Research Article

Open Access

CrossMark

Elliptic curve based server authentication system for multi-server infrastructure

Abstract

A server authentication scheme for a multi-server infrastructure has been proposed. In this scheme, each member involved in communication has to prove its authentication before any information is exchanged. This scheme secures the servers against phishing and other such attacks. Dynamic properties of the group are handled with ease, making the scheme suitable for real-life applications.

Keywords: elliptic curve cryptography, visual cryptography, multi server system, group communicating server

Volume 2 Issue 5 - 2018

Nancy Girdhar,[1] Himanshu Monga[2]

[1]Department of computer science and engineering, JCDM COE, India

[2]Principal JCDM COE, Sirsa, India

Correspondence: Himanshu Monga, Principal JCDM COE, Sirsa, India, Tel +919418030062 ,
Email himanshamonga@gmail.com

Received: July 24, 2017 | **Published:** November 28, 2018

Introduction

Over the years different authentication schemes have been proposed by the researchers. But most of them are either incompetent or take too much time to respond which makes them useless for real life applications.[1] However,[2–4] have proposed authentication schemes using cryptographic techniques, but the existing schemes are mostly defined for specific type of groups. They provide authentication at user side but not at server side. In practical scenario forgery attacks may occur at server side as well. In this paper we propose an authentication scheme based on elliptic curve cryptography and visual cryptography, to protect the distributed servers form such attacks. Visual cryptography, proposed[5] is a technique, devised for sharing images securely. In visual cryptography scheme, an image is divided into n shares, out of which k shares alone mean nothing, thus protecting the information stored in the image safe.[2] Proposed scheme is appropriate for a multi-server infrastructure in which group of members are connected to one of the many interconnected group communicating servers. Although there exists various multi-signature schemes for multi-server infrastructure, but in multi-signature schemes there is a fundamental drawback. In those schemes, the authentication center could be exploited by forging the signatures thus those schemes are vulnerable to attacks. Proposed scheme conquers all such forgery attacks as the communicating members provide their identity and also the identity of their group in terms of image shares. The remainder of the paper is organized as follows: Section 2 describes the multi-server infrastructure, on which the server authentication scheme has been proposed. In section 3, proposed scheme has been discussed. In section 4 we discuss the implementation of system on the basis of our proposal. Section 5 discusses the dynamic alterations and adjustments in the group and in the end section 6 gives the conclusion and future scope.

Multi-server systems

Multi-Server systems generally have distributed servers. In a multi-server system Group Communication Servers and members together constitute groups. Within a group, members are connected to GCS. GCSs of various groups are interconnected and are responsible for all the communication. This scenario is common for Multinational companies or companies that deal with large amount of data.[1]

Figure1 shows one such multi-server scheme. In this figure two groups have been shown, their GCSs are connected to each other and each GCS is also connected to four members. A member can access data from a member of the same group or a member of other group. All the communication, whether it's inter-group or intra-group takes place via GCSs. While communicating GCS acts as a mediator between the involved members, it receives and delivers messages securely on their behalf. In case of inter group communication the members communicate messages to their own GCSs and then the respective GCSs of the involved groups communicate to each other. As all the communication is carried out via GCSs, thus they play an important role in the security and information exchange. Various priority algorithms are used at GCSs so as to make sure there are no prolonged delays in data delivery.

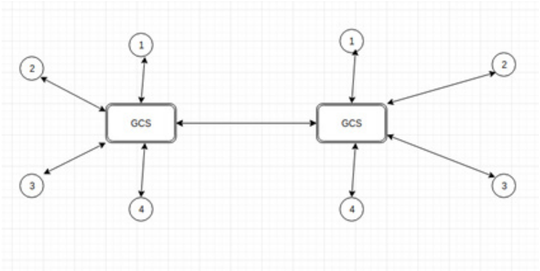

Figure 1 Multi-server infrastructure.

Proposed scheme

Proposed scheme works as follows: Let's assume, a member of the group1 wants to communicate with a member of group2. So he will contact his server, let's call it GCS1. Now GCS1 asks the member to authenticate itself. After verifying the identity of the member, GCS1 gets itself verified. After all this authentication GCS1 informs the other GCS, say GCS2 and all the other members of his own group. Each and every member involved in the communication authenticates itself and provides his share of the group's proof of authenticity, that is group's image share . GCS uses the individual image shares to generate a group verification image share. This image share is validated by other GCS and all the group members. This way both the groups authenticate each other. This scheme works on the assumption of there being a public directory that stores verified image shares of all different groups. The concerned party can verify the authenticity by overlapping the public share over the received share, and if product is uniform original image then the group is said to be genuine, and if the image is distorted from any part then group is said to be compromised and connection is broken. Elliptic curve cryptography plays an essential role in member- -server authentication procedure to keep the image shares secure. Elliptic curve cryptography was introduced by [6,7] in 1985. All the distributed servers are placed such that, they give the impression that they have been placed on an elliptic curve and the main calculation associated is in performing the operation Q=nP which is the equivalent to the addition of p to itself n times. Here Q and P are the points on the curve and n is an integer known as the scalar multiplier. Security of the procedure is proportional to the infelicity of determining n from Q=nP, provided Q and P, this problem is known as elliptic curve discrete logarithm problem.[8] This is because of the fact that addition of two points on an elliptic curve yields another point on the same elliptic curve.

