International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.229-238
http://dx.doi.org/10.14257/ijsia.2016.10.7.20

Mobile Internet Tourism Information Security Research

ShanXue

Qingdao Hospitality Management Vacational And Technical College, Qingdao Shandong province, China, 266100
boshisheng55@163.com

Abstract

In the mobile Internet era, people via mobile devices for tourism information query, booking, and record information more and more, makes human tourism and communicate with each other very convenient, also make life more colorful, however, with the development of mobile Internet, the information security, especially the tourism information and information involves the privacy protection problem increasingly highlight, need to study, aiming at this problem, this paper presents a mobile Internet tourism information security algorithm, to protect the user personal travel information, so as to guarantee the safety of travel

Keywords*: Tourism information; Mobile network; Information security*

1. Introduction

With the digital technology rapid development, the various business processing of social economy, information collection and summary analysis are widely used for computer, network economy is profoundly changing the human life and economic operation mode. Online shopping and online sales are the important of the Internet as a commercial platform tool, Internet users and businesses can through the Internet platform, and to get mutual benefit, is worthy of the government and the society advocates for tourism electronic commerce network applications, due to the particularity of tourism products, make consumers to purchase travel products online with greater risk. This makes to reduce or reduce consumer's perceived risk and increase trust is key to the key to the success of tourism e-commerce effect. Visible study tourism electronic commerce risk, identify the root causes of it, analyzes its types and characteristics, and actively eliminate or avoid risk, which can help tourism e-commerce operators in the development of e-commerce platform, reduce the risk of consumers, so as to stimulate the purchase behavior has important practical significance.

Analyze the mobile Internet era from the user's point of view of information security to protect the status quo, including the user's safety behavior and safety awareness. At the same time, the paper analyzes the main leakage channels, mobile network information and the current information protection facing new difficulties and new challenges. And try to from the build to provide personal information protection mechanism of the relevant strategies and Suggestions. Theoretical sense, proposed the new concept of the mobile network personal information, and from the fundamental problems of in-depth analysis of information protection problems faced, multi-angle analysis helps to deepen the understanding of the problem. And on the protection mechanism, put forward in the information communication and the core of the balance between information protection, a breakthrough significance. Real sense, to investigate the correlation of personal information protection for users, help the objective understanding of user behavior, and the analysis of the leakage channels hope can reveal the relevant management and Internet companies to adjust sex change. Due to the mobile Internet era of personal information

ISSN: 1738-9976 IJSIA

protection problems involved with wider range of disciplines, is a frontier field of study, is at the exploration stage, so the space is very broad, can do it according to their own interest in the depth of the different point of view of thinking[1-2].

2. Related Works

2.1. Information Security is Introduced

Information security is to point to by a variety of computer, network and the key technology to guarantee in all kinds of system and network transmission, exchange and storage of confidentiality, integrity and authenticity of the information. Information security includes three layers of meaning. One is the security system, it is physical safety and security system operation.2 it is in the system of information security, namely through control of the user permissions, such as information encryption to ensure that information is not the grantee access and tampering. Three is safety management, with comprehensive measures of information resources and the safe operation of the system for effective management.

Network information security is refers to the security of network system, online information, its purpose is to explore the network information system of anti aggression, confidentiality, integrity, availability, and controllability. Network information security technology research object is mainly the network information security problems of the space, involving information confidentiality, availability, non-repudiation, authenticity and integrity and other related theory and technology, its purpose is to maintain the order of cyberspace communication, prevent the attacker to eavesdropping and tampering with information and network system, counterfeit and destruction of attack, protect the interests of the legitimate users and privacy. From a technical perspective, the technical features of the network information security is mainly manifested in the following aspects:

1) Confidentiality

Confidentiality is the network information not be leaked to unauthorized users, entity or process, or for their use features. That prevent information leaked to unauthorized individuals or entities, characteristics of the information only for authorized users. Confidentiality is based on the reliable and usability, an important means to ensure the security of network information.

