

Middle East Technical University  
Department of Computer Engineering  
Wireless Systems, Networks and Cybersecurity (WINS) Laboratory



# An Implementation of BlindBox: Deep Packet Inspection over Encrypted Traffic

CENG781 Network Security  
2018-2019 Spring  
Term Project Report

Prepared by  
Cansin Yildiz, Fatma Demirtas, Seyma Bodur  
Student ID: 1449271, 1927961, 1854512  
cansin.yildiz@metu.edu.tr, fatma.demirtas@metu.edu.tr, bodur.seyma@metu.edu.tr  
Computer Engineering  
25 March 2019

# Table of Contents

List of Figures . . . . .	iii
1 Introduction . . . . .	1
2 Related Work . . . . .	2

## List of Figures

Figure 1	BlindBox Architecture . . . . .	1
----------	---------------------------------	---

# 1 Introduction

Deep Packet Inspection (DPI), which is the computer network filtering technique, controls the content of the traffic and traffic flow [2]. DPI is used in several areas such that protection to security threats, lawful interception, parental filtering. There are middleboxes to provide the functionality of DPI. In other words, Middleboxes should ensure security. However, there is a problem with some middleboxes: while providing security, they do not put emphasis on privacy. BlindBox, which is a middlebox presented in this report, provide both functionality of the DPI and privacy of the packets. If the BlindBox is used as middlebox, there is no need to decrypt the payload. Inspecting packets is made over encrypted payload.

BlindBox ensures the following properties:

- As all middleboxes do, BlindBox seek for suspicious content for security.
- Sender and receiver do not have knowledge of the rule.
- BlindBox should have at least one trusted endpoint as in intrusion detection (IDS).
- There is no permission for BlindBox to read the traffic unless there is no found suspicious content.

The last property is special for BlindBox, other middleboxes does not provide it.

Below figure shows how BlindBox works:

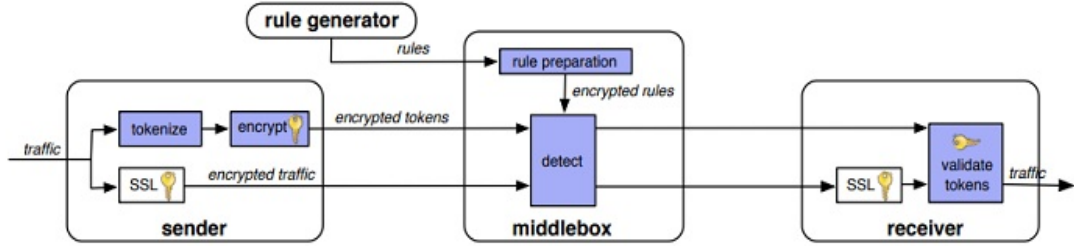


Figure 1 . BlindBox Architecture

There are three different keys to use in this scheme. First one is  $k_{SSL}$  which is used in SSL protocol. The second one is  $k$  which is used for detection. The last one is  $k_r$  and which is used for randomness. These three keys are generated/derived by  $k_0$  which is the key sender and receiver agree by SSL Handshake. In that way, sender and receiver are connected.

As it is seen in the figure, there is a connection between the rule generator and the middlebox. Rule generator encrypts keywords/rules with the key  $k$ . And middlebox gets these rules to detect suspicious content without the knowledge of the key  $k$ . While this happening, endpoints should not have the knowledge of the rules, too.

After these connections, traffic should be encrypted with SSL by the sender as we can see in the Figure. Then, the sender starts to divide the traffic into substring to tokenize. These tokens are sent after encrypted with DPIEnc. DPIEnc works as

$$salt, AES_{AES_k(t)}(salt)modRS$$

where salt is random number,  $t$  is token,  $k$  is key and  $RS$  which reduced the size of ciphertext is  $2^{40}$

When the traffic comes to the middlebox, BlindBox Detect algorithm seek for a match between encrypted tokens and encrypted rules. If any suspicious content found in the traffic, it could be stopped or dropped as what is required. Otherwise, the traffic is sent to the receiver.

When the traffic comes to the receiver, it is decrypted and receiver authenticates the traffic using SSL. Also, the receiver controls whether encryption of the tokens is done correctly or not.

## 2 Related Work

There are many related works on middleboxes. Some of them are accepted insecure. As explained in [5], man in the middle attack is built using counterfeit certificates on SSL by some systems. In that way, security of the SSL could be broken, and middlebox can decrypt the traffic for detection scan. That is, E2E security of SSL is destroyed which is insecure. In addition, there is a system called Meddle [6]. Its goal is to increase transparency in mobile networks. This is done by endpoints and the third-party are authorized to control the traffic, which is not required in BlindBox. The systems APLOMB [7] and Beyond the Radio [9] are similar to Meddle.

Some middleboxes use encrypted payload for detection. But, they have some properties that are not required for BlindBox. For example, fully homomorphic encryption[4] and general functional encryption [3] can be used in order to encrypt the payload. Their computation speed is so slow when they are compared with an encryption scheme used in BlindBox.

Also, searchable encryption schemes can be used in order to encrypt the rules. However, such schemes encrypt the rules in such a way that it does not meet the security which BlindBox require. In addition, symmetric key searchable scheme [8] and public key encryption with searching [1] can also be used for packet processing. However, they have some weakness: symmetric key searchable scheme is slower than the scheme which BlindBox uses, and the public key searchable scheme is also not proper for performance because it should create cryptographic pairs for each token.

All these means, security and speed desires cannot be obtained by all these encryption schemes. Therefore, BlindBox uses different encryption scheme which is called DPIEnc. DPIEnc takes the speed of deterministic searchable encryption scheme and it takes the security of the randomized encryption scheme.

## References

- [1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search. 2004.
- [2] C.Fuchs. Implications of deep packet inspection (dpi) internet surveillance for society, 2012.
- [3] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. 2013.
- [4] C. Gentry. Fully homomorphic encryption using ideal lattices. 2009.
- [5] L.-S. Huang, A. Rice, E. Ellingsen, and C. Jackson. Analyzing forged ssl certificates in the wild. 2014.
- [6] A. Rao, J. Sherry, A. Legout, W. Dabbout, A. Krishnamurthy, and D. Choffnes. Meddle: Middleboxes for increased transparency and control of mobile traffic. 2012.
- [7] J. Sherry, S. Hasan, A. Krishnamurthy C. Scott, S. Ratnasamy, and V. Sekar. Making middleboxes someone else’s problem: Network processing as a cloud service. 2012.
- [8] D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. 2000.
- [9] N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, N. Weaver, and V. Paxson. Beyond the radio: Illuminating the higher layers of mobile networks. 2015.