System set up and initialization

GCSs are set up and are interconnected to each other thus a network of servers is established. Group members are connected to GCSs. An elliptic curve is chosen with a generator g having large prime order q, along with some additional parameters. Individual public and private keys are conceived all members including GCSs. These keys are used for intra-group authentication purposes. After that a group key for group identification and authentication is created and is stored on a public directory. This key is used for inter-group authentication (Figure 2).

a. An elliptic curve having a point g as its generator is elected, and a one-way hash function H(.) is chosen.
b. Each member elects a random integer let ‘a’ as its private key where value of a may vary from 0 to q-1, where q is the order of elliptic curve for that particular group.
c. Using the elliptic curve discrete logarithm equation Q_a=aP, Each member generates its public key Q_a and broadcasts it.
d. Similarly Each GCS elects his private key assume ‘b’, uses this to generate public key let Q_b and then broadcasts the public key.
e. Now group public key ‘Q’ is calculated by adding all the previously generated keys.

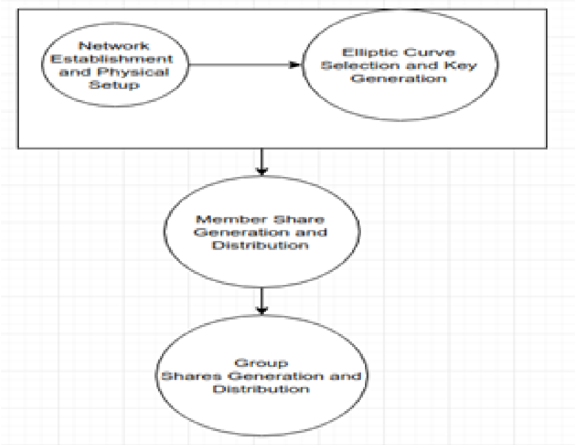
Network Establishment and Physical Setup
Elliptic Curve Selection and Key Generation
Member Share Generation and Distribution
Group Shares Generation and Distribution

Figure 2 System set up and initialization.

For a member to be able to identify itself, it needs to have some sort of identity proof. In our scheme a member creates his own identity in the form of an image share. Each member including GCS chooses an image of his will and creates two shares of the image using visual cryptography. Each member distributes one share along with the original image to all the other members of the same group. While distributing the shares they are encrypted using public keys of the receivers. Group members keep the received shares and images private. These personal image shares are used for authentication purpose later in the communication. For a group to communicate with another, it needs to prove its authenticity to another group. In order to prove its authenticity a group needs to have an identity proof, which authenticates the whole group at once. So as to achieve that during setup phase GCS chooses an extra image. This image is approved by each and every member of the group before being put to use. After the image is approved, GCS creates n+1 shares of the chosen image(where n is number of members in the group including the server). One share is uploaded onto the public directory and rest of the shares are distributed in the group, one to each member.

Prototype implementation

Main factors that vouch for our design are, the feasibility of the system, ease of installation & use, and less cost of computation. This authentication scheme can be tested upon home computers, by operating them as servers. Figure 3 shows a group structure from a multi-server system with two GCSs where each GCS have two members. Scheme works as: First a member of group1, say M1 wants to communicate with member m4 of group2, so it informs the server(GCS1) of the communication it wants to make. GCS1 asks the member to authenticate his identity. M1 transfers his share of the image encrypted using GCS1’s public key and asks the GCS1 to authenticate himself. GCS1 after receiving the image share decrypts it using his private key and then the two shares, one received now and the other that was given to the receiver during setup phase, are stacked transparently and in a way that their pixels align properly to generate the original image. If the previously sent image and the reproduced image reckoned to be same then the sender is said to be authenticated. After authenticating the member GCS1 forwards the member his image share encrypted using M1’s public key and forwards M1’s share to all the other members to inform them of the communication that’s about to occur. M1 authenticates the GCS1 in exactly same manner. After all the authentication GCS1 asks the members to transfer their share of the group’s image. After receiving those shares GCS1 overlaps them with his share and generates one single share from those n shares then encrypts it using the other GCS’s say GCS2’s public key and transfers it over to prove its authenticity and asks GCS2 to authenticate his group. GCS2 follows the exact same procedure and proves group’s authenticity. After the authenticity has been proven further communication takes place. Computation cost of the scheme can be calculated by calculating the cost at a node as except the share stacking process all other steps are common to all members.

