DEVELOPMENT OF SECURE MODELS AND ALGORITHMS FOR THE EXCHANGE OF SERVICE MESSAGES BY MESSENGERS

M.M.Karimov
Director of the State Test Center under the Cabinet of Ministers of the Republic of Uzbekistan
Sh.R.G`ulomov
Dean of the Faculty of Cyber Security of Tashkent University of Information Technologies named after Muhammad al-Khorazmi, Uzbekistan
T.T.Eshniyozov
Master's degree, Faculty of Cyber-Security,Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

Abstract: *Recently, intrusion detection systems (IDS) have been introduced to effectively secure networks. Using neural networks and machine learning in detecting and classifying intrusions are powerful alternative solutions. In this research paper, both of Gradient descent with momentum (GDM)-based back-propagation (BP) and Gradient descent with momentum and adaptive gain (GDM/AG)-based BP algorithms are utilized for training neural networks to operate like IDS. To investigate the efficiency of the two proposed learning schemes, a neural network based IDS is built using the proposed learning algo- rithms. The efficiency of both algorithms is inspected in terms of convergence speed to achieve system learning, and elapsed learning time using various settings of neural network parameters. The result demonstrated that the GDM/AG-based BP learning algorithm outperforms the GDM-based BP learning algorithm.*

Mobile Instant Messenger is one of the most application which use to exchange a message between Sender and Receiver over public network, so that it is very important building an application with good level of security aspect and fast communication. This paper propose a secure Mobile IM in excanging data over internet with an virtual network method. In this model, we propose a Mobile Instant Messenger with virtual network. It will implemented in JXTA protocols which establish a virtual network overlay on top of the Internet, allowing peers or device to directly interact and self-organize independently of their network connectivity and domain topology. This method developed with Pipes as virtual communication channels used to send and receive messages between services and applications, the pipe binding consists of searching and connecting the two or more ends of a pipe. This is new approach of IM communication method, that is message must be deliver over virtual network with good level security.

Keywords: *Intrusion detection systems (IDSs), Neural networks (NNs),Back-propagation (BP), Secure messaging; Cryptography; Encryption; Decryption; Web application; Android apps.*

Introduction. Currently, Instant Messenger (IM) as one of the most application used in message transaction certain need a security aspect and effective communication. The well known of P2P communications and applications have increased in the implementation

of wired network for few years ago. However, there is no effective adaptation of these new technologies in development of mobile environment. Today, a lot of mobile device like smart phones and computer tablet have become a commodity and highly-capable devices that running in the mobile environment. On the other hand, the introduction of a Direct protocol on top of the existing technologies in wireless has provided users with more opportunities to utilize the P2P data transaction with mobile devices at anytime and anywhere. Based on current paper of communication technology development, P2P has grown so rapidly in IM implementation, P2P communication is considered as one of the most important and suitable networking technologies for mobile data transaction between sender and receiver, P2P model will allows direct communication between devices, free and extensible distribution of resources in a network and search for amount of resources which will implement to maximize the network performance. Most of existing IM application have ability monitoring user who are online at that time and make an informsation transaction with each other user almost in real-time. In addition, IM have ability to identify who are in a presence, and start a text message for real time chat. Most of IM application is easy to install in a hardware like computer or smartphone so that it has made the application very popular. When IM has been installed, user of IM must log in to a public IM service network to start IM service, most of IM application who are users still online in that time. The user just selects which user to communicate and the user can send any message to selected users. Communication in IM application for all messages can either be transmitted client server model or directly through peer-to-peer connections. In this paper we propose a scheme to delivery peer to peer message with a virtual network environment. Message authentication is one of the most important security services in computer and communication application. Nowadays, Knowledge-based authentication (use password) and key-based authentication (use public/private key) are the two most popular approaches. Knowledge-based authentication has some security drawback. Most users like to use simple and short passwords. It will make privacy data will be risk for unauthorized person Unauthorized people can easily crack the simple passwords and making attack. To solve the problems, public-key cryptography has been implemented to provide user authentication. Most of application use Public-key-based authentication which needs a certificate authority (CA) to give the authenticity of public keys. As we know, public-key computations will need large memory and long time enough, for this problem algoritm choice become a solution to alleviate overhead. Computational overhead is one of the main concerns for publickey based authentication.

