ATHENA

We'd call it Hermes, but we're not just a messenger.

Athena – a suite of programs providing encrypted communications via RSA

Developers:

Gregory LeBlanc
Norman Maclennan
Stephen Failla

Latest Revision: May 3, 2010

Abstract

The purpose of this application is to ensure the delivery of messages over the Internet using a fully encrypted transfer mechanism. The application will have its own authentication server in which users will verify their information. Users will also have the ability for encrypted file and image transfer. This application will use the most updated encryption standards (RSA and AES) – it will also use the SHA-256 hashing algorithm to hash the user's private key. The key exchange process will be totally seamless. The user will not have to remember his or her public or private key, only their password that they will use to login. Their private keys will be stored, encrypted, on their machines; we will never store a copy of their private key. Once the users are connected to one another, they will have the option to generate and use a session key (via Diffie-Hellman) and AES encryptions instead of public keys and RSA encryption for increased speed and security (one-time keys are less traceable). The user will be able to send and receive encrypted emails using a permanent email address with the service ([username]@athenachat.org). They will also be able to send 'one-off' encrypted emails using a randomly generated email address that changes each time the user sends something. The user will also be able to export his or her key pair.

Value

Over the past 5 years, more emphasis has been put on security – especially when it comes to sending messages over the Internet. Many people have fallen victim to their information being stolen by an unauthorized listener. There are many ways to secure your data when it comes to data transmission such as IM and email. This application wishes to simplify the operation and use of such technology. Our application will make the complicated process of securing IM chat and email a thing of the past. There will be no difference in the setup of the program from any other Instant Messaging client that one has used in the past. A person's information, whether it be a message they are trying to send to their significant other or a Department of Defense document, is very important, and our application removes the risk of a third party being able to see this information. In addition, many oppressive governments across the world have taken to censoring the Internet and spying on their citizens. This software will allow citizens of these oppressed countries (especially human rights activists and journalists) to communicate freely with the outside world without fear of government reprisal. Our server will not keep logs of connections or conversations, so even if subpoenaed by law enforcement, we would be unable to retrieve any information about a user's conversation.

Simplicity

Athena will be extremely simple and straightforward. User creation will be only filling in a few lines of text and clicking a few “next” buttons. Once your username has been registered with our authentication server, the key generation process will take place. This should only last a few minutes. Once the user is logged back in they will see the standard “buddy list” type screen. They will have many options from there to choose from. The GUI will be very intuitive. Any option will be clearly defined and the application will have a clear and detailed help menu. This program is designed for a person that is familiar with the basic operations of a computer, such as: clicking on an icon, doubling clicking on an icon, finding the start menu, understanding the meaning of “instant messaging.” We will also have a detailed community webpage where users will find updates to Athena and forums to discuss bugs and possible content for future releases.

Current Technology

There currently are three other fully encrypted instant messaging clients (See link: http://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients). The current clients out there are: X-IM (http://X-IM.net), Brosix, and BitWise Communications. Brosix is an “Enterprise” only chat client – it is meant for businesses to implement in their networks. They do have a free version but it is designed to be a trial version of the full product. BitWise communications has one free version and two paid versions – they also market heavily on enterprise communication. X-IM's aims are closer to that of Athena, but it differs in a few key areas. X-IM offers a similar level of encryption, but they application is entirely closed-source, meaning the user has no way to verify that the application works the way the company claims. X-IM also offers two different tiers of service: free and 'pro'. The free version lacks file transfers, digital signatures, and is supported by advertisements. The main difference right away is Athena will always be free and open source. That is something that we pride ourselves upon. Our software will be easily implementable by anyone with a computer capable of running MySQL (server) and the Java JRE (client/server). This application will be different because it is not only designed for the business world – is designed for the average security conscious user as well. We would like to create a community that prides itself on being secure and being private. The other three clients generally use the same encryption standard as our application (because it’s becoming the industry standard).

Requirements

Minimal Hardware Requirements:

Operating Systems: Windows XP SP2 or greater

Linux Kernel Version 2.4.x or greater

Mac OSX Leopard or greater

Architecture: x86, x86_64

Memory: 64 MB

Software Requirements:

Java 6 JRE or greater

An Internet connection