Scientific Journal of Impact Factor (SJIF): 3.134
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 2, February -2016

Authenticated Key Exchange Protocols for Parallel Network File Systems

Megharaj Patil[1], Sonali Rangdale [2]
[1,2]Dept of Computer Engineering, Siddhant College Of Engineering ,

Abstract *— The problem is motivated by the proliferation of large-scale distributed file systems supporting parallel access to more than one storage devices i.e. to the multiple devices. Our work mainly focuses on the current Internet standard for such file systems, i.e. the parallel Network File System. This makes use of Kerberos for establishing the parallel session keys between the clients and the storage devices. Our analysis about the existing Kerberos-based protocol displays that it has a number of limitations. In this paper, we are trying to propose a variety of authenticated key exchange protocols which are designed to address the issues which were faced by the existing system. We show that our protocols are efficient to handle the reducing up to approximately of the workload of the metadata server and concurrently supporting forward secrecy and escrow-freeness. Only a small fraction of increased computation overhead at the client is what all required.*

Keywords- *Parallel Network File system (pNFS), Kerberos, forward secrecy, Escrow-free.*

I. INTRODUCTION

In parallel file system, the file data is spread across the multiple storage devices or nodes to allow the concurrent access by many different tasks of a parallel application. [7]This is frequently used in large-scale cluster computing that focuses on high performance and reliable access to large datasets. That is, higher I/O bandwidth is achieved through concurrent access to multiple storage devices within large compute clusters; while data loss is protected through data mirroring using fault-tolerant striping algorithms. [1]In this work, we examine the problems of secure many-to-many communications in large-scale network file systems which support the parallel access to multiple storage devices.

That is, we examine a communication model where there are a huge number of clients (potentially hundreds or thousands) accessing multiple remote and distributed storage devices (which also may scale up to hundreds or thousands) in parallel. Especially, we focus on how to exchange key materials and build parallel secure sessions between the clients and the storage devices in the parallel Network File System (pNFS).[6] The development of pNFS is driven by Netapp, Panasas, Sun, IBM, EMC and UMich/CITI, and thus it shares many common features and is compatible with many existing commercial/proprietary network file systems.

The primary goal here is to design an efficient and secure authenticated key exchange protocol that meets the specific requirements of pNFS. The main aim is to achieve the properties like scalability, forward secrecy, Escrow-free. The main aim of this paper is to propose a variety of authenticated key exchange protocol which is very efficient to handle the reducing up to approximately of the workload of the metadata server and concurrently supporting forward secrecy and escrow-freeness.[3] All this requires only a small fraction of increased computation overhead at the client. We define an appropriate security model and prove that our protocols are secure in the model.

II. LITERATURE REVIEW

1. FARSITE: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment
AUTHORS: A. Adya, W.J. Bolosky, M. Castro
Description:
This paper Farsite provides the file availability and reliability with the help of randomized replicated storage. They ensure the secrecy of the file contents with the help of cryptographic techniques. They also maintain the integrity of the file and the directory data with a Byzantine-fault-tolerant protocol. They designed a system which is scalable by using a distributed hint mechanism and delegation certificates for path name translations and also achieve good performance by locally caching file data, lazily propagating file updates, and varying the duration and the granularity of the content leases. Farsite is designed to support the files and also the I/O workload of desktop computers in a large company or university. It provides availability and reliability through replication; privacy and authentication through cryptography; integrity through Byzantine-fault-tolerance techniques; consistency through leases of variable granularity and duration; scalability through namespace delegation; and reasonable performance through client caching, hint based pathname translation, and lazy update commit.

2. Block level security for network-attached disks

AUTHORS: Marcos K. Aguilera, Minwen Ji, Mark Lillibridge

Description:

They propose a practical and efficient method for adding security to network-attached disks (NADs). Their design requires no changes to the data layout on disk, minimal changes to existing NADs, and only small changes to the standard protocol for accessing remote block-based devices. They have implemented a prototype NAD file system, called Snapdragon that incorporates their ideas. They also evaluated Snapdragon's performance and scalability. In this paper they have presented a new block-based security scheme for network-attached disks (NADs). In contrast to previous work, their scheme requires no changes to the data layout on disk and only minor changes to the standard protocol for accessing remote block-based devices.

3. Authenticated key exchange secure against dictionary attacks.

AUTHORS: M. Bellare, D. Pointcheval, and P. Rogaway

Description:

Password-based protocols for authenticated key exchange (AKE) are designed to work despite the use of passwords drawn from a space so small that an adversary might well enumerate, off line, all possible passwords. While several such protocols have been suggested, the underlying theory has been lagging. The author begin by defining a model for this problem, one rich enough to deal with password guessing, forward secrecy, server compromise, and loss of session keys. The one model can be used to define various goals. The author takes AKE (with "implicit" authentication) as the "basic" goal, and they give definitions for it and for entity-authentication goals as well. Then they prove correctness for the idea at the center of the Encrypted Key-Exchange (EKE) protocol of Bellovin and Merritt: they prove security, in an ideal-cipher model, of the two-flow protocol at the core of EKE.

