMY)عبارة عن مجموعة من بروتوكولات الأمان التي تستخدم مجموعة من تقنيات التشفير، بما في ذلك تشفير المفتاح العام وتشفير المفتاح المشترك، لإنشاء قنوات اتصال آمنة. تقدم هذه الورقة نظرة عامة على بروتوكولات BGJKMY ومبادئ تصميمها. تستخدم هذه البروتوكولات جولات متعددة من عمليات تبادل التحدي والاستجابة لمنع هجمات إعادة التشغيل وتتطلب المصادقة المتبادلة قبل بدء الاتصال. تتيح بروتوكولات BGJKMY الاتصال الآمن، حتى عندما لا تكون قناة الاتصال آمنة تمامًا. على سبيل المثال، لا تستطيع أدوات الاعتراض التابعة لجهات خارجية فك تشفير الرسائل بدون المفتاح الخاص حيث يمكن تبادل المفاتيح العامة واستخدامها لتشفير الرسائل بدون سر مشترك موجود مسبقًا.

الكلمات المفتاحية: التشفير، بروتوكولاتBGJKMY ، المفتاح العام .

I. Introduction

Shared-key cryptography is an encryption technique that uses a single key exchanged between the sender and receiver of a message[1]. The key is used to both encrypt and decrypt the data, making it a symmetric encryption method. This means that the same key that is used to encrypt the data can also be used to decrypt the data. Shared-key cryptography has been widely used for a long time and is considered a secure encryption method when implemented correctly[2]. However, there are some potential security issues to be aware of with this method.

The main problem is that the key must be exchanged between the sender and the receiver, and this exchange process must be secure. The data can be easily decrypted if a third party intercepts the key[3]–[5]. One way to mitigate this risk is to use a shared-key cryptography protocol. Many different protocols use this method, each with its peculiarities[6]:

1. Advanced Encryption Standard (AES): This symmetric encryption algorithm uses a block cipher and a fixed block size. AES is considered one of the most secure encryption algorithms and is widely used in various applications, including wireless networks and hard disk encryption.
2. Data Encryption Standard (DES): This older encryption algorithm uses a block cipher and a fixed block size. Although AES has largely replaced DES, it is still used in some applications for compatibility.
3. Triple-DES (3 DES): This is an extension of the DES algorithm that uses three keys instead of one. Data is encrypted with the first key, decrypted with the second key, and then encrypted with the third key. It makes the algorithm much more secure than the standard DES and much slower.
4. RSA: This public-key encryption algorithm can encrypt and decrypt data. RSA is widely used for secure communications over the Internet and is also commonly used to sign digital certificates and electronic documents.

Each of these protocols has its specific uses, and the choice of which protocol depends on the application's requirements. For example, AES is commonly used for wireless network encryption, while RSA is used for secure communications over the Internet[7]. When using a shared key cryptography protocol, it is essential to consider the length of the key. The longer the key, the stronger the encryption. For example, AES keys can be 128 bits, 192 bits, or 256 bits long, and the longer the key, the stronger the encryption. However, longer keys also mean the encryption is slower, so a tradeoff must be made between security and speed[8]. Another consideration when using a shared-key cryptography protocol is the encryption mode used. Different encryption modes provide different levels of security and speed, and the choice of which mode to use depends on the application's specific requirements[9]. For example, CBC (Cypher Block Chaining) mode provides a high level of security but is slower than ECB (Electronic Codebook) mode.

Bird Gopal Herzberg Janson Kutten Molva Yung protocols (BGJKMY) are a set of authentication protocols designed to achieve secure communication in open networks[10]. These protocols were developed by a team of researchers, including Bird, Gopal, Herzberg, Janson, Kutten, Molva, and Yung, to address the weaknesses of existing authentication protocols. The BGJKMY protocols use cryptographic techniques to establish secure communication channels, including public-key encryption and shared-key cryptography. BGJKMY protocols are a reliable approach for secure communication in a distributed system, and they are utilized in numerous applications, including secure communication over the internet. However, it is essential to adhere to best practices and guidelines while using these protocols and regularly update and patch systems to tackle any identified weaknesses.

The BGJKMY protocols come in various forms, each with unique advantages and disadvantages. The Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols, which are widely used to allow secure communication over the internet, are among the most commonly used protocols[11].

Although BGJKMY protocols offer a high level of security, it is crucial to remember that if they are not implemented and used correctly, they may still be susceptible to specific attacks, such as man-in-the-middle attacks. Thus, it is essential to adhere to best practices and recommendations when utilizing these protocols and routinely upgrade and patch systems to fix known vulnerabilities.

