www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 9 September 2013 Page No. 2831-2841

PREVENTION OF TRESPASSER ACCESSING IN NETWORKS USING TICKET GRANTING SERVICE

[1]C.Jayalakshmi, [2]Mr. A. Senthil Kumar

Research Scholar Department of computer science Tamil University
Thanjavur-10
E-mail: cjaya16@yahoo.com

Asst. Prof in Computer Science Tamil University
Thanjavur-10.

Abstract:

This paper addresses the problem of protecting the system from non trusted users access the policy share. Web site administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonym zing network. As a result, administrators block all known exit nodes of anonym zing networks, denying anonymous access to misbehaving and behaving users alike. To address this problem, we present Nymble, a system in which servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. The interactive counterparts of group signatures are identity escrow schemes or group identification scheme with revocable anonymity. This work introduces a new provably secure group signature and a companion identity escrow scheme that are significantly more efficient than the state of the art. In its interactive, identity escrow form, our scheme is proven secure and coalition-resistant under the strong RSA and the decisional Diffie-Hellman assumptions.

Keywords: Nymble, anonymity, anonymous blacklist, privacy-enhanced revocation.

1.Introduction

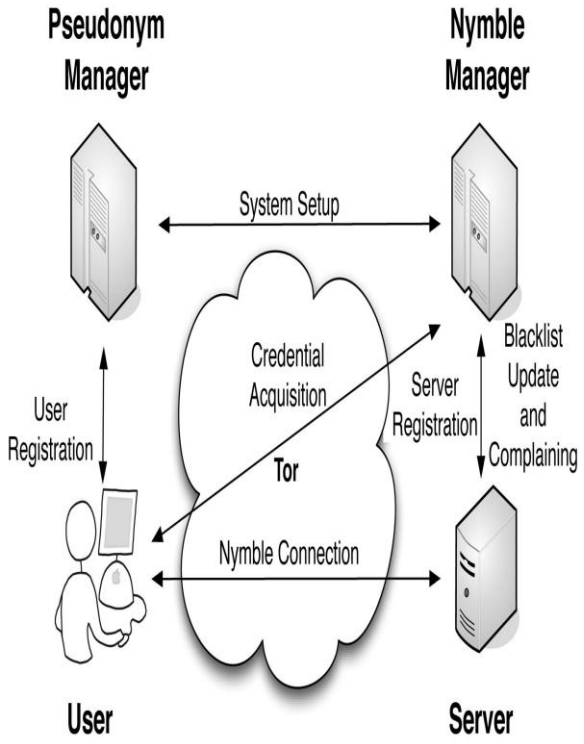
Traditional network security solution starts in access control from un-trusted network (e.g. Internet) to trusted internal networks. Many routers using ACL (Access Control List) to control access any host and service based specific IP address and port number. This solution does not needed high Performance because only looking for suspicious and defined IP address in packet header. So many early routers and low-end switches perform well. Nowadays we need control outbound traffic is important as well as inbounds and need to inspect payload data because protect to leakage of important data and follows many security compliance and policy. That means we need to control OSI Layer 7(application) data like login ID, user account, file extension as many considerable fact even existing IP address and port number. Moreover network, represent by Ethernet already changing gigabit very fast. Even some routers and switches have 10Gigabit processing capability. Evolving network environment accelerate because it is essential to provide new services such as Web 2.0, VoIP and T-commerce. Many of the existing network security solutions work in perimeter between internet and intranet. Just few years ago, many security solutions composed of OS and security application. It was no different general application and raising many problems like performance and scalability. To solve the problem most of the current network security solution adapt appliances which designed specific hardware and embedded software. However problem still remained. It does not according evolving network bandwidth and changing network paradigm aforementioned. This paper presents new system design having inline architecture that evolving system performance and responding flexibly changing security paradigm.

2.Background

Many older network security solutions work on general systems based multipurpose CPU (e.g. PENTIUM, SPARC) and OS (e.g. UNIX, LINUX). It means whole system performance depends on what kind of CPU and OS used in solution. Multipurpose general CPU is not suitable packet processing, and some feature in OS is unnecessary. Most of current solution adopt rack type appliance which reinforce performance and reliability because it works well bad condition than PC and Server. As changing network

environment and security challenge, lots of research has been progressed to improve performance. Krueger and Valeur have proposed slicing mechanism that divides the overall network traffic into subset of manageable size to detecting intrusion accurately. Many network vendor like Nortel, proposed integrated system like 'switched firewall' which mixed legacy firewall and switch to get high performance. Many improved security relative algorithm such as encryption, decryption have proposed. These methods have been helpful improved performance but still remain some problem. Krueger's intrusion detection very powerful but difficult to adopt real network and switched firewall has limit to add new feature.

Diagram:



2.1 The packet processing tasks

1.Forward: Input packet forward to main memory or Degrees after complete process.