4. Analysis of key-exchange protocols and their use for building secure channels

AUTHORS: Ran Canetti and Hugo Krawczyk

Description:

In this paper author presents a formalism for the analysis of key-exchange protocols that combines previous definitional approaches and results in a definition of security that enjoys some important analytical benefits: (i) any key-exchange protocol that satisfies the security definition can be composed with symmetric encryption and authentication functions to provide provably secure communication channels (as defined here); and (ii) the definition allows for simple modular proofs of security: one can design and prove security of key-exchange protocols in an idealized model where the communication links are perfectly authenticated, and then translate them using general tools to obtain security in the realistic setting of adversary-controlled links. This paper adopts a methodology for the analysis of key-exchange protocols. They follow the approach of the adversarial model.

5. Authenticated Key Exchange Protocols for parallel Network File Systems

AUTHORS: Hoon Wei Lim Guomin Yang

Description: In this paper the authors study the problem of key establishment for secure many-to-many communications. The problem is inspired by the proliferation of large-scale distributed file systems supporting parallel access to multiple storage devices. Their work focuses on the current Internet standard for such file systems, i.e., parallel Network File System (pNFS), which makes use of Kerberos to establish parallel session keys between clients and storage devices. They overcome the number of limitations: (i) a metadata server facilitating key exchange between the clients and the storage devices has heavy workload that restricts the scalability of the protocol; (ii) the protocol does not provide forward secrecy; (iii) the metadata server generates itself all the session keys that are used between the clients and storage devices, and this inherently leads to key escrow.

III. SURVEY OF PROPOSED SYSTEM

Our work mainly focuses on the current Internet standard for such file systems, i.e., parallel Network File System. This makes use of Kerberos for establishing the parallel session keys between the clients and the storage devices. Our review of the existing Kerberos-based protocol shows that it has a number of limitations. In this paper, we propose a variety of authenticated key exchange protocols that are designed to address the above issues. We show that our protocols are efficient to handle the reducing up to approximately of the workload of the metadata server and concurrently supporting forward secrecy and escrow-freeness. All this requires only a small fraction of increased computation overhead at the client.

