Build a trust and Reliable Authentication Module in Ad Hoc Network

Sahar Adil
Babylon University-Science collage for woman Computer Science Dept.
E-mail: salaa_38@yahoo.com

Abstract

Ad hoc network is a collection of wireless nodes dynamically forming a temporary network without any infrastructure and centralized control, its operations are usually performed in a fully distributed manner. This means every node is carrying out an equal role and sharing its job evenly. From this point providing security support for large adhoc wireless networks is a big challenge due to their unique characteristics, such as mobility, dynamic node joins and leaves using wireless connection. According to the connection nature of nodes in ad hoc,a trust relationship must exist to transmit their packetsbetween them. Security demands that all nodes must be authenticated before transmitting process start.In this research we propose an authentication module to assist in building a trust relationships between ad hoc nodes by using Kerberos protocolIncluding Kerberos in ad hoc net prevents of identity forgery, mutual authentication between nodes, and secure distribution of messages between nodes in a particular net, and between different nets belong to other realms.
Keywords: ad hoc network, Kerberos, realm, authentication.

الخلاصة

شبكة الآد هوك هي مجموعة من العقد اللاسلكية المتحركة ديناميكيا تشكل شبكة بدون الحاجة الى وجود قاعدة او سيطرة مركزية, وتنجز عملياتها بصورة موزعة, وهذا يعني ان كل عقدة في الشبكة لها دور مشابه للاخرى. من هذه النقطة توفر الامنية ودعمها لهذه الشبكة هو التحدي الاكبر تبعا لمواصفاتها الخاصة, مثل التنقل, انضمام العقدة الى الشبكة او تركها. ولطبيعة ترابط العقد في هذه الشبكة فلابد من وجود علاقة موثوقة لنقل المعلومات بينهم. وهذا يعني ان كل عقدة في الشبكة يجب ان توثق قبل بدء عملية النقل. في هذا البحث تم بناءموديل توثيقي للمساعدة في بناء علاقات موثقة وامنة بين عقد شبكة الآد هوك باستخدام بروتوكول الكربروس. وجود هذا البروتوكول في الشبكة يمنع من تزوير الشخصية, امكانية تبادل الثقة بين العقد, توزيع آمن للرسائل بين العقد في الشبكة الواحدة وبين الشبكات الاخرى
الكلمات المفتاحية: شبكة الاد هوك، كيربروس, منطقة, توثيق

1- Introduction

Mobile ad hoc networks are special type of wireless networks in which a collection of mobile hosts with wireless network infrastructure may form a temporary network, without the aid of any fixedinfrastructure or centralized administration. In mobile ad hoc networks, nodes within their wireless transmitter ranges can communicate with each other directly (assume that all nodes have the same transmission range), while nodes outside the range have to rely on some other nodes to relay messages. Thus a multi-hop scenario occurs, where the packets sent by the source host are relayed by several intermediate hosts before reaching the destination host. Every node functions as a router. The success of communication highly depends on the other nodes cooperation.

While mobile ad hoc networks can be quickly and inexpensive setup as needed, security is a critical issue compared to wired or other wireless counterparts.In recent years, ad hoc security has received critical attention in both academic and industry. This emerging technology seeks to provide users "any time, anything" networking services in potential large-scale ad hoc wireless network. Users are expected to execute secure data communications among one another and with the rest of the network at any time, at any place, this made security design increasingly important and big challenge [Kong, Zefros; Luo, Lu; Kong, Gudenial; William; Guttman].

Confidential, integrity, non-repudiation, authentication,, and availability are considered as the main service of a security system. Among these services authentication has been identified as a bottleneck. The compromise of the authentication service breaks down the whole security system and cannot proceed to provide the other services without the valid identities of communicating nodes being successfully established. In our scheme we use Kerberos authentication techniques to authenticate the identity of ad hoc nodes within the same net or with other nets in different realms. It is a computer authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner [Luo, Lu; Wikipedia; Miller].

2-Related Work.