2.Parse: Analyzes and classifies the contents of the packet header and fields.

3.Search: Tables are searched for a match between the content that was classified and pre-defined contents and rules.

4.Resolve: The destination and QoS (Quality of Service) requirements are resolved and the packet is routed to its destination.

5.Modify: Where necessary, the packet is modified (e.g. certain fields within the packet are changed) All tasks do not apply all ingress packets.

Some packets are applied only parse to access control based IP address but another packets are applied all tasks to inspect antivirus in payload. It depends on security and network policy.

Each processing tasks are related in security application and Solution.

Many network security solutions perform security application and are divided on the basis of how many and how sophisticated doing security applications. Of course, even one solution performs all security application. In case of security appliances, all security application process single or dual general CPU and whole system performance depends on performance of CPU that cannot expect high performance. Many VPN solutions need to high computing power to processing packet encryption and decryption. Moreover if it need to high bit-strength or increasing packet flooding, can need more computing power that occurs CPU bottleneck. As a result the whole system performance is very lower. OS Only performed only packet forwarding ingress to egress without any task. Access Control (AC) performed parse task which compared IP address in ingress packet field and predefined IP address in security policy. AES (Advanced Encryption Standard) performed all ingress packets are encrypted by AES. Not much difference performance between OS Only and AC which means parse task do not need high computing power.

A secure group signature scheme must satisfy the following properties:

Correctness: Signatures produced by a group member using SIGN must be accepted by VERIFY.
Unforgeability: Only group members are able to sign messages on behalf of the group.
Anonymity: Given a valid signature of some message, identifying the actual signer is computationally hard for everyone but the group manager.
Unlink ability: Deciding whether two different valid signatures were computed by the same group member is computationally hard.
Exculpability: Neither a group member nor the group manager can sign on behalf of other group members. A closely related property is that of no framing; it captures the notion of a group member not being made responsible for a signature she did not produce.
Traceability: The group manager is always able to open a valid signature and identify the actual signer.
Coalition-resistance: A colluding subset of group members (even if comprised of the entire group) cannot generate a valid signature that the group manager cannot link to one of the colluding group members.

3.Contributions Of This Paper

Our research makes the following contributions:
1. Blacklisting anonymous users. We provide a means by which servers can blacklist users of an anonymzing network while maintaining their privacy.
2. Practical performance. Our protocol makes use of inexpensive symmetric cryptographic operations to significantly outperform the alternatives.
3. Open-source implementation. With the goal of contributing a workable system, we have built an open-source implementation of Nymble, which is publicly available.

4.Time

Nymble tickets are bound to specific time periods. Time is divided into link ability windows of duration W, each of which is split into L time periods of duration T. We will refer to time periods and likability windows chronologically as t1; t2; . . . ; tL and w1; w2; . . . , respectively. While a user's access within a time period is tied to a single nymble ticket, the use of different nymble tickets across time periods grants the user anonymity between time periods. Smaller time periods provide users with higher rates of anonymous authentication, while longer time periods allow servers to rate-limit the number of misbehaviors from a particular user before he or she is blocked. For example, T could be set to five minutes, and W to one day. The link ability window allows for dynamism since resources such as IP addresses can get reassigned and it is undesirable to blacklist such resources indefinitely, and it ensures forgiveness of misbehavior after a certain period of time.

5. Nymble Connection Establishment

To establish a connection to a server sid, the user initiates a type-Anon channel to the server, followed by the Nymble connection establishment protocol described below.

5.1 Blacklist Validation

1. The server sends hblist; certi to the user, where blist is its blacklist for the current time period and cert is the certificate on blist. (We will describe how the server can update its blacklist soon.)
2. The user reads the current time period and link ability window as tðUÞ now and wðUÞ now and assumes these values to be current for the rest of the protocol.
3. For freshness and integrity, the user checks if
VerifyBLusrState_sid; now; now; blist; cert_ ¼ true:
If not, terminates the protocol with failure.

5.2 Privacy Check

Since multiple connection establishment attempts by a user to the same server within the same time period can be linkable, the user keeps track of whether she has already disclosed a ticket to the server in the current time period by maintaining a Boolean variable ticket Disclosed for the server in her state.
Furthermore, since a user who has been blacklisted by a server can have her connection establishment attempts linked to her past establishment, the user must make sure that she has not been blacklisted thus far. Consequently, if ticket Disclosed in usrEntries½sid_ in the user's usrState is true, or
UserCheckIfBlacklistedusrStatesid; blist ¼ true; then it is unsafe for the user to proceed and the user sets safe to false and terminates the protocol with failure.10

