SECURITY AND AUTHENTICATION FOR NETWORKED STORAGE

V. Kumar Murty
Department of Mathematics, University of Toronto, Toronto, ON, Canada

Guangwu Xu
Department of EE & CS, University of Wisconsin-Milwaukee, Milwaukee, WI, U.S.A.

Keywords: Storage area network, authentication, ID based cryptography.

Abstract: Authentication and access control are important measures for the security of a storage area network (SAN). In this paper, the current methods of authentication and access control in a SAN are reviewed and a new identity-based authentication scheme is proposed. This scheme has the advantage that it is lighter weight and more suited for the high speed switches that operate in a SAN fabric.

1 INTRODUCTION

Storage Area Networks (SANs) are an infrastructure for data storage solutions. SANs were originally designed for high reliability and security was not a major concern. It was felt that the security threat to a SAN was contained because the components were concentrated in one physical location that could be easily secured. With the advent of the internet, there is an increasing use of SANs with components spread in diverse locations. Thus, security is now becoming an issue.

Firewalls provide perimeter security but do not offer internal security. Also, WAN/LAN security does not help the SAN. In a storage environment, the insider threat is high. Indeed, it is estimated that in the data center, 70% of security threats are from insiders (source: Electric Crimes Task Force). There are risks from snooping, unauthorized access to and modification of data, and prevention of legitimate access. At present, the SAN infrastructure is sufficiently complicated that attacks may not be widespread. Security breaches will become more common as scripts become generally available and as intruders see a higher reward/(risk of being caught) ratio. This ratio increases dramatically with the connection of SANs to the internet. Restricting what can be accessed by a client in a SAN is a common method to provide security. This can be achieved using zoning and Logical Unit Number (LUN) Masking. In a FibreChannel (FC) storage network, zoning divides the members by port, name, or address and is implemented at the level of fabric switches. A further restriction of access is given by LUN Masking, which specifies logical storage units.

However, access control does not address all security concerns. Other security issues are also of considerable importance, one of them being authentication. Currently, there are two authentication schemes used in SANs, namely the Diffie- Hellman Challenge-Handshake Authentication Protocol (DH-CHAP) and the Fibre Channel Authentication Protocol (FCAP). The former is based on shared secret (passphrase) while the latter uses certificates from Public Key Infrastructure (PKI). Both methods carry an overhead that make them impractical in the context of the high-speed switches that operate in a storage fabric.

In 1984, Shamir (Shamir, 1984) proposed the concept of identity based cryptography. The idea is, instead of using certificates as in PKI, the users identifier (such as e-mail address, IP) is used as the public key. Therefore, the systems complexity can be reduced.

Some ID based signature methods have been proposed some time ago, see (Fiat and Shamir, 1987; Feige et al., 1988). More recently, two well defined ID based encryption schemes were suggested (Boneh and Franklin, 2001; Cocks, 2001). A mathematical object called pairing is used in the Boneh-Franklin ID based encryption system. Since then, the construc-

Kumar Murty V. and Xu G. (2008).
SECURITY AND AUTHENTICATION FOR NETWORKED STORAGE.
In *Proceedings of the International Conference on Security and Cryptography*, pages 477-480
DOI: 10.5220/0001927804770480

tions of ID based cryptography using pairings has become a very active field of research. (See for example, the monograph (Blake et al., 2004).)

In this article, we discuss the application of ID based methods for SAN security, especially for authentication. Some similar discussion for private area networks (PANs) can be found in (Garefalakis and Mitchell, 2002).

The organization of the paper is as follows. In section 2, current technologies on SAN authentication are reviewed. The ID based cryptography is introduced in section 3. We describe authentication based on the new crypto-methodology in section 4.

2 ACCESS CONTROL AND AUTHENTICATION

Components of network security include confidentiality, data integrity, non-repudiation, and authentication.