IV. SYSTEM ARCHITECTURE

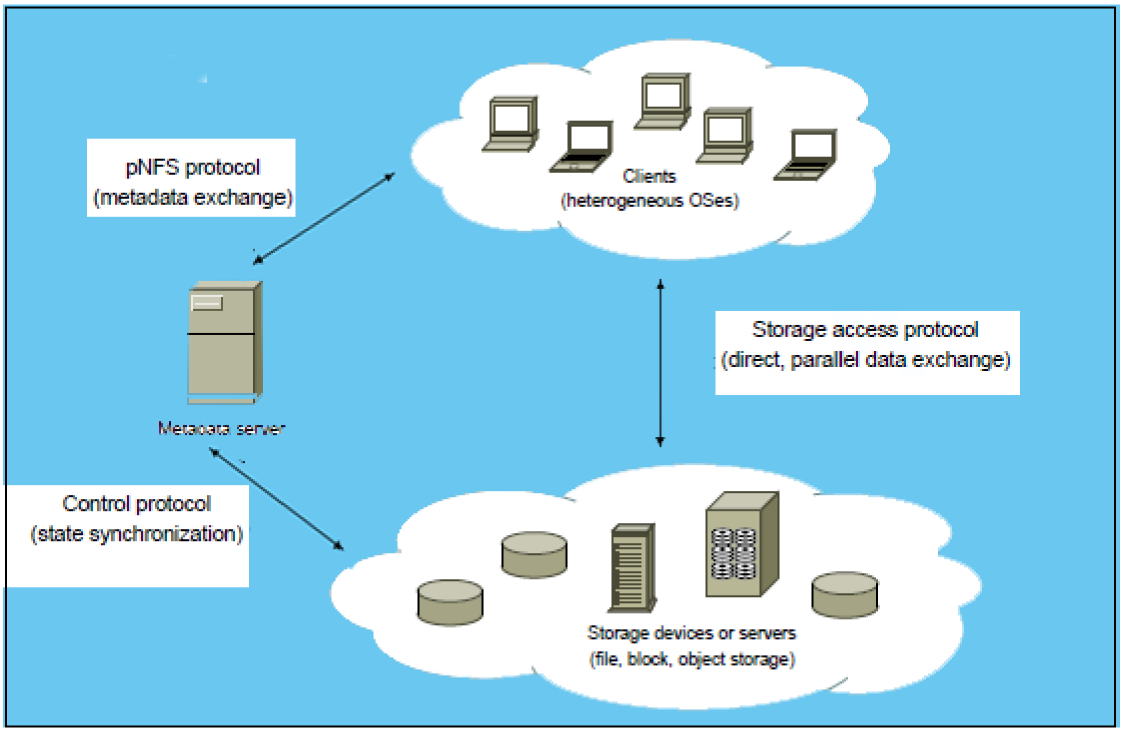

Fig 1: System Architecture

The system architecture is as shown in fig 1. The client can share the data, upload the files and also can download the files. The server has the authority to accept the users and the files. The files are then uploaded on the cloud. The uploadations of only three types of files are allowed i.e. the JAVA, DOT NET and the PHP file.

V. MODULES

The module description is as below,

1. Parallel Sessions

The parallel sessions are the parallel secure sessions between the clients and storage devices which are in the parallel network file system (pNFS). These are the current internet standards in an efficient and scalable manner. These are similar to the situations where once the adversary compromises the long-term secret key, it can learn the subsequence sessions. If an honest client and an honest storage device complete the matching sessions then they compute the same session key. Secondly two of our protocols provide forward secrecy: one is partially forward secure with respect to multiple sessions within a time period.

2. Authenticated key exchange

The primary goal in this work is to design the efficient and secure authenticated key exchange protocol that meets the specific requirements of pNFS. Three new provably secure authenticated key exchange protocols are the main results of this paper.We describe our design goals and give some intuition of a variety of pNFS authenticated key exchanged (pNFS-AKE) protocols that we consider in this work.

3. Forward secrecy

The protocol should guarantee the security of the past session keys when the long-term secret key of a client or a storage device is compromised as the protocol does not provide any forward secrecy. To address key escrow while achieving forward secrecy simultaneously, we incorporate a Diffie-Hellman key agreement technique into Kerberos-like pNFS-AKE-I. However, it is to be noted that we gain only partial forward secrecy, by trading efficiency over security.

4. Client

The Client performs the following tasks,

Share Data

The user can share their data into another user in same group then the data will translate by path setting data.

Upload Data
The user can upload the file to the cloud. And then the Admin can allow the data to store on the cloud.

Download File
The user can also download the cloud file by the conditions.

5. Server Authentication
Accept user
The admin can accept the new users request and can also block the users.

Allow user file
The users can upload the file to cloud. And the admin can allow the files to cloud then only the file can store the cloud.

6. CLOUD
Upload Data
The cloud can mostly upload the 3 types of files to users namely JAVA, DOT NET and PHP.

VI. CONCLUSION

We proposed the three authenticated key exchange protocols for the parallel network file system (pNFS). The three appealing advantages are offered by our protocols over the existing Kerberos-based pNFS protocol. Firstly the metadata server which is executing our protocols has much lower workload as compared to that of the Kerberos-based approach. Secondly, two of our protocols provide the forward secrecy: one which is partially forward secure, while other is the fully forward secure. Thirdly we also have designed a protocol which provides forward secrecy as well as is escrow-free.

VII. ACKNOWLEGEMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

VIII. REFERENCES

[1] M. Abd-El-Malek, W.V. Courtright II, C. Cranor, G.R. Ganger, J. Hendricks, A.J. Klosterman, M.P. Mesnier, M. Prasad, B. Salmon, R.R. Sambasivan, S. Sinnamohideen, J.D. Strunk, E. Thereska, M. Wachs, and J.J. Wylie. Ursa Minor: Versatile cluster-based storage. In Proceedings of the 4th USENIX Conference on File and Storage Technologies (FAST), pages 59–72. USENIX Association, Dec 2005.
[2] C. Adams. The simple public-key GSS-API mechanism (SPKM). The Internet Engineering Task Force (IETF), RFC 2025, Oct 1996.
[3] A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer. FARSITE: Federated, available, and reliable storage for an incompletely trusted environment. In Proceedings of the 5th Symposium on Operating System Design and Implementation (OSDI). USENIX Association, Dec 2002.
[4] M.K. Aguilera, M. Ji, M. Lillibridge, J. MacCormick, E. Oertli, D.G. Andersen, M. Burrows, T. Mann, and C.A. Thekkath. Blocklevel security for network-attached disks. In Proceedings of the 2nd International Conference on File and Storage Technologies (FAST). USENIX Association, Mar 2003.
[5] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Communications of the ACM, 53(4):50–58. ACM Press, Apr 2010.
[6] Amazon simple storage service (Amazon S3). http://aws.amazon.com/s3/.
[7] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Advances in Cryptology – Proceedings of EUROCRYPT, pages 139–155. Springer LNCS 1807, May 2000.

AUTHORS

Mr. Megharaj Patil, I am pursuing M.E. in siddhant college of engineering, pune in 2016.

