NTM - Progressive Trust Negotiation in Ad Hoc Networks

Raja Rai Singh Verma, Donal O'Mahony and Hitesh Tewari
{Raja.Verma,Donal.Omahony,Hitesh.Tewari@cs.tcd.ie}
Network and Telecommunications Research Group (NTRG)
Department of Computer Science
Trinity College
Dublin –2, Ireland

Abstract

The dynamic nature of Ad hoc Networks makes it difficult to build trust relationships. This is primarily due to non-availability of online trusted third parties during trust negotiation. Trust Negotiations should also be secure and straightforward. This paper presents an overview of a scheme for progressive trust negotiation to build trust, along with a dynamic key agreement scheme to protect the negotiation. The scheme is sub- divided into two main components namely the peer-to-peer component and the remote component. The peer-to-peer component is lightweight, dealing with securing communications with the neighbours. The remote component is more heavyweight having the dual responsibility of carrying out trust negotiation and establishing secure end-to end communications.

1.Introduction

Ad Hoc Networks have little or no fixed infrastructure making their deployment fast and easy. This frequent membership change coupled with wireless as preferred media for communication makes the topology of an Ad Hoc network dynamic. Let us consider the case of a conference scenario. This scenario calls for a flexible network to be built for a large number of delegates attending a conference. An Ad Hoc Network can be formed with the delegates using their wireless enabled notebook computer to communicate with others. Shared services like printing also can be made be available using wireless access points. The network thus formed is set-up quickly and uses very little fixed infrastructure.

The simple formation and quick deployment of an Ad Hoc Network leads to a host of problems for trust negotiation. Wireless is a core component of Ad Hoc Networks resulting in possibility of *eavesdropping* of transmissions. This makes the encryption of trust negotiation process imperative.

Trust negotiations differ from lax to strict depending on the circumstances. In a military scenario the trust negotiation can be quite strict which contrasts the lax scenario of a group formed to play a game.

The mobility and the dynamic nature of the Ad Hoc Networks make the building of trust difficult. Trust management in traditional networks relies on a centralized entity to govern the trust. In an Ad Hoc Network, having a central entity for maintaining trust information defeats the purpose of having an Ad Hoc Network altogether. The trust negotiation scheme for Ad Hoc Networks must be distributed with little or no reliance on central entity. At the same time is should be simple and be easy to deploy.

Our objective is to develop simple and fast trust negotiation scheme. It should be capable of defending against external and internal intrusions while negotiating trust.

The scheme should be flexible enough for users to migrate between devices still carrying out trust negotiation and maintain the trust independent of the device. This scheme should work well in Ad Hoc situations and have enough flexibility to work on conventional networks. The last objective arises from our belief that in future the line dividing the Ad Hoc and conventional networks will blur.

Section 2 will deal with state of art systems and their shortcomings. Section 3 will give an overview of our model followed with a section on conclusion and the future work.

2.Background and State of Art Systems

Our scheme envisions incremental exchange of information using digital certificates to build trust. There are many systems available for certificate-based authentication and authorization and we discuss some of them briefly. The "IETF Simple Public Key Infrastructure"(SPKI) [1] embeds the authorization to use an application directly into the certificate. This means that the certificates are only to be used for a single purpose. The "KeyNote" system of Blaze et al [2] also uses a similar type of management of capability. The Secure Socket Layer (SSL) [3] or its successor Transport Layer Security (TLS) [4] is the most widely used certificate exchange mechanism on the Web. It provides for certificate exchange during client and server authentication. The server discloses its certificate without waiting for the client's certificate.

The work done by Trust Establishment Project at IBM Hafia Research Laboratory can be applied to Ad Hoc Networks. They put forward an Automated Trust Negotiation [5] scheme using property based digital certificates. The architecture of the Automated Trust Negotiation is targeted at client server applications. In this model the server has a service-governing policy, which the clients when requesting services will have to meet. The certificate disclosure is linked to certificate access policies for the certificates in both the servers and the clients. There is a security agent on the client and server that exchanges certificates according to their respective negotiation strategy. This model also provides for dealing with the sensitivity of certificate and the disclosure of sensitive certificates.