- Kaman based on time-tested and widely deployed Kerberos protocol, it use only the first phase of authentication cycle to exchange the session key between nodes to ensure that the only nodes know the secret key or password and the servers know a cryptographic hash of these passwords [Pirzada; Macdonald].

- Charon provides indirect authentication and secure communication between a lightweight PDA client and a Kerberos Server using an intermediary system called the proxy. Charon uses the Proxy to communicate with the Kerberos Key Distribution Center and the Kerberos Ticket Granting Server to save the computation resources of the client. It operates using two distinct phases. In the first phase known as the Handshake, the client authenticates itself to the proxy and establishes a secure channel with it. In the second phase called the Service Access, the proxy accesses the Kerberos servers on the client's behalf for authentication services. The scheme, although very effective for low resource clients, cannot be used for adhoc networks where simultaneous access to three servers (Proxy Server, Authentication Server and Ticket Granting Server) may not be possible in every scenario. This scheme is also subject to latency delays in the authentication mechanism [Fox, Gribble; Miller].

- M.PKINIT is an amalgamation of the Public Key based Kerberos PKINIT (Tung, Neuman and Wray 2001) and Charon for use in mobile networks. It adds Public Key cryptography to the Kerberos protocol to simplify the key management (from the Kerberos perspective) and the ability to use the existing public key certification infrastructures. It aims to enhance the security of the Kerberos protocol by using a minimal number of public key operations along with a proxy for load distribution. This scheme incorporates asymmetric cryptography which in turn slows the overall authentication mechanism. It also requires simultaneous access to three servers for initial authentication, which we have already deemed limiting in such an improvised environment [A, D.A; Zhu, Tung].

- In the Pretty Good Privacy Model all users act like independent certification authorities and have the capability to sign and verify keys of other users. PGP breaks the traditional central trust authority architecture and adopts a decentralized "web of trust" approach. Each individual signs each other's keys that help build a set of virtual interconnecting links of trust. PGP attaches various degrees of confidence levels from "undefined" to "complete trust" to the trustworthiness of public-key certificates and four levels of trustworthiness of introducers from "don't know" to "full trust". Based on these trust levels the user computes the trust level of the desired party. PGP is suitable for wired networks where a central key server can maintain a database of keys. However, in ad-hoc networks, the inclusion of a central key server creates a single point of failure and also requires uninterrupted access to the nodes. The other option, as in PGP, is for each node to store a subset of the public keys of other users using a subset of the trust graph and to merge these graphs with graphs of other users

in order to discover trusted routes. This scheme involves extensive computation and memory requirements and is considered restrictive for ad-hoc networks [Garfinkel].

3- The proposed work

Our proposed schemadopted in ad hoc networks to build a trust and reliable communication between ad hoc net nodes, by adapting Kerberos authentication protocol.

The procedure of authentication as follow in:-

Phase1:

Req1: C ⟶ AS: [Options|| ID_c|| $Realm_c$|| ID_{tgs}|| Times || Nonce1 || TS]

Step1: AS verifies the request of the node

If the request is valid then step2.

Else

The request is ignored.

Step2: A ⟶ Sker: [$Realm_c$|| ID_c|| Tic_{tgs}|| EK_c[KU_{tgs}||Times || Nonce1 || $Realm_{tgs}$|| ID_{tgs}]]

Step3: ker ⟶ C: request the P.W.

If the P.W is same as the stored one then Req2.

Else

The access is denaied.

Req2: ke r⟶ C: [$Realm_c$|| ID_c|| Tic_{tgs}|| EK_c[KU_{tgs}|| KU_c|| Times || Nonce1 || $Realm_{tgs}$|| ID_{tgs}|| TS]].

$Tic_{tgs:}EK_{tgs}$[flags|| KU_{tgs}|| KU_c|| $Realm_c$|| ID_c|| AD_c|| Times]

Phase2:

Req3: C ⟶ TGS: [Options|| ID_v|| Times || Nonce2 || Tic_{tgs}|| Ath_c]

Ath_c: $E_{KR(c)}$[ID_c|| $Realm_c$|| TS]

Step1: TGS verifies the received request by decrypt Tic_{tgs} to get the public key of the node (KU_c) in order to decrypt the authenticator (Ath_c) and compare between the Tic_{tgs} and Ath_c.

