

Counter-Based Session Key Establishment Protocol for Efficient and Forward Secrecy in Bluetooth BR/EDR

Kajal Santosh Sanap¹ Prof. M. N. Pimple², Prof. A. R. Kardile³, Dr. H. B. Jadhav⁴

Student, Department of Computer Engineering¹

Guide, Department of Computer Engineering²

Co-guide, Department of Computer Engineering³

HOD, Department of Computer Engineering⁴

Adsul Technical Campus, Chas, Ahilyanagar, India

Abstract: Bluetooth BR/EDR is commonly used for short-range wireless communication, so protecting the session key is important for keeping communication secure. Recent attacks such as BLUFFS have shown that the existing Bluetooth session key establishment process has some security weaknesses. This paper presents a counter-based method that aims to improve both security and efficiency. The proposed Counter-Based Legacy Secure Connections (C-LSC) and C-LSC+ protocols use a counter as a fresh value and use Message Authentication Codes (MACs) to protect the counter from unauthorized changes. C-LSC uses counter synchronization, whereas C-LSC+ is designed to work without synchronization. The proposed methods are intended to maintain forward secrecy, reduce the risk of BLUFFS-related attacks and lower communication overhead compared with Enhanced-Legacy Secure Connections (E-LSC). Both proposed protocols use 8 packets for session establishment, which is the same as standard LSC and less than the 10 packets used by E-LSC. Therefore, the counter-based method provides a practical balance between security, efficiency and compatibility with Bluetooth BR/EDR..

Keywords: Bluetooth BR/EDR, Session Key, Counter, C-LSC, C-LSC+, Forward Secrecy, BLUFFS, MAC, Legacy Secure Connections.

I. INTRODUCTION

Bluetooth is a popular technology for short-range wireless communication. It is used in computers, smartphones and many other connected devices. Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) communication uses session keys to protect the data exchanged between two devices. Because of this, the process used to create a session key is an important part of Bluetooth security.

A secure session key process should not only protect the current communication session. It should also help protect the confidentiality of earlier and later sessions. This property is known as forward secrecy. If an attacker can change or control important values during key establishment, the security of communication sessions can be affected.

Recent research and attacks, including the BLUFFS attack, have shown weaknesses in Bluetooth session key establishment. These attacks demonstrate that values used to determine the session key may be manipulated, which can reduce the secrecy of communication. Therefore, there is a need for a method that provides stronger protection without adding too much communication or processing overhead.

Enhanced-Legacy Secure Connections (E-LSC) attempts to improve security by adding random values, Message Authentication Codes and extra communication steps. Although these measures improve protection, they also increase the number of packets, processing time and overall protocol complexity.



The proposed counter-based approach tries to solve this issue by using a counter as a fresh value instead of repeatedly sending large random values. The C-LSC and C-LSC+ protocols are designed to provide the required security while keeping the session establishment process efficient and compatible with existing Bluetooth mechanisms.

II. NEED OF THE STUDY

Bluetooth is being used in a growing number of devices, making secure and efficient session establishment increasingly important. Security improvements should not create unnecessary communication overhead because many Bluetooth devices have limited resources and need efficient wireless communication.

This study is needed to understand the weaknesses of the standard Legacy Secure Connections process, examine the effect of the BLUFFS attack on forward secrecy, and study the efficiency limitations of E-LSC. The proposed counter-based protocols aim to provide stronger security while using fewer packets than E-LSC.

The study also focuses on compatibility with existing Bluetooth standards. Using the standard key derivation function helps keep the proposed approach close to the current Bluetooth session establishment process.

III. PROBLEM STATEMENT

The standard Bluetooth session establishment process has weaknesses that may allow an attacker to influence values used for creating a session key. In particular, the BLUFFS attack can affect the secrecy of both previous and future communication sessions. This creates a need for better protection of the values exchanged during session establishment. E-LSC provides stronger protection by using random values and MAC-based integrity checking. However, these additional security steps increase protocol complexity. Extra random values, MAC exchanges and packets can increase communication overhead and the time needed to establish a session.

Therefore, this study focuses on developing a secure and efficient session key establishment method for Bluetooth BR/EDR. The method should protect against BLUFFS-related weaknesses, maintain forward secrecy, reduce communication overhead and remain compatible with existing Bluetooth communication mechanisms.

IV. EXISTING SYSTEM

4.1 Standard Legacy Secure Connections (LSC)

Standard LSC uses the existing Bluetooth session establishment process to generate session keys. It is designed for Bluetooth BR/EDR communication. However, under the attack conditions discussed in this research, important key-determining values may be manipulated, reused or exchanged without enough integrity protection.

