ICAI 2023
12th International Conference on Applied Informatics
Eger, Hungary, 2023

Scalix mix network*

Ádám Vécsi[a], **Dr. Attila Pethő**[b]

University of Debrecen, Faculty of Informatics, Department of Computer Science
[a]adam.vecsi@inf.unideb.hu

[b]attila.petho@inf.unideb.hu

Abstract

Mix networks are protocols meant to provide anonymous communication against adversaries, who can observe all the traffic in the network. Unfortunately, reaching this level of security usually comes with the cost of high latency. Although that is why recent research focuses on decreasing the communication latency while providing the desired security, they ignore scalability and load balancing. Our work offers a solution to these bottlenecks using Identity-based Encryption and Attribute-based Encryption.

Introduction

A mix network is a system designed by Chaum [1] that includes multiple stages of mixes, where every stage receives multiple messages, performs some cryptographic transformation for each message, and permutes them. After every mix, tracking the path of the messages gets more and more complex, achieving untraceability. Unfortunately, the path is usually picked by the message sender randomly or by their preferences, which is contra-productive in two different ways.

In systems like this, load balancing is crucial to prevent the over and underload of nodes. While the former affects only the performance, the latter could decrease anonymity in the system if nodes mix an inadequate amount of messages.

Furthermore, to handpick the path, users have to be able to reach a database of all the mix nodes in the system. Managing this information could be challenging and costly, which increases more and more when the system is upscaling (more users mean more requests, and more mix nodes mean a bigger database).

*The research was supported by the 2018-1.2.1-NKP-2018-00004 Security Enhancing Technologies for the Internet of Things project.

We propose a mix network that keeps the achievements of recent research [2] targeting low latency communication and is also well balanced and needs a much smaller database. These are achieved by applying a combination of identity-based encryption (IBE) and attribute-based encryption (ABE).

Scalix topology

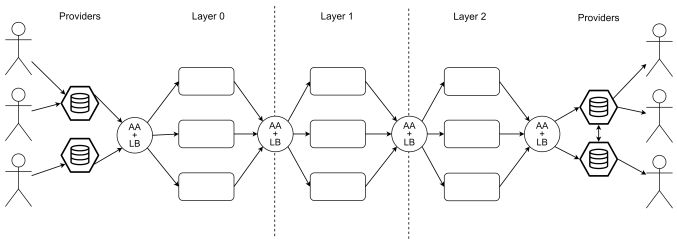

Figure 1. The topology of the Scalix mixnet

Our protocol is built on the fundamentals of Loopix however, its topology is extended with nodes marked as $AA + LB$ on Figure 1, which serve as attribute authority (AA) and load balancer (LB) in the system. Unlike other protocols, in ours, the message sender does not pick the mix nodes the message travels through but the $AA + LB$ node that is located before each layer. The $AA + LB$ node picks the mix node.

We are using multi-authority ABE [3] to efficiently create a single-use decryption key, which is required for only the specified node (the one picked by the $AA + LB$) to be able to do the mix operations. Figure 2 shows how this concept works in our system. Every mix node has one long-term attribute $attr_{layer}$, which is the layer it gets assigned to when it registers to the system, and a single-use attribute $attr_{revoc}$, which is only active for one decryption of a specific packet and gets revoked instantly. When the message sender creates a packet, he encrypts it with a policy that makes both attributes mandatory. This way, even if the packet gets leaked, it can not be decrypted since no one satisfies the $attr_{revoc}$ part of the policy. Once the packet is created, it is sent to the $AA + LB$, which will pick a mix node and assigns the $attr_{revoc}$ to it. After the mix node finishes with its work, the attribute gets revoked.

Scalix packet format

One requirement for our packet format is the usage of ABE with the property of constant-size ciphertext so that the packets will be the same size between any station of their path and the same as all other packets' sizes. This property is required in the case of mix networks to make the packets indistinguishable.

The packet of our system can be separated into a header and a body part. Both parts are built in an onion structure. Each layer of the structure targets one mix layer, containing only the necessary information for the mix node to perform the mix operation.

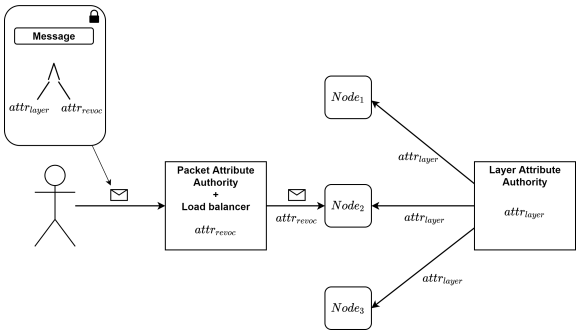

Figure 2. Encrypt to a load balancer picked target in a group

The header includes the delay amount for the Poisson mix strategy and the destination to forward the mixed packet for every mix layer. The destination is an $AA + LB$ in all the layers, except the core of the onion structure, where we can find the address of the receiver's provider concatenated with a fixed amount of random bits. The random bits are required to avoid a dictionary attack since the providers' identities may be known in the system. The receiver's provider is included in the header as a destination so that the load-balanced provider can forward the packet to the correct destination. The core part is also necessary from a security aspect. The packets should have the same size before and after every mix to hide the information about the packet's position in its path and make the packets more indistinguishable. Without the core part of the header, the packet would lose half it's size after the final mix.

To build the body, the sender first generates an Advanced Encryption Standard (AES) key and encrypts the message using it. After that, the sender encrypts the AES key using IBE targeting the receiver's identity. Then, since the receiver's identity should only be known by its provider, the sender encrypts the receiver's identity with the IBE targeting its provider. Finally, the last part of the body's core is to create the cryptographic hash of the encrypted core of the header. In each layer of the onion structure, there is a cryptographic hash of the corresponding header part. This hash allows the mix nodes to verify before the mixing operation that the header was not modified.

References

[1] D. L. Chaum: *Untraceable electronic mail, return addresses, and digital pseudonyms*, Communications of the ACM 24.2 (Feb. 1981), pp. 84–90, URL: https://doi.org/10.1145/358549.358563.

[2] A. M. Piotrowska, J. Hayes, T. Elahi, S. Meiser, G. Danezis: *The Loopix Anonymity System*, in: 26th USENIX Security Symposium, 2017, pp. 1199–1216, URL: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-piotrowska.pdf.

[3] X. Zhang, F. Wu, W. Yao, Z. Wang, W. Wang: *Multi-authority attribute-based encryption scheme with constant-size ciphertexts and user revocation*, en, Concurr. Comput. 31.21 (Nov. 2019), URL: https://doi.org/10.1002/cpe.4678.