Shared-key cryptography, also known as symmetric cryptography, is an essential protocol in modern security. Shared-key cryptography is because it allows two parties to communicate securely, even over an insecure channel[12]. It means that a third party intercepting the communication cannot understand the content of the message without the shared key.

Below are some reasons why shared key cryptography is a crucial protocol:

1. Confidentiality: the main goal of shared key cryptography is to ensure that the message's contents are hidden from unauthorized parties. It is achieved by encrypting the message so it can only be decrypted using the shared key[13].
2. Speed: Shared key cryptography is faster than other types of encryption because it uses a single key for encryption and decryption[14]. It is ideal for real-time applications such as video conferencing and online gaming.
3. Simplicity: since shared key cryptography uses a single key for encryption and decryption, it is relatively easy to implement and use. This makes it an excellent option for applications with critical ease of use[15].

4. Flexible: Shared-key cryptography is versatile and can be used in various scenarios, such as securing email communications and protecting financial transactions[16]. It makes it a flexible protocol that can be used in numerous contexts.
5. Resilience: shared key cryptography is a mature technology that has been extensively tested and validated over several years[13]. Therefore, it is a very robust and resilient protocol that can withstand many attacks and security threats.

II. Bird Gopal Herzberg Janson Kutten Molva Yung protocols (BGJKMY):

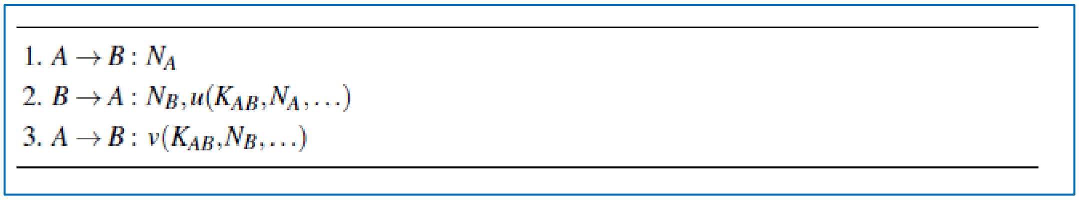
In 1993, Bird et al., researchers from IBM, published a paper that presented a range of attacks on numerous authentication protocols, including a protocol proposed by ISO[10]. This paper was one of the first to demonstrate such attacks. As a result of their findings, the researchers developed a set of security criteria to prevent similar future attacks. They also proposed new protocols that satisfied these criteria[10]. The researchers began with a basic protocol that they deemed insecure and then gradually improved it by analyzing various attacks and design requirements. Eventually, they arrived at a protocol that met their standards for security**.**

Although not commonly used, the term "Bird Gopal Herzberg Janson Kutten Molva Yung Protocols" may refer to a group of cryptographers who have contributed to developing various cryptographic protocols or systems[17]. Some examples of well-known protocols or procedures that have been created or co-developed by individuals with these last names include:

- The **Herzberg-Kutten-Yung** (HKY) Protocol is a secure key exchange protocol that provides mutual authentication and perfect forward secrecy.
- The **Janson** protocol is a secure key agreement protocol that provides perfect forward secrecy and is used for secure group communication.
- The **Molva-Yung** Protocol is a secure key establishment protocol that provides perfect forward secrecy and is used for secure electronic transactions.
- The **Bird** scheme is a cryptographic system that provides data encryption and integrity protection using a symmetric key.

Using BGJKMY protocols is a dependable method for achieving secure communication in a distributed system, and they find applications in various fields, including secure communication over the internet. It is crucial to follow best practices and guidelines while using these protocols and to update and patch systems regularly to address any vulnerabilities that may be discovered.

The protocol in figure 1 is the primary protocol of Bird et al. Here u and v are two functions such that K_{AB} is needed to calculate them, and they do not give away K_{AB}.



1. $A \rightarrow B : N_A$
2. $B \rightarrow A : N_B, u(K_{AB}, N_A, \ldots)$
3. $A \rightarrow B : v(K_{AB}, N_B, \ldots)$

Figure 1: Bird et al. canonical protocol 1

At first, we assume that the functions u and v are identical. However, this assumption fails to fulfill the matching conversation objective, which Bird et al. considered a crucial aspect of any secure authentication protocol. Attack (figure 1) akes advantage of this vulnerability by exploiting A as an oracle against B. To illustrate, suppose an adversary named I aim to launch an attack on the protocol. First, I initiate a protocol run with B while impersonating A. Concurrently, I commence a protocol run with A while masquerading as B.