Materials. A secure architecture is divided into four modules; chat module, transceiver module, secure module, and routing module. In this research, hash algorithm was applied in secure module. The main function of hash algorithm is to encrypt and convert into hash value. The purpose of this encryption is to ensure unauthorized person cannot view the original data or information through the network. IM application was developed and tested for security analisys. Another autentication for security method called group authentication, which authenticates all users at once. The group authentication is specially designed to support grouporiented applications. In the group

authentication, the group manager. The propose a special type of authentication, called group authentication, which is specially designed for group-‹›riented applications. The proposed group authentication is no longer a one-to-one type of authentication and it is a many-to-many type of authentication. Group authentication can authenticate multiple users at once. Our proposed (t; m; n) group authentication schemes, A reseach in securing 1M message was developed a specific protocol for 1M which consist of EIGamal cryptosystem, RSA algoritm, and Chinese Remainder Theorem (CRT). In the protocol, the CRT used to update user private key while effort of those algoritm interaction depends on integer factorization problem (IFP) dan discrete logarithm problem (DLP). In the system. the EIGamal Cryptosystem regard as a middle way (connector) between Diffie-Hellman and temporary key applying. This method regard more secure and give faster system in 1M.

Methods. P2P systems usually constructed by various types of architectures and internal logics. The design of systems is to adapt to the specificities of the networks on top of which they operate and to the characteristics of the applications using them. For instance, the ability to identify a single node quickly in a large network size is required by some applications especially for real time communications, while the focus of others such as file sharing is placed on locating the same resource in different end nodes for more reliable retrieval of the resource. In order to address these challenges, various approaches have been adopted in P2P applications. The approaches can be comprised into two main parts: that is structured and unstructured. The structured P2P network is a network in which nodes cooperatively maintain routing information about how to reach all nodes in the overlay and the contents sharing are placed only at specified peers. This architecture maintains the sending messages to reach to the correct and accurate destination even if the network contains a huge number of nodes. The examples of such structured P2P networks Distributed Hash Tables (DHTs).

Results. In real implementation of of P2P there is more chalanges and limitation. Since the P2P concepts have been increasingly realized in the ensemble mobile environment, many challenges arise in this particular domain. It can be summarized that the majority of such challenges are constituted by the heterogeneity of the mobile environment (networks, devices, users). Thus, in the current paper concerning with mobile P2P, we especially refer to heterogeneity compared with conventional, fixed network P2P systems in which, to the largest degree, homogeneous nodes are assumed. There are requirements which have to be taken into consideration for P2P in ensemble mobile environments, and they are listed as follows: The P2P communication is responsible for providing a facade that makes two peers that don't have a direct connection to each other seem as if they do. This makes the JXTA network appear to be a many-to-many network topology. Having a separate protocol for this virtual connection means that the endpoint service doesn't need to know whether two peers are directly connected. To accomplish this, the protocol defines a number of messages, consisting of queries and responses (in much the same way many of the other protocols do). The query and response messages are as follows: Ping query—The endpoint service sends this message to determine whether there is a route between peers in networks. In most situations, the connection will be a direct one

and won't involve propagation. When a peer receives a ping query message, it responds to the message for indicating that the peer destination is active and can be routed. Ping response—When a peer receives a ping query, it sends a ping response message. The message will let the source peer know that a route is available between the peers. Route query—this operation must be run when a peer needs to send a message to another peer, but doesn't have a direct route, it sends a route query message to the peer's directly connected peer looking for a route to the peer. Route response— this operation must be run when a peer has a route to a target peer, the peer sends a route response to the requesting peer. In other words, in this step the route response message is an answer to a route query message. In this model a device, service or application called as peer. A peer is a virtual communications point. This approach will have multiple peers on a smart phone or device. A peer is not the same as a user because a user may have peers on their phone, office/home computer, or other devices. It is also possible to have multiple peers on a single device, not necessarily an ideal situation but good for debugging. Because a peer is not the same as a user, applications need to abstract the idea of user separately from peers. Any abstraction of users should be viable when a user has access to multiple peers. Peers will be included with specific network services that they provide while connection

