Review “Kerberos”

Name: Wenhui Zhang
Email: wuz49@ist.psu.edu

Paper Name：

Neuman, B. C., & Ts'o, T. (1994). Kerberos: An authentication service for computer networks. *IEEE Communications magazine*, *32*(9), 33-38.

Contribution:

Neuman et. al. defines authentication, Integrity, confidentiality and authorization in this paper. To illustrate how authentication works for real-time and interactive computer networks scenario, this paper introduces Kerberos, which is an authentication protocol based on cryptography.

Motivation:

People discover that password based authentication does not fit the needs of computer networks. It is claims as passwords are vulnerable with threats due to eavesdropping and impersonating on the network. People also discover that although authentication by assertion is more convenient for users, this method could be thwarted by modification of application. Thus authentication methods based on cryptography is required.

Related works:

Kerberos is developed from Needham and Schroeder’s authentication protocol. In addition to authentication servers, conventional algorithms, and multiple authentication servers mentioned in Needham and Schroeder’s authentication protocol, Kerberos also assumes all systems on the network to be synchronized.

This paper also discusses about other two approaches for enhancing network security: (1) one-time passcodes, which is superior to Kerberos in case of password stolen by Trojan horse on users’ side; (2) public-key cryptography, which is superior to Kerberos in case of supporting for non-repudiation.

Methodology:

In Kerberos protocol, 3 sub-protocol are mentioned: (1) Authentication Service Exchange; (2) Ticket Granting Service Exchange; (3) Client/Server Exchange. A third party authenticator is involved, it is named after Ticket Granting Server. In sub-protocol (1), client requests ticket from authentication server, KDC verifies identity of client, client decrypts Session Key using Master Key, and get Ticket Granting Ticket(TGT). In sub-protocol (2), client sends Ticket Granting Service Request to KDC, so that client requests tickets without repeatedly sending credentials. In sub-protocol (3), authentication server sends tickets and encrypted request to application server.

Results:

Kerberos accommodates 3 scenarios: (1) client-verification without sending sensitive data through network with potential threats; (2) ticket granting service frees client from requesting tickets with repeatedly sending credentials; (3) Kerberos allows users making authentication cross-realm

Take away:

Kerberos is better than password authentication in computer networks environment. Kerberos uses private key encryption, thus it suffers from scalability problems.