One of the schemes designed specifically for Ad Hoc Networks is by Zhou et al [6], which proposed a key management service using threshold cryptography and public key/secret key paradigm. The scheme provides for distribution of the secret key for the service among some special Ad Hoc nodes designated as servers. To compromise the secret key of the service, one has to compromise a certain threshold number of servers. This means that the service can recover if the number of servers compromised is less than the threshold number for the service. This scheme involves the designation of a few nodes as servers for the scheme and has facilities to switch to a new threshold when required. Hubaux et al [7] proposed a new public-key distribution for Ad Hoc Networks, which has similarity with PGP "web of trust" concept [8]. Each user has a certificate repository and selects a subset of it to disclose to the other user. Both the users then merge the certificate repositories to build certificate chains. This scheme is differs from PGP as there are no certificate directories for distribution of certificates but instead each user stores and distributes the certificates from their own certificate stores.

The current systems mentioned briefly above are not well adapted to Ad Hoc Networks. KeyNote and the IETF SPKI are too restrictive as they bind application-accessing capability to the certificates restricting their use. SSL and TLS have no

mechanism for gradual trust building. The client cannot request for more of server's certificates other than those already released. The application of IBM Haifa Research Lab approach of gradual trust negotiation in the case of Ad Hoc Networks presents several difficulties. Ad Hoc Networks operate peer-to-peer while the approach by Winsborough et al is client server oriented. The trust negotiation in the peer-to-peer architecture is very different from that of the client-server architecture as the same node may be in different roles during negotiations (i.e. the same node can be a client in one negotiation and a server in another).

The Key Management Service proposed by Zhou et al is a good distributed service but there needs to be a lot of prior communications between the Ad Hoc nodes to form trust. PGP leads to introduction of self-signed certificates that has little trust value unless there is complete explicit trust in a certificate. The scheme proposed by Hubaux et al leads to disclosure of too much information, which may be a security risk. These shortcomings in the present scheme lead us to design a new scheme for Ad Hoc Networks.

3.The NTRG Trust Model (NTM)

The NTM is currently being implemented on the NTRG Ad Hoc Networking test bed, which has test nodes running Windows CE on Hewlett Packard Jornada Palmtop devices. The Palmtops are linked using FM radios. Dynamic Source Routing (DSR) [9] and Zone Routing Protocol (ZRP) [10] algorithms are used for routing. The NTRG software stack [11,12] structure is shown in figure 1.

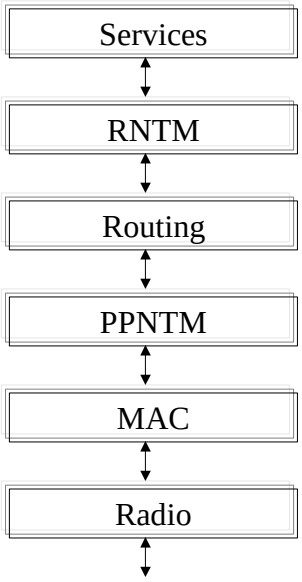

Figure 1 : Layer Structure

One of the applications that the stack provides at present is a Session Initiation Protocol (SIP) [13] based telephony service. The security system is divided into two distinct layers: the Peer-to-Peer NTM (PPNTM) layer and the Remote NTM (RNTM) layer. The PPNTM layer is situated below the routing layer, as its primary goal is to secure communications between the neighbours (i.e. nodes in the radio range). The RNTM layer provides end-to-end encryption so consequently it has to be located just above the routing layer. The threat of eavesdropping by an external attacker is

mitigated by the PPNTM layer. Since the symmetric encryption keys are to be negotiated between the neighbours using Station-to-Station (STS) [14] it is impossible for a node to eavesdrop on communications without authenticating itself. The end-to-end key negotiated by RNTM layer will protect against the internal attacker. We assume that all the links are bi-directional. Figure 2 depicts the solution proposed.