If they same then Req4 can done.

Else

The access is denaied.

Req4: TGS⟶ C:[$Realm_c$|| ID_c|| Tic_v || EK_{tgs}[KU_v|| Times || Nonce3|| $Realm_v$|| ID_v]]

$Tic_{v:}EK_v$[flags|| KU_v|| $Realm_c$|| ID_c|| AD_c|| Ts ||Times]

Phase3:

Req5: C ⟶TGS: [Options|| Tic_v|| Ath_c]

Ath_c: $E_{KR(c)}$[ID_c|| $Realm_c$|| TS|| Subkey|| Seq#]

Req6: TGS ⟶ C: $E_{KR(tgs)}$[TS|| Subkey|| Seq#]

4- Analysis of Proposed System

In ad hoc infrastructureassumes that all data exchanges occur in an environment where packets can be inserted, changed, or intercepted at will. This section describethe proposed algorithm and the role of Kerberos in providing reliable and strong security basis in an open environment such as ad hoc nets as one layer of an overall security plan. In below analysis of each phase and the security basis can gain.

From the view of phase1: The client and server must be able to establish an encryption connection .The authentication server will handle all the functions required for authentication. When a client initialize the node request the Authentication Server replies with an error packet indicating the need to pre-authenticate to reinforce security. The client, in light of the error, asks the user to enter the password and resubmit the request with adding a time stamp,if there is one. the AS, since it knows the secret key of the user, attempts to decrypt the timestamp present in the request and if it is successful and the timestamp is in line, i.e. included within the established tolerance, it decides that the requesting user is authentic and the authentication process continues normally.

When AS, receives the request by the client and verifies that the client is indeed the computer it claims to be the verification service done by created a **timestamp** ,by puts the current time in a user session, along with an expiration date. When encryption key created, The timestamp ensures that when time is up, the encryption key is useless. (This is used to make sure a hacker doesn't intercept the data, and try to crack the key.Since Kerberos uses timestamps to handle all activities, the clocks on all host machines must be within the Kerberos server's clock and up to date.The password has been used in the proposed work of type salt.
In general, phase 1 check the user information if his identity is illegal or not and authorize him to phase2 .

From the view of phase2:The user is authorized to deal with TGS in order to get TGT as a credential card to get his request in connection with the net nodes. It creates the service ticket, putting inside the requesting user's principal, the service principal, the date and time in timestamp format, the lifetime (as the minimum between the lifetime of the TGT and that associated with the service principal) and lastly authenticator (***Ath)*** encrypted by the user private key.When the previous request arrives, the application server decrypt the ***Ath*** to verifies the following conditions:

- the ticket has not expired;
- The Client present in the authenticator matches the one present in the ticket;
- The authenticator is not present in the replay cache and has not expired;

The previously checked conditions prove that the TGT really belongs to the user who made the request and therefore the TGS starts to process the reply as in Req4.

From the view of phase3:
Req5 and Req6 represent the node communication with the other nodes is now reliable and trust authentic, also Req6 is considered as a mutual authentication process between the communicated process.

- Subkey represent the agreed exchange secret key between the node and SGT.
- Seq# indicate the no. of requests that will be exchanged between the participant parties without any gab in numbering of requests

The authentication process itself can viewed as:

- Cross-authentication, is based on the assumption that there is a trust relationship between the realms involved. Where The user belong to a certain realm is authenticate and access the services of another realm.
- Direct -authentication, It occurs when the KDC of realm B has direct trust in the KDC of realm A, thus allowing the users of the latter realm to access its resources.
- Transitive-authentication, when the number of realms in which cross-authentication must be possible increases, the number of keys to exchange increases quadratically. To solve this problem, transitivity has been created : if realm A trusts

realm B and realm B trusts realm C then A will automatically trust C. This relationship property drastically reduces the number of keys (even if the number of authentication passages increases).