In attack (figure 1), B accepts the conversation despite it not matching, leaving the authentication protocol vulnerable. Bird et al. realized that the functions u and v need to be different to prevent such attacks. This ensures that an adversary cannot exploit A's response in the parallel session to complete the first run. However, while using different u and v functions is sufficient for security purposes, it is not necessary to achieve the authentication objective. As long as the functions u and v include the identities of the sender and the intended partner, the authentication objective can still be fulfilled even if the functions are the same[10]. Although this modified protocol is open to a similar attack, the attack would not breach the authentication objective.

III. Limitations and solutions of BGJKMY protocols

This section discusses the limitations and potential solutions of BGJKMY protocols.

1- Complexity

The complexity of these protocols lies in the design principles used to achieve their security goals. One of the key design principles of BGJKMY protocols is using multiple rounds of challenge-response exchange to prevent replay attacks. Attackers use replay techniques to trick recipients into thinking they are receiving brand-new messages by intercepting legitimate messages and resending them. By using challenge-response exchanges, each message is made to be distinct and impossible for an attacker to replay.

The complexity of BGJKMY protocols can be reduced through clear documentation, user-friendly tools, abstraction, training and support, and open-source software. By making these protocols easier to understand and use, it is possible to increase their adoption and make them more accessible to a broader range of users and applications.

2- Performance

Performance is critical in designing and implementing protocols using shared key cryptography[18]. The performance of a protocol is determined by the speed at which it can process and transmit data and the number of resources, such as memory and processing power required. It's important to note that the specific steps for enhancing the performance of the BG-HJKMY protocol will depend on the particular implementation and use case. It may be necessary to seek the assistance of an expert in the field.

3- Key management

Protocols using shared key cryptography rely on the same secret key for encrypting and decrypting messages, making key management critical [19]. The key must be kept a secret and kept out of the hands of anyone but those involved in secure communications. In protocols that use shared-key cryptography, ensuring the efficient and secure distribution, generation, and revocation of secret keys is a crucial component of key management. This can be accomplished using a variety of strategies and methods. The BGJKMY protocols combine public-key encryption and shared-key cryptography to create secure communication channels. To ensure that both parties authenticate one another and that secret keys are exchanged securely, these protocols' key management is based on multiple rounds of challenge-response exchange. Although the key management in the BGJKMY protocols is intended to be secure, it has some drawbacks. When using these protocols, it's crucial to adhere to best practices and recommendations. Systems should also be routinely updated and patched to fix any vulnerabilities that are found. In addition, additional mechanisms, such as key revocation mechanisms or other security measures for public key exchange, might be required to address the shortcomings of the key management in these protocols.

4- Certificate Management

Certificate management is an essential aspect of protocols using shared key cryptography. In these protocols, parties must have a way to verify each other's identities before they can securely communicate[20]. Certificates provide a means to establish trust in the identity of the communicating parties. In BGJKMY can include implementing automatic certificate renewal processes, developing certificate revocation systems, and using certificate authorities to manage certificates.

5- Security

The security of shared key cryptography protocols requires careful consideration of key management, key size, key exchange, authentication, replay attacks, and secure implementation. Enhancing the confidentiality, integrity, and availability (CIA) of encrypted data is crucial to improving the security aspect of BGJKMY protocols. These measures are vital to ensuring that the data remains secure, intact, and readily accessible when needed.

6- Interoperability

Interoperability refers to the ability of different systems or components to work together and exchange data seamlessly[21]. Interoperability in shared-key cryptography protocols means that different systems or components can utilize identical cryptographic algorithms and keys to safeguard their communications.[22]. To address interoperability challenges, efforts can be made to standardize BGJKMY protocols and develop systems that can support multiple protocols. This may include the use of open standards, the development of gateways that can translate between different protocols, and the development of software that can support multiple protocols.

IV. Conclusion

Shared key cryptography is an important factor in securing network communications, and there is a need for ongoing research to improve the security of these protocols. The importance of BGJKMY protocols for secure communication in open networks and the need for further research to improve their security and usability The BGJKMY protocols provide a secure method for communication in a distributed system, but they also have certain limitations that should be considered. These limitations include complexity, performance issues, key and certificate management issues, vulnerability to attack, and interoperability issues. It is important to carefully consider these limitations when deciding whether to use BGJKMY protocols and to plan strategies to address potential problems. There are several strategies to overcome the limitations of BGJKMY protocols, including simplification, performance optimization, key management, certificate management, security, and interoperability. By overcoming these challenges, it is possible to improve the security and reliability of these protocols and make them more accessible and usable for a wider range of users and applications.

Reference:

[1] S. Garg, V. Jindal, H. Bhatia, R. Johari, and S. Gupta, “Community oriented socio-behavioural PentaPlicative Cipher Technique,” *Egypt. Informatics J.*, 2023.

