World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 136-139, 2014
ISSN 1818-4952
© IDOSI Publications, 2014
DOI: 10.5829/idosi.wasj.2014.29.csea.2243

Trusted Tree Signature Authentication for Multicasting

K.P. Thooyamani, R. Udayakumar and V. Khanaa

School of Computing Science, Bharath University, Chennai-73, India

Absract: Conventional block-based multicast authentication schemes overlook the heterogeneity of receivers by letting the sender choose the block size, divide a multicast stream into blocks, associate each block with a signature and spread the effect of the signature across all the packets in the block through hash graphs or coding algorithms. The correlation among packets makes them vulnerable to packet loss, which is inherent in the Internet and wireless networks. Moreover, the lack of Denial of Service (DoS) resilience renders most of them vulnerable to packet injection in hostile environments. In this paper, we propose a novel multicast authentication protocol, namely MABS, including two schemes. The basic scheme (MABS-B) eliminates the correlation among packets and thus provides the perfect resilience to packet loss and it is also efficient in terms of latency, computation and communication overhead due to an efficient cryptographic primitive called batch signature, which supports the authentication of any number of packets simultaneously. We also present an enhanced scheme MABS-E, which combines the basic scheme with a packet filtering mechanism to alleviate the DoS impact while preserving the perfect resilience to packet loss.

Key words: Multicasting · Merkle tree

INTRODUCTION

Multicast is an efficient method to deliver multimedia content from a sender to a group of receivers and is gaining popular applications such as realtime stock quotes, interactive games, video conference, live video broadcast, or video on demand. Authentication is one of the critical topics in securing multicast [2-7] in an environment attractive to malicious attacks. Basically, multicast authentication may provide the following security services:

Data Integrity: Each receiver should be able to assure that received packets have not been modified during transmissions.

Data Origin Authentication: Each receiver should be able to assure that each received packet comes from the real sender as it claims.

Nonrepudiation: The sender of a packet should not be able to deny sending the packet to receivers in case there is a dispute between the sender and receivers [1]. All the three services can be supported by an asymmetric key technique called signature. In an ideal case, the sender generates a signature for each packet with its private key, which is called signing and each receiver checks the validity of the signature with the sender's public key, which is called verifying. If the verification succeeds, the receiver knows the packet is authentic [8, 9]. Designing a multicast authentication protocol is not an easy task. Generally, there are following issues in real world challenging the design. First, efficiency needs to be considered, especially for receivers. Compared with the multicast sender, which could be a powerful server, receivers can have different capabilities and resources. The receiver heterogeneity requires that the multicast authentication protocol be able to execute on not only powerful desktop computers but also resource-constrained mobile handsets. In particular, latency, computation and communication overhead are major issues to be considered. Second, packet loss is inevitable [10]. In the internet, congestion at routers is a major reason causing packet loss. An overloaded router drops buffered packets according to its preset control policy. Though TCP provides a certain retransmission capability,

Corresponding Author: R. Udayakumar, School of Computing Science, Bharath University, Chennai-73, India.

multicast content is mainly transmitted over UDP, which does not provide any loss recovery support. In mobile environments, the situation is even worse. The instability of wireless channel can cause packet loss very frequently. Moreover, the smaller data rate of wireless channel increases the congestion possibility [11]. This is not desirable for applications like real time online streaming or stock quotes delivering. End users of online streaming will start to complain if they experience constant service interruptions due to packet loss and missing critical stock quotes can cause severe capital loss of service subscribers. Therefore, for applications where the quality of services is critical to end users, a multicast authentication protocol should provide a certain level of resilience to packet loss.

Specifically, the impact of packet loss on the authenticity of the already-received packets should be as small as possible.

MATERIALS AND METHODS

Digital Signature Scheme: A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions and in other cases where it is important to detect forgery and tampering.

Definition: A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Mathematical Definition:

Key Generation for the Dsa: Each entity creates a public key and corresponding private key.

Each entity A should do the following:

- Select a prime number q such that $2^{159} < q < 2^{160}$.
- Choose t so that $0 = t = 8$ and select a prime number p where $2511+64t < p < 2^{512+64t}$, with the property that q divides (p - 1).
- (Select a generator α of the unique cyclic group of order q in $Z^*_{p.}$)
- Select an element $g \Sigma Z^*_p$ and compute $\alpha = g^{(p-1)/ q}$ mod p.
- If $\alpha = 1$ then go to step 3.1.

Select a Random Integer a Such That:

$1 = a = q - 1$.

- Compute $y = \alpha^a$ mod p.
- A's public key is (p, q, α, y);
  A's private key is a.

Dsa Signature Generation: Entity A signs a binary message m of arbitrary length. Any entity B can verify this signature by using A's public key.

Signature generation: Entity A should do the following:

- Select a random secret integer k, $0 < k < q$.
- Compute $r = (\alpha^k \bmod p) \bmod q$.
- Compute $k^{-1} \bmod q$.
- Compute $s = k^{-1} \{h(m) + ar\} \bmod q$.
- A's signature for m is the pair (r, s).

Dsa Signature Verification: To verify A's signature (r, s) on m, B should do the following:

- Obtain A's authentic public key (p, q, α, y).
- Verify that $0 < r < q$ and $0 < s < q$; if not, then reject the signature.
- Compute $w = s^{-1} \bmod q$ and h(m).
- Compute $u_1 = w.h(m) \bmod q$ and $u_2 = rw \bmod q$.
- Compute $v = (\alpha^{u1} y^{u2} \bmod p) \bmod q$.
- Accept the signature if and only if $v = r$.