Currently, there are two approaches for SAN authentication. They are based on shared secret (passphrase) and certificates (public key infrastructure) respectively. It is noted that the former has been adopted as an ANSI standard. Existing access controls in SANs include zoning and LUN Masking. The former is an infrastructure level access control, while the latter is a SCSI access control. Detailed description of these schemes is given below.

2.1 DH-CHAP

DH-CHAP stands for Diffie-Hellman Challenge-Handshake Authentication Protocol and is the current standard of shared secret approach in SAN.

We first describe CHAP–the Challenge-Handshake Authentication Protocol. Suppose that we have two characters **A** and **B**. **A** wants to prove to **B** that it knows a shared secret K (the passphrase) without sending the secret in the clear. If this can be done, then **B** authenticates **A**.

The procedure works as follows:

Step 1. **A** requests inclusion in the network of trust from a trusted central authority **S**.

Step 2. **S** verifies **A** and with **A**'s help generates a password. The password is sent to **A** and stored securely in both **S** and **A**. All of this is done offline.

Step 3. **A** requests a service from **B** that requires authentication.

Step 4. **B** sends **A** a challenge C and session identifier id.

Step 5. **A** sends **B** a response R. The computation of R involves C, id and **A**'s passphrase K. To be more specific, $R = H(C\|K\|id)$, where H is a hash function (e.g., SHA-2).

Step 6. Since **A**'s passphrase is stored in **S**, a query (involves R, C, and id) is sent by **B** to **S** to verify the correctness of **A**'s response R.

Step 7. Once **S** confirms that R is the correct response, **B** authenticates **A**.

CHAP as it stands is vulnerable to an off-line dictionary attack. To remedy, it is augmented with a Diffie-Hellman key exchange. The resulting protocol is called DH-CHAP. In the Diffie-Hellman protocol, a cyclic group $G = < g >$ of order p is specified, where p is a large prime number. **A** generates a random number x and computes g^x, **B** generates a random number y and computes g^y. Each of them transmits its result to the other party:

$$\begin{tikzcd} \mathbf{A} \arrow[r, shift left, "g^x"] & \mathbf{B} \arrow[l, shift left, "g^y"] \end{tikzcd} .$$

Therefore, both of them can compute $g^{xy}\big(= (g^x)^y = (g^y)^x\big)$.

DH-CHAP integrates the the transmission of g^x and g^y into the original CHAP. In step 4, **B** sends C, id and g^y to **A**, while in step 5, **A** sends $R = H(id\|K\|H(C\|g^{xy}))$ and g^x to **B**. In step 6, **B** sends R, id and $H(C\|g^{xy})$ to **S** for confirmation.

It is noted that this process generates a shared key g^{xy} as a by-product of authentication. DH-CHAP is now the ANSI standard for authentication in the SAN environment. DH-CHAP is stronger but is still vulnerable to a combination of an on-line man-in-the-middle attack and an off-line dictionary attack.

2.2 FCAP

The second approach to authentication is to use certificates as in PKI. In this scenario, each entity has two keys (a public key and a private key). What is locked by the public key can be unlocked only by the private key and vice versa. More specifically, an encryption can be created by a public key, so the private key is used to decrypt; while a digital signature can be created using a private key, the public key is for signature verification. PKI is the basis of the Fiber Channel Authentication Protocol (FCAP).

In PKI, the certificate authority (CA) issues certificates to its clients. A certificate contains information about identification of the holder of the certificate, period of validity of the certificate, public key of the holder, and signature of the authority that issued the certificate. Other fields of a certificate are optional and can specify the services that a client is eligible for etc.

A more detailed description of FCAP follows.

Step 1. At set up, **A** presents its credentials off-line to the **CA** and requests a digital certificate.

Step 2. After the **CA** verifies the credentials of **A**, it issues a certificate.

Step 3. **A** sends a signed request for service from **B** and includes its certificate to prove its identity

Step 4. **B** obtains **A**'s certificate and verifies its validity (by consulting a Certificate Revocation List (CRL)).

