Security in Emergency Situations

A Preliminary Report

Jun Yi, Yiming Peng

A. Abstract

In emergency situations, more and more the wireless communication network technology are used, this kind of emergency response system improves the efficiency of emergency response and management. However, there are also a great deal of information network security issues, including data integrity, information confidentiality, user authority authentication, interception in communication, eavesdropping and so on. It is important and necessary to make sure the security of emergency response system and provide a secure communication system for emergency situation. In this project, we mainly consider two security issues, first one is the user authority authentication of emergency responder, and the other one is the security of the whole communication process between the client and the server. In the security system, we choose the most popular encryption algorithm- MD5 Salt in front login system, and take the network authentication protocol- Kerberos algorithm as our theory basement in the whole communication encryption to prove the data authenticity, integrity and confidentiality. Finally, we will present the whole process of encryption and transportation in a specific interface. We also plan to design another hacker simulation program to prove the reliability of the system.

Keyword: emergency response system, security, Kerberos, MD5 Salt

B. Specific Aims

The goal of this project is to build a security system, which enhances the emergency response system (e.g. DIORAMA) by offering authorization and encryption for information disclosure and network communication. The security system includes two main targets and there is an overview of the whole system design below.

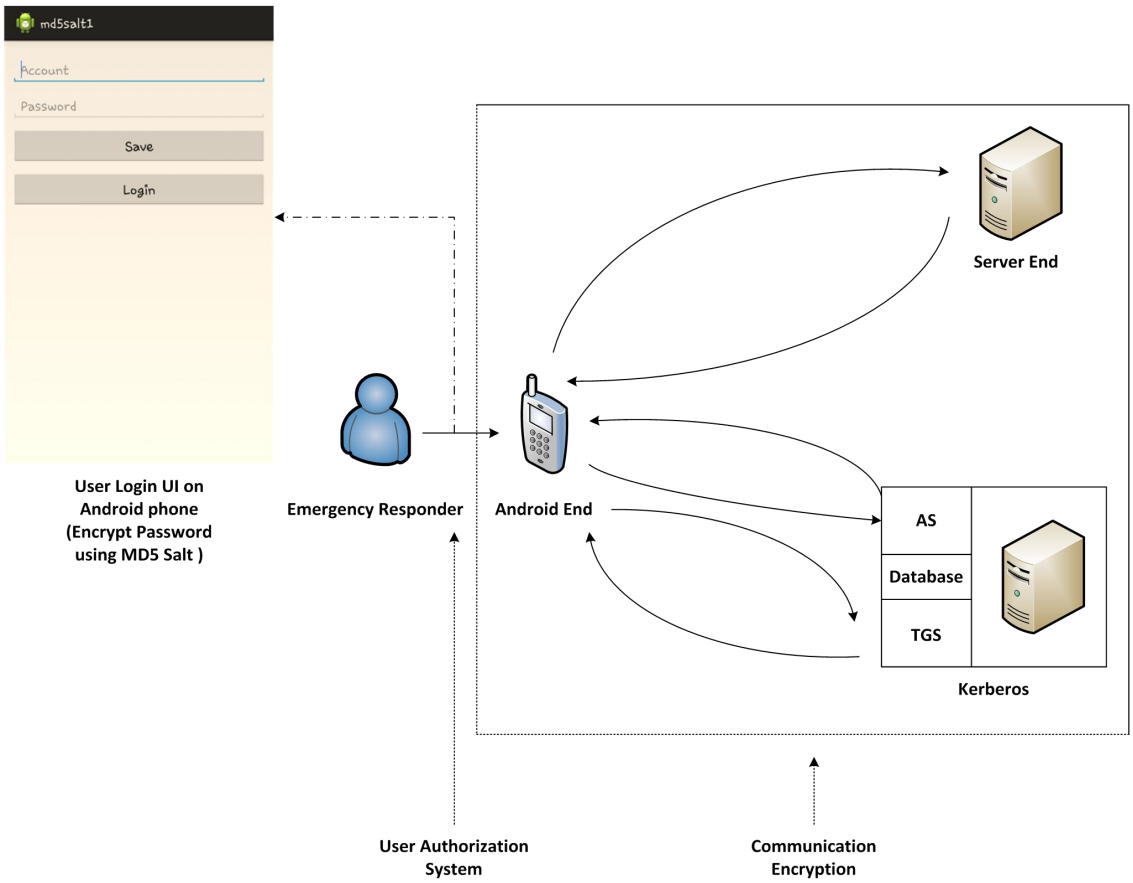

Figure 1 Overview of the security system

Part i User Authorization System

The objective of this part is to design a user authorization system in both Android end and server end, to authenticate the user authority of responder. It is necessary for responders to enter their username, password to login to the emergency response system and get the specific authority to visit the server using their smart phone. The password will be encrypted using MD5 Salt, an irreversible encryption algorithm, and transported to the server. By this way, we can make sure the confidentiality of the emergency response system.

Part ii Communication Encryption

The objective of this part is to build a communication encryption system, based on the network authentication protocol- Kerberos algorithm, to encrypt the whole communication process between client and server. A set of Kerberos algorithm model including Authentication Server(AS), Ticket Granting Server(TGS), and Kerberos Database need to be established. Using the protocol, we can provide a more secure communication process, making it impossible for the unauthorized users to get access to the protected data.

C. Background and Significance

i Background of emergency response system

Emergency response systems (e.g. DIORAMA) are designed to assist the incident commanders in the management of a mass casualty incident, and make emergency responders rescue more efficient.

Emergency response and recovery efforts require timely interaction and coordination of emergency services in order to save lives and property, thus, to prove the data authenticity, integrity, and confidentiality in the emergency system is our motivation to make this design.

ii Evaluation of MD5 Salt algorithm

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of security applications. It is also commonly used to check data integrity.