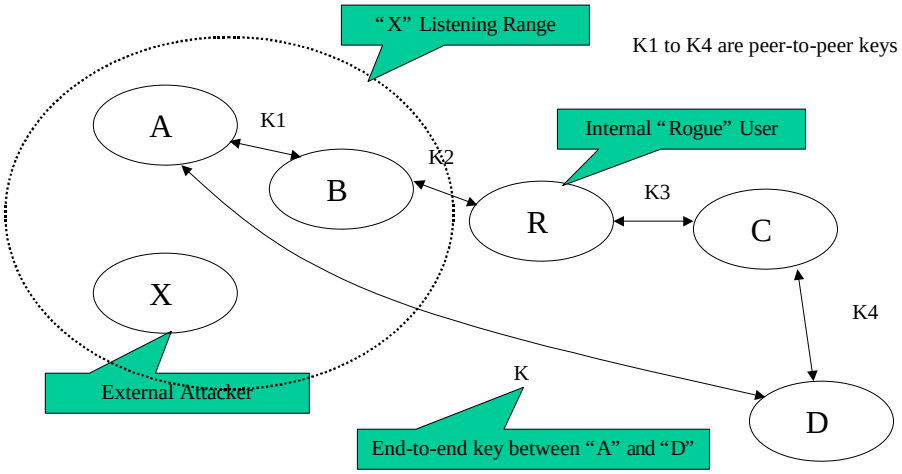

Figure 2 : Key Formation in NTM

Each node has to have at least one Network Address Certificate that entitles it to use certain network address(s) and participate in packet relaying. This certificate is used in PPNTM layers STS key exchange for authentication. The RNTM layer requires that the user have at least one Identity Certificate for identification. RNTM relies on Identity Certificate so that user can move between nodes still maintaining trust. The certificates have to be signed by a third party. Absence of the trusted third party during negotiations is taken care of by using one of the three models proposed at the end of this section.

The PPNTM layer is a simple layer that will try to negotiate a symmetric key with neighbours. Using three models proposed at the end of this section does authentication of the remote certificate involved in the STS key formation. The RNTM layer has the responsibility of carrying out trust negotiations and negotiation an end-to-end encryption key. This dual responsibility makes this layer somewhat intricate. The trust negotiation is carried out by incrementally exchanging certificates. The certificates are asked for by using the attribute name / value pair. Usually a node trying to access some services on the remote node for which it hasn't being cleared triggers the trust negotiation. The trust negotiation can be also be explicitly triggered by the RNTM layer.

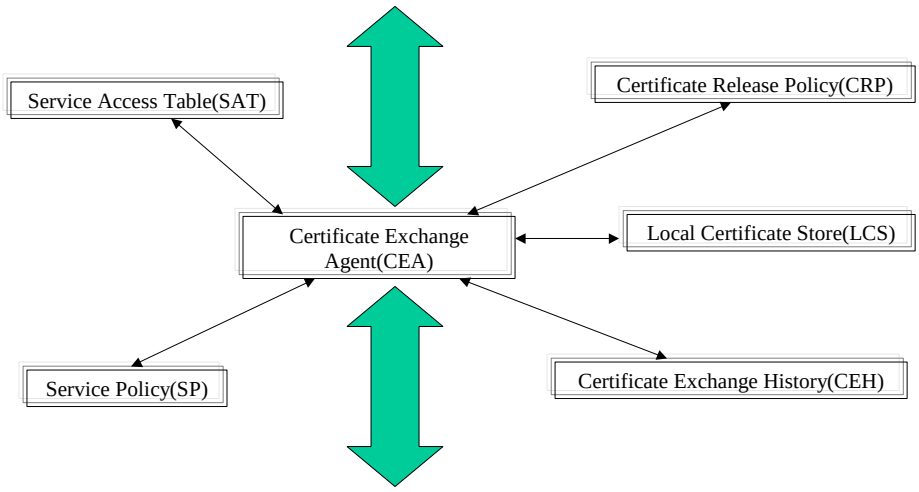

Figure 3: Internal Organization of RNTM

The internal organization of RNTM layer is shown in Figure 3. The Certificate Exchange Agent CEA is the heart of this layer. It gets the message from the layers above or below and acts on them accordingly. The CEA is programmed with a negotiating strategy for the trust negotiation and does so with the help of other data structures in the layer. The Local Certificate Store LCS contains the local certificates to be used in negotiation and the certificates of the trusted certificate issuers and their respective certificate revocation list (CRL). The CRP contains the release policies for each of the certificate in the LCS to be used for trust negotiation. An association between the certificates and the services is maintained in the SP. The CEH keeps a record of the old trust negotiations for ease of future negotiation. The mapping between the services allowed and the identity to which it is allowed is kept in the SAT. It also contains the end-to-end encryption keys.