Step 5. If the certificate is okay, **B** uses information from the certificate to interpret **A**'s request.

The advantages of FCAP is it does not require a shared secret to be established at the outset and securely stored (as in passphrase systems such as CHAP). The only secret that has to be centrally safeguarded is the private key(s) of the CA. However, in general, the implementation of PKI carries an overhead. It needs to maintain a huge database for certificates. To verify the validity of the certificate, B has to consult the CRL (Certificate Revocation List). In a storage environment, this could create unacceptable delays as the high speed storage switches will time out.

2.3 Zoning and Lun Masking

Zoning is a method by which one can control who can see what in a SAN. It permits communication only between defined sets by switching port or by World Wide Name (WWN) of components. It is implemented at the infrastructure level (switches) and is protocol independent. Within a zone, the member can have any-to-any connectivity. Hard zoning defines a zone by linking the ports of members. A zone established by linking the member's WWNs is referred to as soft zoning. It is also desirable to define zone sets as small as one can, and disable ports by default.

LUN Masking is a process that makes a LUN available only to a subset of initiators. It masks off the LUNs that are not assigned to the application server. This restricts access even further. LUN Masking is implemented primarily at end devices and applicable only to SCSI protocol. Thus, it is another layer of security above zoning (protocol specific). In the use of LUN masking, all access should be disabled by default. Only initiators that need the logical unit are enabled. Multi-pathing should be used. If authorization types is implemented, they should also be used.

3 ID BASED CRYPTOGRAPHY

The purpose of ID based cryptography is to reduce the overhead in the traditional PKI. In the ID based environment, the public key is a string which can be specified easily (eg. email address, IP, device identifier, etc.). It can also incorporate a period of validity. There is a trusted third party in such a system, which is also referred to as central authority (CA) or private key generator (PKG).

In the setup stage, the central authority generates a key pair, the public key pub_M and private key $priv_M$. They are called the master public key and private key of the CA.

The following is how the ID based encryption (IBE) works. If **A** is intended to send a cipher to **B**, it encrypts a plain text K using **B**'s identifier ID_B and pub_M, then transmits the cipher to **B**. To recover the plaintext, **B** obtains its private key $priv_{ID_B}$ (which key is computed by CA using $priv_M$ and ID_B) from CA (if it has not done so), then performs the decryption.

A well-known IBE system was proposed by Boneh and Franklin (Boneh and Franklin, 2001), which uses a mathematical structure called the Weil pairing. Digital signatures can be realized in the ID based system as well.

If **A** wants to create a signature in ID based setting, it first obtains the private key $priv_{ID_A}$ from CA (if it has not already done so). Then **A** signs the message K using $priv_{ID_A}$, and sends the signature to **B**.

B verifies **A**'s signature using ID_A and pub_M.

An example of ID based signature (IBS) scheme is found in (Cha and Cheon, 2003). In some sense, this IBS can be regarded as a dual to the IBE in (Boneh and Franklin, 2001).

Certificates are eliminated from ID based systems, it is efficient and easy to use. One of the disadvantages of such systems is that they provide key escrow since the central authority knows every user's private key. Some schemes were proposed to avoid key escrow, but they suffer other problems.

4 APPLICATIONS TO SAN

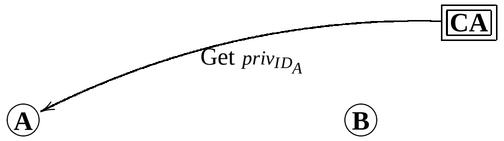
In this section, we propose the use of ID based cryptography in the authentication problem for SANs. It is parallel to FCAP under PKI, but has the advantage of being light weight.