2) Availability

Availability is the network information can be used by authorized entities to access and according to the demand characteristics of the network information service when needed, allow authorized users or the entity to use features, or is partially damaged, the damage or to relegation when using network, still can provide authorized users with the characteristics of effective service. Availability is the network information system safety performance for users. Network information is the most basic function is to provide services to users, and the needs of users is random, and various, and sometimes time requirements. Usability system is commonly used in normal use the ratios measure time and the whole work time.

3) Non-repudiation

Non-repudiation also called non-repudiation. In the process of network information system of information interaction, convinced that real identity of participants, *i.e.*, all participants could not deny or denial once completed operation and commitment. Source of evidence can be used to prevent transmitting party does not deny himself send

information truthfully, submit to receive evidence can be used to prevent the receiving party later denied receiving information.

4) Reliability

Reliability is a network information system can under prescribed conditions and within the stipulated time to complete the prescribed features. Reliability is one of the most basic requirements of system security, is that all the network information system construction and the line of the target. Reliability is mainly embodied in the hardware reliability, software reliability, reliability, environmental, *etc*. Hardware reliability is the most intuitive and common. Software reliability is within the prescribed period of time, the probability that the sequence run successfully. Reliability refers to the personnel the probability of successfully completing job or task. Ring reliability refers to the regulation environment, ensure the network running the probability of success. The environment here is mainly the natural environment and electromagnetic environment.

5) Integrity

Integrity is one of the characteristics of network information without authorization cannot change, the network information in the process of storage or transfer remaining is not accidentally or deliberately to delete, modify, forgery, out-of-order and replay, insert damage loss characteristics. Integrity is a kind of facing the security of information, it requires to keep the information of the same, that is the correct new interest generated, correct storage and transmission.

For the realization of the network information security, must from the laws, regulations and policies, management and technology on three levels to take effective measures, the three phase full accord, no single level of security measures is likely to provide a comprehensive range of protection. First of all, from the laws, regulations and policies, state and industry departments must formulate strict laws and regulations. Due to the computer network is a new thing, can't can depend on many of its behavior, lead to the network computer crime in a state of disorder. In front of the computer crime has become increasingly serious, it is necessary to establish the corresponding laws and regulations, and can give to deter illegal molecules. Secondly, from the safety management, each unit shall establish corresponding network security management methods, to strengthen internal management, pay attention to the training of relevant personnel, improve the overall safety consciousness. Finally, technically, to prevent the customer information in the process of network transmission intercepted and tamper with the information. To ensure information security, an important task is to design a computer system. Need a variety of methods to ensure information security, information encryption technology is an important part of the protection of information security, realize the core of the network information security technology[3-6].

2.2. An overview of Cryptography

Key cryptography is the study of communication security discipline, which include two branches: cryptography and cryptanalysis. Password code transformation mainly studies the information, to protect information in the process of transfer from the adversary stealing, interpretation and use of the method of cryptography and cryptanalysis, and on the contrary, it mainly studies how to analyze and decode. Between the two is both contradictory and promote each other. The password technology can encrypt confidential information, not the grantee to extract information. No message called plaintext, the encrypted message called ciphertext. From plaintext cipher encryption process is called, and its inverse process, namely the ciphertext to restore the original plaintext called decryption, the receiver trying to illegally from expressly referred to as the process of

deciphering of the cipher text analysis. Part to cryptographic operations staff called plaintext encrypted or password. On the plaintext encrypted password member of a set of rules called the encryption algorithm, adopted at the time of the cipher decryption, a set of rules called decryption algorithm. Encryption algorithm and decryption algorithm is in a group only by legitimate users know the secret information, called under the control of the key, used in the process of encryption and decryption key points as the encryption and decryption keys. Conventional password information system is shown in Figure 1:

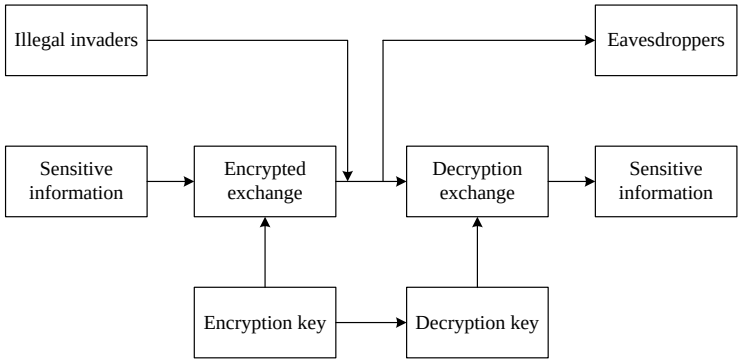

Figure 1. Conventional Password Information System

Network information encryption is to transmit the information encrypting processing first, will be the information encoded in is not easy to be intruder read or understand form to protect the security of information, and then to the network, even if the information was cut, intercept is also hard to get useful information from the encrypted garbled, but it can be authorized to obtain information on the resulting content reduction and get the information. With the development of information and information technology of modern cryptography, not only be used to solve the confidentiality of information, but also used to solve the information integrity, availability, and controllability. Can say, the password is the most effective means of solving the information security, password technology is the core of solving the information security technology, it is widely used in to protect confidential data encryption, identity authentication, message authentication, digital.

There are many ways to the classification of the cryptosystem and each are not identical.If based on the key, can be divided into symmetric key cryptosystem and public key cryptosystem. Symmetric key cipher system at the same encryption key and decryption key, the key to the safety of key channel by the information sender to the receiver, public key cryptosystem, decryption USES two different keys.

Password analysis, is the decipher technology research. Encryption and decode is a pair of contradictions, is in full accord, understand to decipher encryption is very necessary for research. Analyzed the ciphertext only to intercept and any tampering with the system, this kind of attack methods called passive attack. Another type of attack is counterpart of attack, in this kind of attack, the attacker active jamming system, delete, change, add, replay, forge method to give false information to the system. Passive attack is very difficult to detect, because it does not cause any change in data, to deal with the key is to prevent the passive attack rather than testing; Completely prevent the attack, in turn, is very difficult, can only achieve detecting active attack, and any damage or delay resulting from the attack to be restored. Password attack methods of exhaustive method and analysis method.

Exhaustive method of JieShou ciphertext, in turn, with all kinds of key test for the solvability of the translation, until they get the sense of clear; Or under the same key, plaintext encrypted to all possible until get consistent with intercept ciphertext. As long as there is plenty of computing time and storage capacity, in principle, exhaustive method

can always succeed. But in practice, no one can guarantee safety requirements of practical password will be designed to make this approach is not feasible in practice, such as high cost or time is too long to transfer more than validity.

Decoding method including deterministic crack and statistical analysis to decipher. Uncertainty analysis method using one or several known quantity expressed in mathematical relation between the prayer unknown variables. Known quantity and unknown quantity relationship depends on the encryption and decryption algorithm, for this kind of relationship is the key step in the deterministic analysis. Statistical analysis method is the use of known statistical regularity of plaintext method for decoding. Code interpreter of JieShou ciphertext statistical regularity of statistical analysis, summed up the meantime, compared with comparing the statistical rule of plaintext, and extract the correspondence between the plaintext and ciphertext or change information. Code analysis is likely to be successful, the most fundamental reason is the redundancy in plaintext. Commonly used password attack has four types: 1) the ciphertext only attack.Password analysts from only know intercepted ciphertext is analyzed, concluded expressly or key.2) known plaintext attack. Password analysis not only can capture cipher text, and can get some known plaintext and ciphertext pairs.3) choose plaintext attack. Interpreters can use any clear he has chosen, are under the same unknown key encryption cipher. That is to say, the interpreter can select any clear a ciphertext attacks on to, to determine the unknown key.4) chosen-ciphertext attack. Password analysts can choose different encrypted cryptograph, and can get the corresponding decryption expressly[7-8].