The different models for finding trust in a certificate are necessitated by the absence of an online trusted third party. The simplistic first model assumes that the node is primed for local use and has all the CRL's updated. Any certificate issued by an unknown certificate issuer cannot be verified and will be referred to the user. The second model is a probabilistic model. Each of the trusted certificate issuers has a trust value of 1 associated with it. There is a distrust value, which is subtracted from the trust value of the CRL if the scheduled update of the CRL is missed. Then the trust negotiation takes place with a default trust value and it should be exceeded for negotiation is to succeed. The third and last model assigns weights to the certificates.

The paper is an overview of the NTM scheme. The syntax for the policy exchange dialog is currently under development. We have completed the initial design phase and are in the process of developing a prototype implementation.

4.Conclusion and Future work

We have surveyed the existing systems available for trust negotiation and trust formation. Their limitations and drawback for Ad Hoc Networks was discussed briefly. We then outline a scheme for trust negotiation in Ad Hoc Networks that copes

well with the absence of an online trusted third party. Additionally a key formation scheme was also proposed to protect the trust negotiation and other basic mechanisms of Ad Hoc Network. To ensure future compatibility the scheme is designed to operate in conventional networks also.

The NTM can be used to establish the membership for group formation in Ad Hoc Network. Neighbour aware routing solutions can also be aided by our scheme. This scheme can be applied for high security military scenarios and as well as little security civilian scenarios.

Through NTM is somewhat complex we are trying to refine it for a first time user who does not have much experience.

5.References

[1] Simple Public Key Infrastructure (SPKI), http://www.ietf.org/html.charters/spki-charter.html.

[2] M. Blaze, J. Feigenbaum, and A. D. Keromystis, "The KeyNote Trust Management for Public-Key Infrastructures" Cambridge 1998 Security Protocols International Workshop, England, 1998.

[3]A. O. Freier, P. Karlton and P. C. Kocher, “The SSL Protocol Version 3”, http://home.netscape.com/eng/ssl3/ssl-toc.html.

[4] T. Dierks, C. Allen, "TLS Protocol Version 1.0," draft-ietf-tls-protocol-06.txt, November 12, 1998.

[5] W. Winsborough, K. Seamons and V. Jones, "Automated Trust Negotiation," DARPA Information Survivability Conference and Exposition, Hilton Head Island, SC, January 2000.

[6] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, 13(6), November-December 1999.

[7] Jean-Pierre Hubaux, L. Buttyan and S. Capkun “The Quest for Security in Mobile Ad Hoc Networks” Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001), Long Beach, CA, USA, October 2001.

[8] Pretty Good Privacy (PGP), http://www.pgp.com

[9] J. Broch, D. Johnson, and D. Maltz, “The dynamic source routing protocol for mobile ad hoc networks,” http://www.ietf.org/internet-drafts/draft-ietfmanet-dsr-03.txt, Oct 1999. IETF Internet Draft (work in progress).

[10] Z. J. Haas and M. R. Pearlman, "The zone routing protocol (ZRP) for ad hoc networks (Internet-Draft)," Mobile Ad-hoc Network (MANET) Working Group, IETF, Aug. 1998. IETF Internet Draft (work in progress).

[11] O'Mahony, D. & Doyle, L., “Architectural Imperatives for 4th Generation IP-based Mobile Networks”, invited paper, to appear in Proceedings of the fourth international symposium on wireless personal multimedia communications, September 9-12, 2001, Aalborg, Denmark

[12] O'Mahony, D. & Doyle, L., “An Adaptable Node Architecture for Future Wireless Networks, in Mobile Computing: Implementing Pervasive Information and Communication Technologies”, Kluwer series in Interfaces in OR/CS, Kluwer Publishing, in press for August 2001

[13] H. Handley, H. Schulzrinne, E. Schooler and J. Rosenberg, “SIP: Session Initiation Protocol,” http://www.ietf.org/rfc/rfc2543.txt, March 1999. IETF Internet Draft (work in progress).

[14] W. Diffie, P.C. van Oorschot, and M.J. Wiener, “Authentication and authenticated key exchanges,” Designs, Codes and Cryptography 2 (1992).