4.2 Security Vulnerability

The values used to determine a session key are important because they directly affect the final key. If an attacker can interfere with these values or influence the key establishment process, the security of the resulting communication session can be weakened.

4.3 BLUFFS Attack

The BLUFFS attack shows a weakness in Bluetooth session key establishment. An attacker may interfere with the establishment process and cause weak or repeated session keys. Such an attack can affect the secrecy of both earlier and later sessions, making secure session establishment an important requirement.

4.4 Enhanced-LSC

E-LSC improves security by adding random values and MAC-based integrity protection. These features make it more difficult to manipulate session key parameters. However, E-LSC also needs more packets and additional processing steps, which increases execution time and protocol complexity.

4.5 Limitation of Existing System

The main challenge in the existing system is the balance between security and efficiency. Adding more security messages and random values can improve protection, but it also increases communication overhead. The proposed work attempts to reduce this overhead while keeping the required security features.



V. PROPOSED SYSTEM

This research proposes two counter-based protocols called Counter-Based Legacy Secure Connections (C-LSC) and C-LSC+. Both methods use a counter (CTR) as a fresh value instead of repeatedly transmitting large one-time random values. MACs are used to protect the integrity of the counter values exchanged between the devices.

C-LSC uses counter synchronization. In this approach, both communicating devices maintain a coordinated counter value that can be checked during session establishment. C-LSC+ uses a different approach that does not require counter synchronization, making it useful when synchronized counter storage is not available.

The proposed protocols are designed to provide protection against BLUFFS while reducing communication overhead. Both C-LSC and C-LSC+ use 8 packets for session establishment, which is the same number used by standard LSC and fewer than the 10 packets required by E-LSC.

The protocols also use the standard key derivation function. This helps maintain compatibility with existing Bluetooth systems and may make firmware-level integration with existing BR/EDR Bluetooth stacks possible.

VI. PROTOCOL OPERATION

6.1 Counter-Based Fresh Value

A counter is used as a fresh value during session key establishment. Instead of sending large one-time random values repeatedly, the counter provides a changing value for the protocol. This approach is intended to provide freshness while reducing communication overhead.

6.2 Integrity Protection Using MAC

Message Authentication Codes are used to protect the counter values during transmission. This helps prevent an attacker from changing a counter value without being detected. Efficient use of MAC mechanisms is an important part of the proposed protocol.

6.3 C-LSC

C-LSC uses synchronized counters. The two communicating devices keep their counters synchronized so that the counter used during session establishment can be checked by both sides. This provides an organized way to use the counter as a fresh value.

6.4 C-LSC+

C-LSC+ uses a counter-based method without requiring synchronization. This can be useful when maintaining synchronized counters is difficult. It still uses the counter and MAC-based integrity protection to support secure session establishment.

6.5 Session Establishment

The proposed protocols complete session establishment using 8 packets. The counter and efficient MAC mechanisms help improve security without requiring the extra packet exchanges used by E-LSC.

VII. PURPOSE, OBJECTIVES AND SCOPE

7.1 Purpose

The main purpose of this work is to improve the security of Bluetooth BR/EDR session key establishment. It aims to protect communication sessions from attacks that can affect forward and future secrecy, while also reducing the complexity and communication overhead introduced by existing security methods.

Another purpose is to develop an efficient method that can remain compatible with existing Bluetooth standards. The use of counters, MAC-based integrity protection and the standard key derivation function supports this goal.

7.2 Objectives

- To study weaknesses in the standard Bluetooth session key establishment process.
- To understand the BLUFFS attack and its effect on forward secrecy.
- To identify the efficiency problems of the E-LSC protocol.
- To develop counter-based methods for session key establishment.



- To use MAC mechanisms for efficient integrity protection.
- To compare packet count, execution time, security and compatibility of the proposed protocols.

7.3 Scope

- The work mainly focuses on Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR).
- It covers session key establishment and protection against BLUFFS-related weaknesses.
- It considers both synchronized and non-synchronized counter approaches.
- It evaluates security, protocol efficiency and compatibility with standard Bluetooth mechanisms.
- It considers possible firmware-level integration with existing BR/EDR Bluetooth stacks.
- It also considers support requirements for older devices that do not have counter storage or synchronization capabilities.

VIII. SECURITY CONSIDERATIONS

Security is the main reason for introducing the counter-based approach. The proposed protocols are designed to protect the session key establishment process from BLUFFS-related attacks. MACs provide integrity protection for the counter values, making it harder for an attacker to modify these values without detection.