The sequential increasing strength of the above four types of attacks, ciphertext only attack is one of the weakest. Public key cryptosystems chosen-ciphertext attack is mainly used for analysis. A good password algorithm must be able to withstand choose plaintext attack, on the contrary, the minimum requirements for cryptographic algorithm is able to resist ciphertext only attack.

3. Encryption Security Algorithms

3.1. AES Encryption Algorithm

Current encryption standard is a data encryption standard DES, DES grouping is a symmetric encryption algorithm, with the length of the key pair of the 56 to 64 for the grouping of data encryption. It as the national institute of standards and technology data encryption algorithm, to become the world within the scope of the standard password. During this time it has become the most widely used in the existing password algorithm, the most trusted, research the best algorithm. But as the speed of the computer, 56 of DES encryption algorithm cannot meet the needs of security. So the 3 des algorithm, although to a certain extent, increased security, but did not fundamentally solve the problem of safety in weak key. The rapid development of computer network engineering application technology, puts forward higher requirements on the security of encryption algorithm, in this case, it needs a new encryption standard.1) security: stable mathematical basis, no algorithm weaknesses, password analysis of strength, the algorithm of the output random;2) performance: it must be on multiple platforms to faster implementation;3) size: can't take up a large amount of storage space;4) implementation characteristics: flexibility, adaptability, simplicity of the algorithm of hardware and software, *etc*.

Rijndael block cipher is an iteration, the packet length and key length is variable, only in order to meet the requirements of AES - qualified processing packet size of 128, and length of key is 125, 192, 192, the corresponding iterative round number N;For 10, 12, 14 rounds. For the sake of simplicity, here is 128 introduced with the key length, first gives a brief overview of the algorithm, and then describe in detail each part of the algorithm.

Algorithm is composed of 10 rounds cycle, each round loop has a key, it comes from

the initial key. There is a cycle 0 keys, it is the initial key. Each round loop input is 128, the output is 128.Each round loop is used to replace the whole data packet and confusion in parallel processing, mainly include column transformation, line shift change. This structure is composed of four different stages, including three instead and a confusion:

1) bytes instead of, this is a nonlinear layer, use a were grouped in bytes instead of in the S box, the purpose is to prevent differential and linear cryptosystem attack;

2) line shift, is a simple linear combination of displacement, can lead to several rounds of circulation between individual bits diffusion;

3) column confusion, a use of arithmetic characteristics instead of on the domain, is the same with the purpose of the row transform;

4) keys, using the current group and the expansion of key part of the bitwise exclusive or, that cycle key with upper results are exclusive or operation.

AES algorithm can converge the high security, high performance, high efficiency, easy to use and flexible, *etc*. It is an iterative block cipher algorithm, the packet length and key length is variable. When carries on the exhaustive key attack, exhaustive key expectations of attempts is associated with the length of key, AES algorithm to eliminate the weak key in the DES algorithm and a weak key, in its encryption algorithm, the selection of key without any limitation. Still have not found the obvious disadvantages of AES algorithm, also found no obvious security holes, algorithm has a good safety factor. After verification, AES algorithm can effectively resist any currently known algorithm. AES can be in, including 8 and 64 - bit platform, all kinds of encryption and decryption on the platform and DSP[9-10].

Round transformation of AES algorithm and the S box is completely parallel, it is the inherent high parallelism to facilitate the effective use of CPU resources, even if not to implement this algorithm in the parallel way, its software performance is very good also, the key to establish quickly. In addition, low demand of RAM and ROM of AES, very suitable for limited space environment alone encrypt or decrypt. Can be seen from the above discussion of AES algorithm function calculation simple and quick, with a simple implementation, fast encryption speed, reliable and safe, as well as good anti aggression, is a kind of ideal encryption algorithm. As this century encryption standard, will be widely used.