[2] B. A. Forouzan and D. Mukhopadhyay, *Cryptography and network security*, vol. 12. Mc Graw Hill Education (India) Private Limited New York, NY, USA:, 2015.

[3] A. A. Ahmed and O. M. Barukab, “Unforgeable Digital Signature Integrated into

Lightweight Encryption Based on Effective ECDH for Cybersecurity Mechanism in Internet of Things," *Processes*, vol. 10, no. 12, p. 2631, 2022.

[4] Z. Ashraf, A. Sohail, and M. Yousaf, "Robust and lightweight symmetric key exchange algorithm for next-generation IoE," *Internet of Things*, p. 100703, 2023.

[5] Y. Wu and T. Feng, "An Anonymous Authentication and Key Update Mechanism for IoT Devices Based on EnOcean Protocol," *Sensors*, vol. 22, no. 17, p. 6713, 2022.

[6] A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptogr. Netw. Secur.*, vol. 16, pp. 1–11, 2017.

[7] Y. Zhang, S. Wang, P. Phillips, and G. Ji, "Binary PSO with mutation operator for feature selection using decision tree applied to spam detection," *Knowledge-Based Syst.*, vol. 64, pp. 22–31, 2014, doi: 10.1016/j.knosys.2014.03.015.

[8] J. Gilchrist, "Encryption," H. B. T.-E. of I. S. Bidgoli, Ed. New York: Elsevier, 2003, pp. 87–100.

[9] H. Alabdulrazzaq and M. N. Alenezi, "Performance Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish," *Int. J. Commun. Networks Inf. Secur.*, vol. 14, no. 1, pp. 51–61, 2022.

[10] C. Boyd, A. Mathuria, and D. Stebila, "Protocols Using Shared Key Cryptography BT - Protocols for Authentication and Key Establishment," C. Boyd, A. Mathuria, and D. Stebila, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2020, pp. 95–134.

[11] H. K. Lee, T. Malkin, and E. Nahum, "Cryptographic strength of SSL/TLS servers: Current and recent practices," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, 2007, pp. 83–92.

[12] L. Johnson, "Chapter 11 - Security Component Fundamentals for Assessment," L. B. T.-S. C. E. Johnson Testing, and Assessment Handbook, Ed. Boston: Syngress, 2016, pp. 531–627.

[13] J. A. Sarumi, "A review of encryption methods for secure data communication," in *Proceedings of the 30th iSTEAMS Multidisciplinary & Inter-tertiary Research Conference*, 2022, pp. 63–82.

[14] A. Chhatrapati, S. Hohenberger, J. Trombo, and S. Vusirikala, "A performance evaluation of pairing-based broadcast encryption systems," in *Applied Cryptography and Network Security: 20th International Conference, ACNS*

2022, Rome, Italy, June 20–23, 2022, Proceedings, 2022, pp. 24–44.

[15] A. Baksi, S. Bhasin, J. Breier, D. Jap, and D. Saha, “A survey on fault attacks on symmetric key cryptosystems,” *ACM Comput. Surv.*, vol. 55, no. 4, pp. 1–34, 2022.

[16] A. Ganji and D. Usha, “Knowledge Challenges and Responses in the Internet of Technologies,” in *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, 2022, pp. 1–8.

[17] M. Bellare and P. Rogaway, “Entity authentication and key distribution,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 773 LNCS, pp. 232–249, 1994, doi: 10.1007/3-540-48329-2_21.

[18] G. Gaubatz, J.-P. Kaps, and B. Sunar, “Public key cryptography in sensor networks—revisited,” in *Security in Ad-hoc and Sensor Networks: First European Workshop, ESAS 2004, Heidelberg, Germany, August 6, 2004, Revised Selected Papers 1*, 2005, pp. 2–18.

[19] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. Najmus Saqib, “Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key,” *Int. J. Commun. Syst.*, vol. 32, no. 16, p. e4139, 2019.

[20] A. A. Ahmed, “Lightweight Digital Certificate Management and Efficacious Symmetric Cryptographic Mechanism over Industrial Internet of Things,” *Sensors*, vol. 21, no. 8, p. 2810, 2021.

[21] A. N. Gohar, S. A. Abdelmawgoud, and M. S. Farhan, “A Patient-Centric Healthcare Framework Reference Architecture for Better Semantic Interoperability Based on Blockchain, Cloud, and IoT,” *IEEE Access*, vol. 10, pp. 92137–92157, 2022.

[22] M. Goworko and J. Wytrębowicz, “A secure communication system for constrained IoT devices—experiences and recommendations,” *Sensors*, vol. 21, no. 20, p. 6906, 2021.