Another benefits Kerberos can provide:

- The user's password must never travel over the network;
- The user's password must never be stored in any form on the client machine: it must be immediately discarded after being used;
- The user's password should never be stored in an unencrypted form even in the authentication server database;
- The user is asked to enter a password only once per work session. Therefore users can transparently access all the services they are authorized for without having to re-enter the password during this session.
- The key is sent back to the client in the form of a **ticket-granting ticket**(TGT). This is a simple ticket that is issued by the authentication service. It is used for authenticating the client for future reference by forwarded the ticketfrom one host to another, thus once authenticated it is possible to access the login on all the desired machines without having to re-enter any password.
- A ticket can be renewable , i.e. it is reassigned the entire lifetime. Obviously, the AS will honor the renewal request only if the ticket has not expired yet and has not exceeded the maximum renewal time,the able to renew a ticket combines the necessity of having short duration tickets for security reasons.
- Replay Cache has been used with application server and TGS, in order to remember authenticators which have arrived within the last minutes, and to reject them if they are replicas. This technique resolve the problem of copying the ticket and authenticator as long as the impostor is not smart enough and make them arrive at the application server before the legitimate request arrives.

5- Conclusion

In this research, Kerberos protocol scheme adopted to provide reliable authentication service as one of security basics required in an open environment and insecure networks where communication between the hosts belonging to it may be intercepted. Its provide a means of verifying the identities of principals without relying on authentication provided by the host operating system, without basing trust on host addresses, and without requiring physical security of all the hosts on the network and under the assumption that the packets tracing along the network can be read, modified, and inserted as will.Our scheme is applicable to ad hoc net works in an open-managed environment where there is an option for bootstrapping the Kerberos servers and clients. The scheme is modular, secure, and reliable due to its distributed architecture

6- Refrences

- A.Harbitter, D. A. Menasce, 2001; "the performance of public key enabled Kerberos authentication in mobile computing applications", proc of the 8th ACM conference on computers and communications security, P: 78-85.
- Fox A., Gribble S.D., 1996; "Security on the move: indirect authentication using Kerberos", Procofbthe second annual international conference on mobile computing and networking, P: 155-164.
- Garfinkel, S., 1995;"*PGP:Pretty Good Privacy*, O'Reilly& Associates".
- Guttman Joshua D.; "Security Protocol Design via Authentication Tests", MITRE Corporation, 2002.

- Kong Jiejum, GuDenialLihul, and Geria Mario, 2002; "Adaptive security for multilevel of ad hoc network", available at:www.cs.ucla.edu/pdf docs/wcmco2.pdf .
- Kong Jiejum, ZerfosPetros, …etal; "Providing robust and ubiquitous security support for mobile ad hoc networks", available at:Citeseerx.Ist.Psu.edu/view doc/download? doi=10.1.1.156.3699.pdf.
- LuoHaiyun, Lu Songwn, 2000; " ubiquitous and robust authentication service for ad hoc wireless networks", available at:Citeseerx.Ist.Psu.edu/view doc/download? doi=10.1.1.29.327.pdf.
- Miller.S.P, B.C Neuman, et al,1988; " Kerberos Authentication and Authorization System", available at: http://citeseer.ist.psu.edu/cache/papers/cs/miller88kerberos.pdf.
- PirzadaAsad Amir, Macdonald Chris, 2004; "Kerberos assisted authentication in mobile ad hoc networks", available at:Citeseerx.Ist.Psu.edu/view doc/download? doi=10.1.1.4.735.pdf.
- Wikipedia, Free enclopedia, 2010**;** **”**Kerberos protocol”, available at: en.wikipedia.org/wiki/kerberos protocol
- William Stalling, 1999; " Cryptography and Network Security Principles and Practice", Second Edition, Prentice Hall Inc.
- Zhu, L., and Tung, B.; 2006; " Public keycryptography for initialauthentication in Kerberos", available at: www.ietf.org/rfc/rfc 4556.txt