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512.

MD5 is also irreversible, so we consider MD5 as a reliable encryption algorithm. However, we also consider a specific implementation of this algorithm to make sure the security of the emergency response system. That is to encrypt the password using MD5, add a Salt value to the hashed result and encrypt the whole string using MD5 one more time. In our algorithm, the value of Salt considered to be the hash of the username. In this way, we do not need to establish another database for salt while providing a more secure encryption algorithm rather than single MD5.

iii Evaluation of Kerberos algorithm

Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client- server model and it provides mutual authentication- both the user and the server verify each other's identity. The messages based on Kerberos protocol are protected against eavesdropping and replay

attacks.

Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication.

The specific protocol is described using a diagram below.

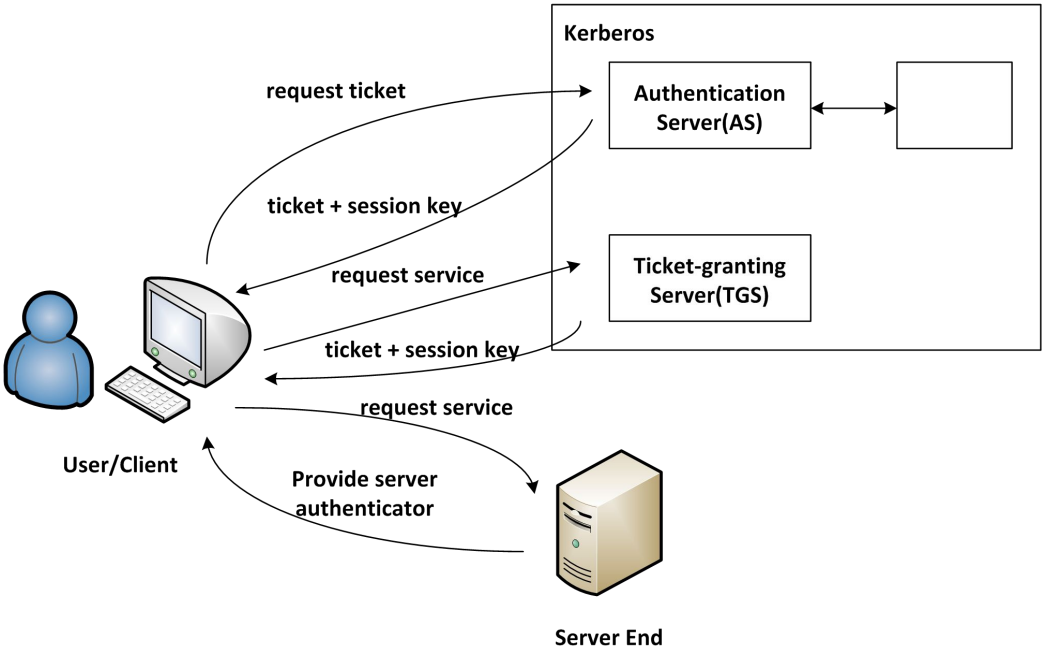

Figure 2 Kerberos Algorithm

In the project, Kerberos Algorithm is the theory basement of the encryption in communication between client and server. And the communication encryption part is also considered the core part of the security system.

iv Significance

The project is designed to build a security system in emergency situation. Different from other security systems, our design focuses on the communication encryption. Considering the importance of the reliable information in emergency situation, it is significant to provide the integrity and authenticity of the whole communication process. By that way, we can make sure the incident commander and emergency responder take measures efficiently and securely.

D. Proposed Work

[1] Jung Ha Paik, Seog Chung SEO, Yungyu Kim, HwanJin Lee, Hyun-Chul Jung, and Dong Hoon Lee, “An Efficient Implementation of Block Cipher in Android Platform”, 2011 Fifth FTRA International Conference on Multimedia and Ubiquitous Engineering

[2] Zhao Hu, Yuesheng Zhu, and Limin Ma, “An Improved Kerberos Protocol based on DiffieHellman-DSA Key Exchange”, Shenzhen Graduate School, Peking University

[3] Radek Pospíšil, “Authentication in Computer Networks and Proposal of One-Time Increase of User Permissions”

[4] Maurizio Casoni, and Alessandro Paganelli, “Security Issues in Emergency Networks”, Vignolese 905, 41125 Modena (MO), Italy

[5] Yunhua XIANG, Qian ZHANG, and Liwei ZHANG, “To Strengthen the Role of Social Security in Emergency Management”, Wuhan University

[6] Qin Li, Fan Yang, Huibiao Zhu, and Longfei Zhu, “Formal Modeling and Analyzing Kerberos Protocol”, Shanghai Key Laboratory of Trustworthy Computing, Software Engineering Institute, East China Normal University, Shanghai 200062, China

[7] Alan H. Harbitter, and Daniel A. Menasce, “Performance of Public-Key-Enabled Kerberos Authentication in Large Networks”, PEC Solutions, Inc., George Mason University

[8] Praveen Gauravaram, “Security analysis of salt // password hashes”, Tata Consultancy Services Innovation Labs, Tata Consultancy Services Limited, Hyderabad, India

[9] Konrad Lorincz, David J. Malan, Thaddeus R.F. Fulford-Jones, Alan Nawoj, Antony Clavel, Victor Shnayder, Geoffrey Mainland, Steve Moulton, and Matt Welsh, “Sensor Networks for Emergency Response: Challenges and Opportunities”, Harvard University, Boston University

[10] Prashant Rewagad, and Yogita Pawar, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”, Dept of Computer Science & Engineering, G.H.Raisoni Institute of Engg and Management, Affiliated to North Maharashtra University, Jalgaon, India