3.2. RSA Encryption Algorithm

RSA is a kind of public-key cipher algorithm, is a kind of the use of number theory construction, and so far in theory is the most mature and perfect public key cryptosystem, more and more widely accepted by people, it is also currently the only widely used in the world of public key cryptosystem. RSA algorithm is based on seeking two large prime Numbers is simpler, and will take them integral to solve extremely difficult this principle design. The algorithm has withstood the in-depth analysis of the password for many years, although the password analysts can neither prove nor deny the security of RSA, but this just shows that the algorithm has a certain credibility. RSA in many parts of the world has become the DE facto standard, in public-key cipher algorithm has been put forward which is the most easy to understand and implement.

Encrypted in the process of the application of various network security, random Numbers play an important role. Many study of network security based on password coding algorithm using random Numbers, for example in mutual identification scheme, the generation of session key, the key in the RSA algorithm have also want to use a random number. The real random number sequence must meet the following requirements:

1) The Degree of Random

Random degree, refers to the usually produces a series of claims to be a random value, we are concerned about a series of values in a statistical sense is random. Whether a column value is random usually use the following two criteria to verify:(l) uniform distribution: this series of numerical distribution should be uniform, that is to say, the frequencies of each number are equal;(2) independence: any of a number of series can't from several other speculation. Although in a series of numerical has clear to obey a certain distribution test method, but there was no test method can prove that independence. On the other hand, there are many test method can be used to prove that a sequence has no independence. The general strategy is a series of tests, until we trust in the independence of sex is strong enough.

2) The Degree of Unpredictable

The so-called unpredictable, is the requirement of sequence each subsequent number is unpredictable. For really random sequence, each number with other number are statistically independent, therefore is unpredictable. However, we rarely use the real random number. On the contrary, the seemingly random numerical sequence is generated by an algorithm. In this case, it is necessary to ensure that an attacker from the sequence elements cannot predict the future in front of elements.

3) Cannot be Reproduced

Cannot be reproduced refers to as far as possible if you use the same input completely eliminate interference effects of sequence generator for two times, you will receive two random sequence. The real source of random Numbers are hard to get. Physical noise generator as a possible source, but these devices cannot be used in network security applications. Published in another way is to find high quality random Numbers, however, the number of these random number cannot satisfy a considerable size of the need of network security applications. In addition, although such number do have statistical randomness, they are predictable, cannot meet the requirements in terms of unpredictability.

Password encoding technology commonly used algorithm to generate the random Numbers, these algorithms are deterministic, so the numerical sequence statistics is not random. However, if the algorithm is very good, the sequence of reasonable can lead to too many random test, these Numbers are often referred to as the pseudo random number. So to be able to use a good although pseudo random number generator has been very good, but still need to make the actual sequence is to produce, so that part of the attacker even if they know the sequence is not enough to determine the sequence of elements in the future.

The implementation of RSA algorithm needs to perform a large number of large integer multiplication and division, this leads to the efficiency of RSA algorithm implementation is very low. Speed difference is only in most of the actual system use RSA to encrypt a small amount of information, and a large number of message encryption is still one of the reasons for using other encryption algorithm to encrypt. To sum up, although addition, RSA algorithm decryption speed is slow, but it is by far the most perfect, has experienced all sorts of attack test public-key cipher algorithm[11].

4. Encryption Security System Implementation Algorithm

4.1. Encryption Technology Design

As described earlier, the public key cryptosystem, decryption algorithm running speed is very slow, and symmetric key cryptosystem key distribution, storage, security is a

thorny issue. Therefore, the public key cryptosystem and symmetric key cryptosystem combined composition more secure encryption system, for many in the field of encryption methods. Process description as follows: using symmetric key cipher algorithm using the session key to encrypt a longer message content, using public key cipher algorithm to encrypt the short session key. The design of this system is based on this idea, symmetric key cipher algorithm choose AES algorithm, public key cipher algorithm RSA algorithm. The network information encryption transmission process as shown in Figure 2:

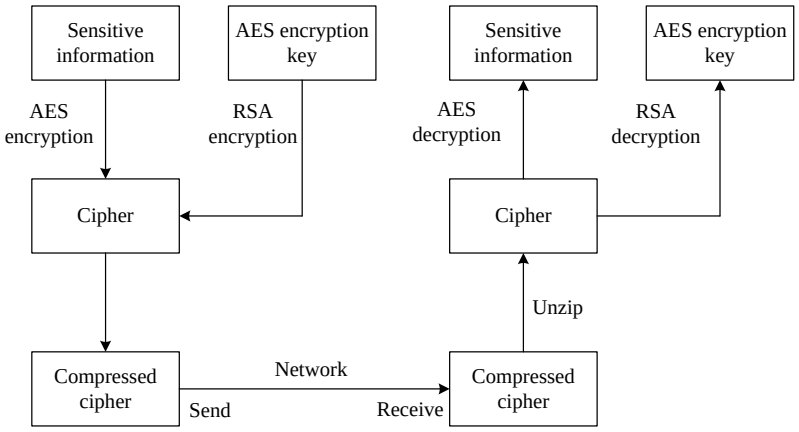

Figure 2. The Network Information Encryption Transmission Figure

In order to overcome the AES session key, because the user manual input tend to input their own information, to produce safe hidden trouble, so the generation of AES session key adopted the method that can automatically generated by the system. Before the information encryption, the user can on the length of the key to choose between 128, 192, 256, this system according to a 128 - bit key length is encrypted. The encryption process is shown in Figure 3:

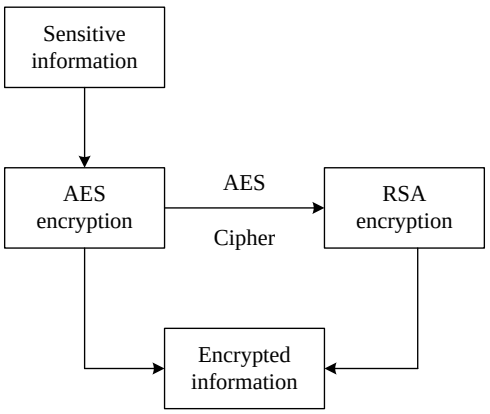

Figure 3. Data Center System Information Encryption Process

Information sender need from RSA public key management center to obtain the transmitter of RSA public key RSA encryption.The encryption is performed for the following steps:

1) produce AES session key;

2) sensitive information before transmission network, the use of AES algorithm using the session key to encrypt sensitive information. First to find to encrypt information, and

determine the location, and then select the AES session key to choose a 128 - bit key length, finally click the AES encryption information button to perform the AES encryption;

3) the information after executing the AES encryption, can to perform RSA encryption AES session key. Here need to search for information in the public key management center the recipient's public key, or public key to each other by the data center storage, convenient to call at any time. Then put the information the recipient's public key and the RSA encryption key modulus, and write the original AES encryption cipher text, this completes the information encryption process[12-14].

4.2. Decryption Technology Design

Decryption process is shown in Figure 4:

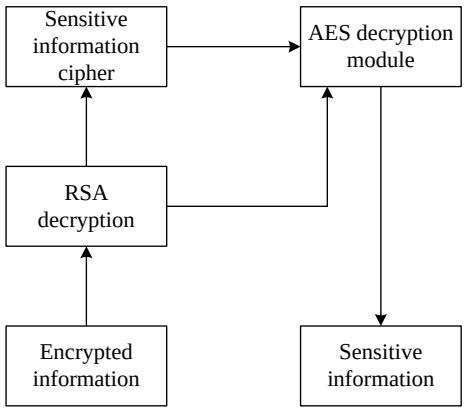

Figure 4. Data Center System Information Decryption Process

Decryption process is relatively simple, in contrast to the encryption process completely, but when performing RSA decryption must call their private key, rather than the public key[15].

