DISTRIBUTED SYSTEMS - ENGR-4790U

DISTRIBUTED SECURE CHANNEL PROJECT PROPOSAL

REVISION 1.5

CREATED BY

DANIEL SMULLEN

JONATHAN GILLETT

JOSEPH HERON

11/03/2013

TABLE OF CONTENTS

INTRODUCTION

CURRENT APPROACHES AND THEIR PROBLEMS

Nearly all widely adopted cryptographic systems are based on a centralized model rather than being distributed. One of the most widespread forms of cryptography, Public Key Infrastructure (PKI), is used for TLS - Transport Layer Security (used in HTTPS). It depends on a direct client-server interaction in addition to a centralized Certificate Authority (CA). Even in other systems which are somewhat more distributed (such as WPA cryptography, which is used for wireless access points), the system still relies on the use of a centralized authority (the wireless access point) to authenticate nodes.

CURRENT DISTRIBUTED APPROACHES AND THEIR PROBLEMS

Other common methods of distributed cryptography rely on the use of a symmetric key, such as JGroups. In this mode, all nodes in the distributed system use the same key for encryption and decryption. While this method can be effective, it has many inherent shortfalls in functionality when it is scaled to larger distributed networks. These flaws revolve around providing authentication, issuing new keys, and the signing of messages to ensure integrity - no distributed facility is available for another node on the network to perform these functions.

OUR PROPOSED NOVEL SOLUTION

This project aims to address the challenges of distributed cryptography. It will do so by creating an innovative new Distributed Secure Channel (DSC) as a means to provide a distributed, fault-tolerant, secure channel for communicating over an insecure network. It is based on the concepts of the two most popular distributed cryptographic systems: Pretty Good Privacy (PGP) and Bitcoin. It relies on peer to peer network technologies, peer discovery, and a novel authentication scheme.

HIGH-LEVEL SYSTEM REQUIREMENTS

The requirements for the system are broken down into functional and nonfunctional requirements as specified in the following table. In order to focus the efforts of the project on creating a working DSC, rather than focusing on the underlying peer-to-peer networking, the JGroups library will be used to address the networking requirements of the project.

Number	Requirement Name	Type	Description
1	Distributed Architecture	Non-functional	The system must be distributed without any central node that all other nodes are dependent on.
2	Secure Channel	Non-functional	The system must have the ability to create a secure communication channel that cannot be overheard or tampered with without the knowledge that messages have been tampered with.
2.1	Public Key Verification	Functional	The system must have a means of verifying the public key of new nodes attempting to join the network.
2.2	Public Key Signing	Functional	The system must have a means of signing the public key of a new node attempting to join the network.
2.3	Authenticated Node Announcement	Functional	The system must have a means of announcing each new authenticated node that has joined the network to all other nodes.
2.4	Joining the Network (Authentication)	Functional	The system must have a means so that an already authenticated node that is reconnecting to the network can receive an updated list of authenticated nodes.
3	Stream Cipher	Functional	The system must have a stream cipher to facilitate the encryption and decryption of information exchanged by nodes.
4	Relay Chat	Functional	One application of the network (for demonstration purposes) must show a simple Internet Relay Chat style client, which allows users to send messages to all other users subscribed to the network.

PRELIMINARY ARCHITECTURE

The architecture of the system is a peer-to-peer network that is operating on top of the underlying UDP network infrastructure. The JGroups library will be used to facilitate the creation of a reliable multicast distributed system. Nodes will belong to a cluster, which will be used to send messages to all nodes connected to the JGroups cluster.

The cryptographic implementation of the system will facilitate distributed authentication and signing. Encryption through the use of both public key cryptography for the signing and authentication, and symmetric key cryptography for the encryption and decryption of messages will be required. The architecture of the cryptographic system is dependent on the peer to peer network for facilitating the authentication and encryption/decryption in a distributed manner.

PROPOSED DISTRIBUTED TECHNOLOGIES

PEER TO PEER NETWORK

A peer-to-peer overlay network is created on top of the underlying UDP network infrastructure. Rather than creating our own overlay network, the JGroups library will be used to facilitate the creation of a reliable multicast distributed system.

NEW PROTOCOL ARCHITECTURE

The DSC shares a common network channel with other untrusted clients. However, the DSC peer to peer network facilitates transmitting messages securely even in this insecure environment. Only peers that have been authenticated and are trusted can join the peer to peer network and disseminate messages to other nodes on the secure channel. Since any type of message can be disseminated, the peer to peer network architecture and the cryptographic system itself can be used as a secure channel for any type of application. Facilities for encapsulating higher-layer messages so that other applications can be built on the secure channel will be included as part of the design.

DISTRIBUTED CRYPTOGRAPHY

The system will use a new distributed cryptosystem that facilitates distributed authentication rather than relying on a centralized signing authority. It will support network scalability by adding newly authenticated nodes. Most traditional cryptosystems involve either asymmetric or symmetric communication between two clients, or a client to many peers through the use of a centralized signing authority (such as HTTPS). The proposed cryptosystem will require both distributed encrypted communication and distributed signing and authentication.

APPLICATIONS

For the purpose of demonstrating the functionality of the distributed secure channel, a simple Internet Relay Chat style client will be created that allows users to send messages to all other users subscribed to the network. Due to the dissemination behavior of the network, IRC style chat makes good use of the ability for messages to be quickly transmitted to all authenticated subscribers of the network.