Forward secrecy is another important security goal. C-LSC and C-LSC+ are intended to maintain forward secrecy while also making session establishment more efficient. Instead of improving security only by adding more communication, the counter-based design attempts to achieve a balance between security and performance.

IX. PROTOCOL ADVANTAGES AND PERFORMANCE

One major performance benefit of C-LSC and C-LSC+ is that they require fewer packets than E-LSC for secure session establishment. Both proposed protocols use 8 packets, while E-LSC uses 10 packets.

According to the results provided in the research presentation, C-LSC is 15.6% faster than E-LSC, while C-LSC+ is 10.4% faster than E-LSC. These results indicate that the counter-based approach can reduce execution time while maintaining the required security properties.

The proposed protocols are also designed to preserve forward secrecy and provide protection against BLUFFS. Since they use the standard key derivation function, they can remain compatible with existing Bluetooth systems.

Protocol	Packets	Relative Performance	Key Feature
E-LSC	10	Reference	Random values and MAC-based protection
C-LSC	8	15.6% faster than E-LSC	Counter with synchronization
C-LSC+	8	10.4% faster than E-LSC	Counter without synchronization

9.1 Security Advantage

C-LSC and C-LSC+ are designed to maintain forward secrecy and protect against BLUFFS while using the same 8-packet establishment count as standard LSC. MAC mechanisms protect the integrity of counter values, and the counter provides a fresh value during session establishment.

9.2 Efficiency Advantage

Using fewer packets than E-LSC reduces communication overhead. The reported execution-time improvements also indicate that the proposed approach can improve security without adding the same amount of communication complexity as E-LSC.

9.3 Compatibility Advantage

The proposed protocols use the standard key derivation function, which supports compatibility with existing Bluetooth systems. This may allow firmware-level integration with existing BR/EDR Bluetooth stacks. However, older devices without counter storage or synchronization support may need additional support.



X. DISCUSSION

The results show that counter-based session establishment can provide a useful balance between security and performance. E-LSC adds security features but also requires additional packets and procedures. C-LSC and C-LSC+ attempt to reduce this overhead through the use of counters and efficient MAC mechanisms.

C-LSC is based on synchronized counters, while C-LSC+ removes the need for synchronization. Therefore, the two approaches can be considered for different implementation conditions. Both approaches have the same overall goal of making Bluetooth session key establishment secure and efficient.

XI. CONCLUSION

Bluetooth session establishment needs strong protection against new and evolving security attacks. The BLUFFS attack has shown that weaknesses in the session key establishment process can affect the secrecy of communication sessions. Although E-LSC improves security by adding random values, MAC exchanges and extra communication procedures, these additions also increase overhead.

The proposed Counter-Based Legacy Secure Connections (C-LSC) and C-LSC+ protocols use counters and efficient MAC mechanisms to achieve a better balance between security and performance. C-LSC uses counter synchronization, whereas C-LSC+ works without synchronization. Both methods are designed to preserve forward secrecy and provide protection against BLUFFS-related weaknesses.

An important feature is that C-LSC and C-LSC+ complete session establishment using 8 packets, which is the same as standard LSC, while E-LSC requires 10 packets. The provided results report that C-LSC is 15.6% faster than E-LSC and C-LSC+ is 10.4% faster than E-LSC. Using the standard key derivation function also helps maintain compatibility with existing Bluetooth systems.

Overall, the counter-based approach provides a possible way to improve the security and efficiency of Bluetooth BR/EDR communication. Its main contribution is to maintain strong security and forward secrecy while reducing communication overhead and keeping compatibility with existing Bluetooth mechanisms.

XII. FUTURE SCOPE

In the future, the proposed counter-based protocols can be studied for practical firmware-level integration with existing Bluetooth BR/EDR stacks. Further work can focus on supporting legacy devices that do not have counter storage or synchronization capabilities. Testing on different Bluetooth devices and in different environments can also help evaluate the practical behavior of the protocols while maintaining their security and efficiency goals.

REFERENCES

- [1] Provided IEEE research paper on Counter-Based Session Key Establishment Protocol for Efficient and Forward Secrecy in Bluetooth BR/EDR.
- [2] Bluetooth BR/EDR security and Legacy Secure Connections material referred to in the provided research presentation.
- [3] Enhanced-Legacy Secure Connections (E-LSC) and BLUFFS-related security discussion provided in the source material.
- [4] Provided presentation: "Counter-Based Session Key Establishment Protocol for Efficient and Forward Secrecy in Bluetooth BR/EDR", covering the introduction, problem statement, existing system, proposed system, objectives, scope, performance and conclusion.