1) the recipient receives the encryption of sensitive information, need to get the AES session key to decrypt the first. System first received the contents of the search, find AES standard a session key position, the AES session key cipher text, read and write memory deleted from the ciphertext AES session key cipher and flags, contain sensitive information cipher text in the receive information;

2) read the encrypted AES session key from memory, call the RSA decryption algorithm, with its own private key to decrypt get AES session key;

3) call the AES algorithm decryption cipher text proclaimed in writing by the sensitive information.

5. Conclusion

Through the analysis of a variety of encryption algorithm, the system USES the symmetrical encryption algorithm for AES algorithm, public key cipher algorithm for the RSA algorithm. System to produce the AES session key, then calls the AES encryption algorithm to encrypt information grouping encryption, then use RSA encryption algorithm encryption AES session key, and to write the encrypted AES session key into the original cipher text so that all the encrypted information integration for an organic whole,

complete information encryption. By trial and error, the system can be on any to transmit information is encrypted and network transmission, protect individual users travel information, so as to guarantee the safety of travel.

References

[1] Krister S., Hakan P. and John D., "System and Method for Providing Voice Service in a Multimedia Mobile Network: US", AU2013216641(A1)[P]. **(2013)**.
[2] Moon B. G. and Thubert P., "Arrangement for autonomous mobile network nodes to organize a wireless mobile network based on detected physical and logical changes: US", US8527457[P]. **(2013)**.
[3] Sabella D., Rost P. and Sheng Y., "RAN as a service: Challenges of designing a flexible RAN architecture in a cloud-based heterogeneous mobile network[C]",// Future Network and Mobile Summit (FutureNetworkSummit), 2013. IEEE, **(2013)**, pp. 1-8.
[4] Backholm A., Salorinne S. and Ylinen H., "Database synchronization via a mobile network: US", US 8620858 B2[P]. **(2013)**.
[5] Abdelrahman O. H., Gelenbe E. and Görbil G., "Mobile Network Anomaly Detection and Mitigation: The NEMESYS Approach[M]", // Information Sciences and Systems 2013. Springer International Publishing, **(2013)**, pp. 429-438.
[6] Hirano J., Aso K. and Lim C. K. B., "Mobile network managing apparatus and mobile information managing apparatus for controlling access requests: CN", US 8539554 B2[P]. **(2013)**.
[7] Schreiber M., "Determining configuration parameters of a mobile network: US", US 8612654 B2[P]. **(2013)**.
[8] Anthony Jr., Bruce O., Billau, Ronald L., Cillis, Canio, "Mobile network services in a mobile data network: US", US8837318 B2[P], **(2015)**.
[9] Maloney M. P., Suit J. M. and C. J. Scott, "Information security analysis system: WO", US7047423[P]. **(2006)**.
[10] A. Da Veiga PhD and J. H. P. Eloff PhD, "An Information Security Governance Framework.[J]", Information Systems Management, vol. 24, no. 4, **(2007)**, pp. 361-372.
[11] Siponen M. and Willison R., "Information security management standards: Problems and solutions[J]", Information & Management, vol. 46, no. 5, **(2009)**, pp. 267–270.
[12] Siponen M. and Willison R., "Information security management standards: Problems and solutions[J]", Information & Management, vol. 46, no. 5, **(2009)**, pp. 267–270.
[13] Eloff J. H. P. and Eloff M. M., "Information security architecture[J]", Computer Fraud & Security, 2005, no. 11, **(2005)**, pp. 10-16.
[14] Finne T., "A conceptual framework for information security management[J]", Computers & Security, vol. 17, no. 4, **(1998)**, pp. 303-307.
[15] Anderson E. E. and Choobineh J., "Enterprise information security strategies[J]", Computers & Security, vol. 27, no. 1-2, **(2008)**, pp. 22-29.

Author

Shan Xue, received Ph.D. from Ocean University of China in Agricultural Economic Management.

His research interests lie at leisure Agriculture and Rural Tourism. He is currently researching on Tourism Information System, focussing on Tourism Information Security System in Qingdao Vocational and Technical College of Hotel Management.