Conclusion. In terms of personal data security and privacy, Signal, Threema, and Wickr Me are the top messengers. However, each service has its pros and cons. The ideal application in terms of absolute security and anonymity of secure instant messaging has yet to be created.

It is impossible to provide high anonymity without sacrificing other features. For example, the speed of message delivery in a more secure messenger is significantly reduced, there is a limit on the size of an attachment, etc. That being said, when choosing a messenger for everyday communication, an ordinary user should find a reasonable trade-off between convenience and security.

The main objective of the proposed system is to transfer message in a communication system securely. Android-based and webbased applications for secure messaging have been developed using cryptographic algorithms for the users to send their message between registered users on any organization securely. The application is supported through user authentication before sending message. The proposed secure messaging system uses minimal processing with little overhead while maintaining security. The authentication of each user is made strong by storing sensitive credentials for each user by using Salt in the database. Encryption and decryption of message are done by using keyword mono-alphabetic substitution algorithm, which is based on Advanced Encryption Standard (AES). This is less secure than the public-key encryption scheme. This is main limitation of this work. An eavesdropper that breaks into the message will return a meaningless message. Obviously encryption and decryption is one of the best ways of hiding the meanings of a message from intruders in a network environment. The proposed secure messaging can be used in many areas with personal and company-wide sensitive data exchanges. For example, financial institutions, insurance companies, public services, health organizations and service providers rely on the protection by Secure Messaging. It is

concluded that the developed application can be considered for chat, messaging, video conferencing and real time file sharing in these application areas. The proposed system has been designed and developed with easy integration and modification to take full advantage of future technologies. There are some limitations in the current system to which solutions will be provided as a future development; such as, small number of keywords uses only keyword mono-alphabetic substitution algorithm and network bandwidth. In future, a public-key encryption scheme will be implanted in secure messaging system.

REFERENCES:

1. Motta, R., Pasquale, J.: Wireless P2P: Problem or Opportunity?, pp. 32-37 (2020).

2. Kirsimäe, S., Norbisrath, U., Singer, G., Narayana Srirama, S., and Lind, A.: Extending Friend-to-Friend Computing to Mobile Environments, pp. 75-80 , (2021).

3. Ishikawa, N., Sumino, H., Kato, T., Hjelm, J., Murakami, S., Kitagawa,K., Saito, N. : Peer-to-Peer Networking Platform and Its Applications for Mobile Phones, Mobile peer-to-peer computing for next generation distributed environments: advancing conceptual and algorithmic applications, p. 374, (2019).

4. Kato, T., Ishikawa, N., Sumino, H., Hjelm, J., Yu,Y., Murakami, S.: A Platform And Applications for Mobile Peer-to-Peer Communications,(2020).

5. Gunter Ollmann (2004). Securing against the threat of instant messengers. Network Security, Vol. 2004, March 2020, pp. 8-11

6. K. Ren, S. Yu, W. Lou, and Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 4554-4564, Oct. 2019

7. L. Harn and J. Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications,"IEEE Trans. Wireless Comm.,vol. 10, no. 7, pp. 2372-2379, July 2021.

8. M. Yusof and A. Abidin, "A secure private instant messenger," in Proc. 17th Ascia-Pacific Conference on Communications, 2021, pp.821-825

9. L. Ham, "Group Authentication," IEEE Trans. Vehicular Technology, vol. 62, no. 9, Sep. 2019

10. I. Downnard, "Public-Key Cryptography Extensions into Kerberos," IEEE Potentials,vol. 21, no. 5, pp. 30-34, 2018