In Table 1, ECE stands for Elliptic Curve Encryption, ECD represents Elliptic curve decryption and stacking represents overlapping operation and similarity check represents image recognition operation.

Handling dynamic property of the group

As the groups are not static, some members may leave and some new may join, so any proposed scheme must be able to handle these scenarios and dynamic property of the group.[1]

New addition to the group

Let a new member is added to the group at some point of time.

When any new member joins the group setup procedure is called again. In this phase GCS of the group asks the member to create his identity, and create a member share. Member also generates his public and private keys. After receiving image share and image from new member, every other member including GCS gives his share of the image to the new member along with their original images. The group image is also changed, GCS chooses a new image, creates shares accordingly and passes them all to the group members. GCS also changes the share stored at public directory.

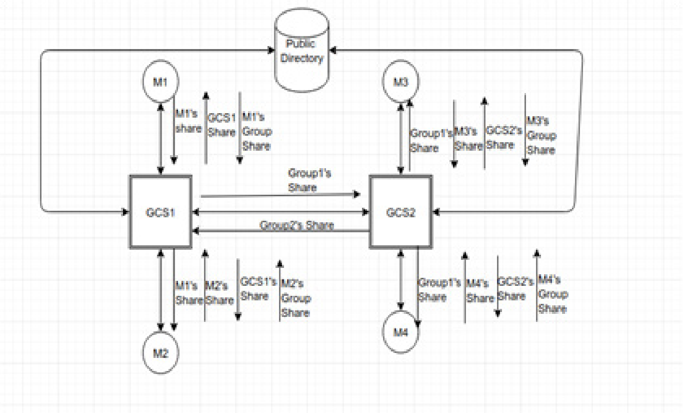

Figure 3 Prototype implementation.

Table 1 Computation cost

Operation	Cost in prototype	Cost in group with n members
Encryption	2ECE	2*n*2*ECE
Decryption	1ECD	2*n*ECD
Stacking	1	n+1
Similarity Check	1	n

Member leaving the group

When a member leaves the group every other member including GCS deletes both, his share of the image and the originally received image. GCS also changes the group image. GCS chooses a new image. Creates share according to the number of members in the group after the modification, transfers the new shares to the members and then changes the share at the public directory.

Conclusion

An authentication scheme has been proposed for multi-server has been proposed. Each member needs to prove its authenticity twice, once as an individual and later as a group member, thus making sure no intruder could break the security by forging someone's identity. Dynamic properties of the groups are handled with utmost ease, ensuring the real life applications of our authentication scheme.

Acknowledgments

None.

Conflicts of interest

The author declares no conflicts of interest.

References

1. Santosh Ghosh, Dipanwita Roy Chowdhury. Elliptic Curve Based Multi-signature Scheme for Multi-server Systems. *TENCON 2008 - 2008 IEEE Region 10 Conference*. 2008.
2. Parveen Kumar P, Sabitha S. User Authentication using Visual Cryptography. *2015 International Conference on Control Communication & Computing India (ICCC)*. 2016.
3. G Eason, B Noble, IN Sneddon. On certain integrals of Lipschitz Hankel type involving products of Bessel functions. *Phil Trans Roy Soc London*. 1955;247(935):529–551.
4. Chetana Hegde, Manu S, P Deepa Shenoy, et al. Secure Authentication using Image Processing and Visual Cryptography for Banking Applications. *2008 16th International Conference on Advanced Computing and Communications*. 2008.
5. M Naor, A Shamir. Visual Cryptography. *Advances in Cryptography -EUROCRYPT'94*. 1995.
6. N Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*. 1987;48(177):203–209.
7. V Miller. Use of elliptic curves in cryptography. *Advances in Cryptology — CRYPTO '85 Proceedings*. 2000;218:417–426.
8. Andrew Odlyzko AT. Discrete Logarithms: The Past and the Future. *Designs, Codes and Cryptography*. 2000;19(2–3):129–145.

Citation: Girdhar N, Monga H. Elliptic curve based server authentication system for multi-server infrastructure. *Electric Electron Tech Open Acc J*. 2018;2(5):313–315. DOI: 10.15406/eetoaj.2018.02.00034