Multicast: Multicast is communication between a single sender and multiple receivers on a network. Typical uses include the updating of mobile personnel from a home office and the periodic issuance of online newsletters.

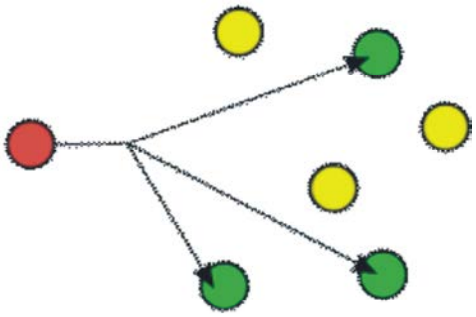

Fig 1:

Teleconferencing and video conferencing also use multicasting, but require more robust protocols and networks.

Diagram for Multicast: In computer networking, multicast is the delivery of a message to a group destination computers simultaneously in a single transmission from the source creating copies automatically in other network elements, such as routers, only when the topology of the network requires it.

Merkle Tree: Merkle tree is used to generate marks. The sender constructs a binary tree for eight packets. Each leaf is a hash of one packet. Each internal node is the hash value on the concatenation of its left and right children. For each packet, a mark is constructed as the set of the siblings of the node along the path from the packet to the root. For example, the mark of the packet p3 is $\{H_4, H_{1,2}, H_{5,8}\}$ and the root can be recovered as

$H_{1,8} = H((H_{1,2},(H(p_3),H_4)),H_{5,8})$.

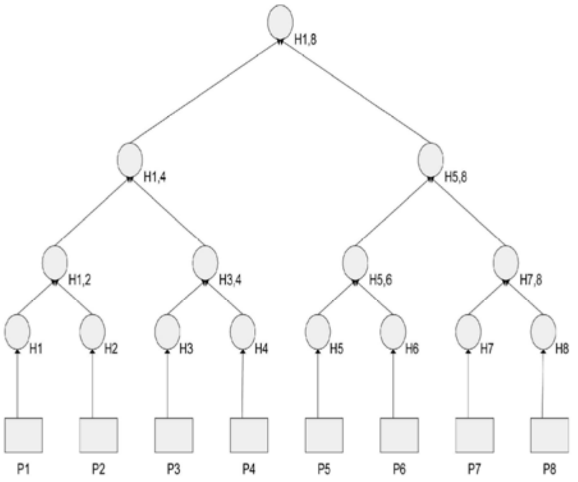

Fig 2:

Constructing a Merkle tree is very efficient because only hash operations are performed. Meanwhile, the one-way property of hash operation ensures that given the root of a Merkle tree it is infeasible to find a packet, which is not in the set associated with the Merkle tree and from which there is a path to the root. This guarantees that forged packets cannot fall into the set of authentic packets.

CONCLUSION

To reduce the signature verification overheads in the secure multimedia multicasting, block-based authentication schemes have been proposed. Unfortunately, most previous schemes have many problems such as vulnerability to packet loss and lack of resilience to denial of service (DoS) attack. To overcome these problems, we develop a novel authentication scheme MABS. We have demonstrated that MABS is perfectly resilient to packet loss due to the elimination of the correlation among packets and can effectively deal with DoS attack. Moreover, we also show that the use of batch signature can achieve the efficiency less than or comparable with the conventional schemes. Finally, we further develop two new batch signature schemes based on BLS and DSA, which are more efficient than the batch RSA signature scheme.

REFERENCES

1. Deering, S.E., 1988. "Multicast Routing in Internetworks and Extended LANs," Proc. ACM SIGCOMM Symp. Comm. Architectures and Protocols, pp: 55-64.
2. Ballardie, T. and J. Crowcroft, 1995. "Multicast-Specific Security Threatsand Counter-Measures," Proc. Second Ann. Network and Distributed System Security Symp. (NDSS '95), pp: 2-16.
3. Judge, P. and M. Ammar, 2003. "Security Issues and Solutions in Mulicast Content Distribution: A Survey," IEEE Network Magazine, 17(1): 30-36.
4. Challal, Y., H. Bettahar and A. Bouabdallah, 2004. "A Taxonomy of Multicast Data Origin Authentication: Issues and Solutions," IEEE Comm. Surveys & Tutorials, 6(3): 34-57.
5. Zhou, Y. and Y. Fang, 2006. "BABRA: Batch-Based Broadcast Authentication in Wireless Sensor Networks," Proc. IEEE GLOBECOM.
6. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013. Images segmentation via Gradient watershed

hierarchies and Fast region merging, Middle-East Journal of Scientific Research, ISSN: 1990-9233, 15(12): 1680-1683.

7. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Online answerback and reply-voice recording, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1861-1865.
8. Udayakumar, R., V. Khanna, T. Saravanan and G. Saritha, 2013. Cross Layer Optimization For Wireless Network (Wimax), Middle-East Journal of Scientific Research, ISSN: 1990-9233, 16(12): 1786-1789.
9. Saravanan, T., and R. Udayakumar and G. Saritha, 2013. Simulation Based line balancing of a single piece flow line, Middle-East Journal of Scientific Research, ISSN: 1990-9233, 16(12): 1790-1793.
10. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. An Integrated Agent System for E-mail Coordination using Jade, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(6): 4758-4761.
11. Udayakumar, R., A. Kumaravel and Rangarajan, 2013. Introducing an Efficient Programming Paradigm for Object-oriented Distributed Systems, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(5S): 4596-4603.