Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Key Protocol Coordination in Mobile Ad-Hoc Networks

Mr.N.Satish Kumar[1], B. Vijay Kumar[2] and Dr.N.Satyanarayana[3]

[1] SVS Institute of Technology, Bheemaram, Warangal(AP), India

Received: 28 May 2011 Accepted: 21 June 2011 Published: 4 July 2011

Abstract

In this paper we propose and design key authentication protocols for wireless networks. We consider three mobile service domains; each has an authentication server. We denote by D1, D2 and D3 corresponding authentication servers. For simplicity, let D1, D2 ,D3 represent those three domains. This mobile system can provide mobile communication services to a large number of users. For simplicity, we assume three users (A, B and C) in the system only, where A has registered with D1 and B has registered with D2 and C has registered with D3.

Index terms—

1 I. INTRODUCTION a) Symmetric-key

An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Contrast this with public-key cryptology, which utilizes two keysa public key to encrypt messages and a private key to decrypt them. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Symmetric-key cryptography is sometimes called SECRET-KEY CRYPTOGRAPHY. The most popular symmetric-key system is the DATA ENCRYPTION STANDARD.

2 b) Types

Symmetric-key algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt the bits of the message one at a time, and block ciphers take a number of bits and encrypt them as a single unit. Blocks of 64 bits have been commonly used.

3 d) Inter Domain

In computing, inter-domain is a term used to describe interaction between domains. It is most commonly used in the fields of multicasting and routing between internets, or as a substitute for the term interserver. Internet protocols that are focused on interdomain functions include: Border Gateway Multicast Protocol, Classless Inter-Domain Routing, Multicast Source Discovery Protocol, and Protocol Independent Multicast. The opposite of inter-domain routing is intradomain routing (routing within a domain or an autonomous system).

4 e) End-To-End Authentication

An authentication protocol is a type of cryptographic protocol with the purpose of authenticating entities wishing to communicate securely. There are many different authentication protocols such as: Kerberos, RADIUS (Remote Authentication Dial In User Service) and so on. End to end authentication protocol is a computer network authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It provides mutual authentication -both the user and the server verify each other's identity. ? B sends D1 a request, including a Token, nonce, "identity package" and hash value. B's subliminal identity for anonymity. ? The Token is encrypted so as to be passed on to D2 without D1 being able to read it. ? The content of the Token will allow D2 to authenticate B. ? D1 cannot verify the hash value or

decrypt the request, since it doesn't have K B,D1 , which is generated using a strong one-way hash function f. Step 1 : A send a request to his home (D1) server that A wants to communicate with B and C.

5 PROPOSED PROTOCOL DESIGN

Step 2 : After verifying request D1 is looking for B and C's home domain and determine that B and C are in the same home domain. Now D1 generate a session key K ABC and send to B along with B's new identity for future communication.

Step3 : Now B confirms to D1 that B is ready to communicate with A and C.

Step 4 : D1 talks to C that A and B want to talk to you; then D1 sends session key K ABC along with new identity of C.

STEP 12 : C ? B

Step 5: C confirms to D1 that C is ready to communicate with A and B, and send identity along with response.

Step 6 : D1 send session key with identity of both B and C to A and A's new identity.

Step 7 : A, B and C can communicate securely.

V.

6 CONCLUSION

We are all aware of the growth in routing complexity, and the rapid increase in allocation of network numbers. So, we need some setup rules for secure communication between end-to-end machines. In Inter-Domain Routing Protocol (IDRP) provides secure routing for OSI defined network environments, which is similar to BGP in the TCP/IP network. The Border Gateway Protocol (BGP) provides a standard mechanism for inter-domain routing among heterogeneous domains, called autonomous systems (AS), here each domain has the administrative control over its intra-domain routing protocol and inter-domain routing policy, which is not known to the other domains.

Figure 1:

[1]

[1] © 2011 Global Journals Inc. (US)

STEP 11 : B ? C ? B sends message to C with nonce and under encrypted with session key K S .

.1 August

? C sends message to B with nonce and under encrypted with session key K S .
STEP 13 : A ? C ? A sends message to C with nonce and under encrypted with session key K S .
STEP 14 : C ? A ? C sends message to A with nonce and under encrypted with session key K S .

.2 ADVANTAGES OF PROTOCOL

There are some key advantages using propose Inter Domain protocol. Advantages are listed below: 1. Using user identity (called anonymity). 2. Nonce -using for anti reply attack. 3. Provides data integrity and confidentiality. 4. Users are authenticated by their home domain. 5. Establishment session key for particular session. 6. Updated identity after each session by the home server.
IV.

.3 CASE STUDY

There is only one mobile service domain and has an authentication server. The authentication server is denoted by D1. Assume there are three mobile users A, B and C, each one is registered with D1. If A, B and C wants to communicate securely with each other then they have to follow the steps below.