5.3 Ticket Examination

1. The user sets ticketDisclosed in usrEntries½sid_ in usrState to true. She then sends ticket to the server, where ticket is ticket now_ in cred in usrEntries½sid_ in usrState.
Note that the user discloses ticket for time period now after verifying blist's freshness. This procedure avoids the situation in which the user verifies the current blacklist just before a time period ends, and then presents a newer ticket for the next time period.
2.On receiving ticket, the server reads the current time period and link ability window.
The server then checks that:

- Ticket is fresh.
- Ticket is valid, the algorithm ServerVerifyTicket returns true.
- Ticket is not linked (in other words, the user has not been blacklisted), i.e., ServerLinkTicketsvrStateticket ¼ false:

3. If any of the checks above fails, the server sends goodbye to the user and terminates with failure.
Otherwise, it adds ticket to slist in its state, sends okay to the user, and terminates with success.
4. On receiving okay, the user terminates with success.

6.Algorithm

ServerLinkTicket
Input: ticket 2 T
Persistent state: svrState 2 SS
Output: b 2 ftrue; falseg
1: Extract lnkng-tokens from svrState
2: nymble; ticket
3: for all i 1 to jlnkng-tokensj do
4: if ; nimble lnkng-tokens i_ then
5: return true
6: return false

7.Security Properties

Correctness: By inspection.
Unforgeability: Only group members are able to sign messages on behalf of the group: This is an immediate consequence of Theorem 2 and the random oracle model, that is, if we assume the hash function H behaves as a random function.
Anonymity: Given a valid signature (c, s1, s2, s3, s4, T1, T2, T3) identifying the actual signer is computationally hard for everyone but the group manager: Because of Theorem 2 the underlying interactive protocol is statistically zero knowledge, no information is statistically revealed by (c, s1, s2, s3, s4) in the random oracle model. Deciding whether some group member with certificate [Ai, ei] originated requires deciding whether the three discrete logarithms logy T1/Ai, logg T2, and logg T3/gei are equal. This is assumed to be infeasible under the decisional Diffie-Hellman assumption and hence anonymity is guaranteed.
Unlink ability: Deciding if two signatures (T1, T2, T3, c, s1, s2, s3, and s4) and (˜ T1, ˜ T2, ˜ T3, ˜c, ˜s1, ˜s2, ˜s3, ˜s4) were computed by the same group member is computationally hard. Similarly as for Anonymity, the problem of linking two signatures reduces to decide whether the three discrete logarithms logy T1/ ˜ Ti, logg T2/ ˜ T2, and logg T3/ ˜ T3 are equal. This is, however, impossible under Decisional Diffie- Hellman Assumption.
Exculpability: Neither a group member nor the group manager can sign on behalf of other group members: First note that due to Corollary 2, GM does not get any information about a user's secret xi apart from axi . Thus, the value xi is computationally hidden from GM. Next note that T1, T2, and T3 are unconditionally binding

commitments to Ai and ei. One can show that, if the factorization of n would be publicly known, the interactive proof underlying the group signature scheme is a proof of knowledge of the discrete log of Aei i /a0 (provided that `p is larger than twice to output length of the hash function / size of the challenges). Hence, not even the group manager can sign on behalf of Pi because computing discrete logarithms is assumed to be infeasible.

Traceability: The group manager is able to open any valid group signature and provably identify the actual signer: Assuming that the signature is valid, this implies that T1 and T2 are of the required form and so Ai can be uniquely recovered. Due to Theorem 1 a group certificate [Ai = A (xi), ei] with xi 2 _ and ei 2 can only be obtained from via the JOIN protocol.

Coalition-resistance: Assuming the random oracle model.

8. Conclusion

A very efficient and provably secure group signature scheme and a companion identity escrow scheme that are based on the strong RSA assumption. Their performance and security appear to significantly surpass those of prior art. Extending the scheme to a blind group-signature scheme or to split the group manager into a membership manager and a revocation manager is straight-forward. Servers can blacklist misbehaving users while maintaining their privacy, and we show how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services.

9.References

[1] J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.

[2] D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), pp. 199-203, 1982.

[3] D. Chaum, "Showing Credentials without Identification Transfeering Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246-264, 1990.

[4] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[5] C. Cornelius, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks," Technical Report TR2008-637, Dartmouth College, Computer Science, Dec. 2008.

[6] I. Damga°rd, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 328-335, 1988.

[7]N. Bari´c and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In Advances in Cryptology — EUROCRYPT'97, vol. 1233 of LNCS, pp. 480–494, Springer-Verlag, 1997.

[8] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In 1st ACM Conference on Computer and Communication Security, pp. 62–73, ACM Press, 1993.

[9] D. Boneh. The decision Diffie-Hellman problem. In Algorithmic Number Theory (ANTS-III), vol. 1423 of LNCS, pp. 48–63, Springer-Verlag, 1998.

[10] S. Brands. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, Centrum voor Wiskunde en Informatica, April 1993.