Our system contains a central authority (CA) with a master public key pub_M and a master private key $priv_M$. For each user **A**, an identifier will be specified and denoted by ID_A. This is **A**'s identity which can be IP address, or device identifier, or WWN, or other properties of **A**. ID_A is regarded as the public key of **A**. The private key $privID_A$ of **A** is obtained as a combination of ID_A and the master private key $priv_M$.

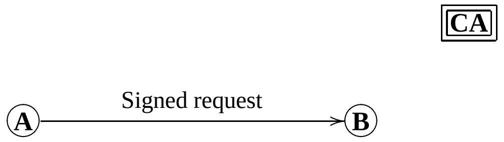
Sometimes it is useful to include other information such as key validity period or serial number of a transaction, in ID_A.

The following routines describe how a user **A** gets authenticated by a server **B**.

Step 1. **A** asks for its private key (if it has not already done so) from the **CA** via secure channel.



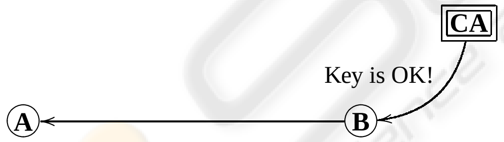
Step 2. **A** sends a signed request for service from **B**.



Step 3. **B** consults a key revocation list to verify that **A**'s private key has not been compromised, or the key has not expired.

CA
Is key valid?
A
B

Step 4. If the key is okay, **B** uses **A**'s public key (i.e., ID of **A**, not a certificate) to interpret **A**'s request.



In this setting, identifiers are acting as the public key. These id's can be world wide names, which are easily obtained. Sophisticated certificates are not needed. This means that the database for certificates and the needs for transmitting certificates are all eliminated. Although we still need central authorities, their duties are much lighter. The key escrow is an acceptable (maybe a very useful) feature here. It is still necessary to consult a key revocation list to ensure the validity of the key. The need for this can be minimized by embedding a period of validity within the public key. However, this does not address the issue of malicious users.

Finally, we would like to remark that a signature scheme, which is not ID based in nature, can be used in SAN authentication. This is a pairing based (in elliptic curve cryptography) scheme which was proposed by Boneh, Lynn, and Shacham (Boneh et al., 2004). The strength of the signature is that its length is half the size of a DSA signature for a similar level of security. The authentication can be made more efficient if this signature is incorporated into FCAP.

5 CONCLUSIONS

In this paper, the security, especially the authentication, of storage area network is discussed. The new technology of ID based cryptography is touched on and its applications to SAN authentication and access control are proposed.

REFERENCES

Blake, I., Seroussi, G., and Smart, N. (2004). *Advances in Elliptic Curve Cryptography*. Cambridge University Press, London.

Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *Advances in Cryptology, Crypt'01, LNCS, vol. 2139*, pages 213–239. Springer-Verlag Heidelberg.

Boneh, D., Shacham, H., and Lynn, B. (2004). Short signatures from the weil pairing. In *J. of Cryptology, vol. 17*, pages 297–319.

Cha, J. C. and Cheon, J. H. (2003). An identity-based signature from gap diffie-hellman groups. In *Public Key Cryptography, PKC'03, LNCS, vol. 2567*, pages 18–30. Springer-Verlag Heidelberg.

Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. In *Proc. the 8th IMA International Conference on Cryptography and Coding, LNCS, vol. 2260*, pages 360–363. Springer-Verlag Heidelberg.

Feige, U., Fiat, A., and Shamir, A. (1988). Zero knowledge proof of identity. In *J. of Cryptology, vol 1*, pages 77–94.

Fiat, A. and Shamir, A. (1987). How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology, Crypto'86, LNCS, vol. 263*, pages 186–194. Springer-Verlag Heidelberg.

Garefalakis, T. and Mitchell, C. (2002). Securing personal area networks. In *13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Lisboa, Portugal*, pages 1257–1259.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *Advances in Cryptology, Crypto'84, LNCS, vol. 196*, pages 47–53. Springer-Verlag Heidelberg.