Approach of Easy and Strong Security Service on Smart-Phone

Jin-Mook Kim[1], Hwa-Young Jeong[2], Bong-Hwa Hong[3]

[1]Division of Information Technology Education, Sunmoon University, Asan-si,
336708, Korea
[2]Humanitas College, Kyunghee University, Seoul, 130701, Korea
[3]Dept. of Information and Communication, Kyunghee Cyber University. Hoegi-dong, Seoul,
130701, Korea

calf0425@sunmoon.ac.kr, hyjeong@khu.ac.kr, bhhong@khcu.ac.kr

Abstract. People become very convenient that has Smart-phone in one's around. And use of smart-phone is very increasing at recent. PC and Internet was main computing environment in existing but devices such as smart-phone. But, serious security problem will happen because anyone is not providing security service for smart device. Perhaps the most dangerous problems for the user identification and smart-phone service provider for the service in the connection between the authentications are still a problem. So, we wish to propose system that offers confidentiality, integrity service in smart device using AES-256 and MD-5. And after pass through certification process about device and user, wish to propose system that apply PEKS technology so that can simplify certification formality about service. Our proposed system can offer various security services that confidentiality and integrity. And it support certification service easily and conveniently to smart-phone.

Keywords: Smart-phone, PKES, Authentication, Security Services, Confidentiality, Integrity

1 Introduction

Recently, the domestic Smart-phone user is increasing sharply to 20 million. Users can handle satisfied works ubiquitously and conveniently using various smart-phone or tablet devices against of existing PC. For example, user can access web surfing or user-demanded services in cloud service environments. But, smart-phone or tablet unit that can offer convenience and strong mobility to users is indifferent about security problems. If follow to reference [1, 2, 4, 6], smart devices can offer to service of speech or data communication using Wi-Fi or Blue-tooth and wireless protocol.

[1] Jin-Mook Kim is First Author

[3] Bong-Hwa Hong is Corresspond Author

However, there don't prepare to preventive measures for much security threat element that is happening often.

As explain in reference paper [5, 6], we will expect security threats increasing because user want more smart device services. So, more security threats appear to us in cloud environments. Specially, reference paper [2] explain that android operating system based smart device be easy to make out or deliver malicious code. And in paper [4] is predicting that average 500,000 suddenness budgets are consumed in one year for solve problems on expected security to happen in smart devices.

Corporation's business environment is changed to easy and rapidly by using smart devices. But security specialists expect to very serious security problems are happen in cloud service environment because business framework provide easy and efficiency work conditions to user. Specially, serious problem is predicted to happen at access process for cloud service utilization by using smart device.

Therefore, we wish to confidentiality service providing system that adding light encryption process among data transmit when user want to use cloud service by smart-phone in this paper. And we propose system (AESSUHEA) that can improve efficiency to provide confidentiality service applying PEKS to prevent delay by using existent PC based encryption algorithm - AES-256 and MD-5. We will expect to solve problem about secret key open while information search process, man-in-the-middle attack and AESSUHEA can support to confidentiality services to user in smart-phone as well as easy and efficiency.

2 Related Works

2.1 Security threats on smart-phone

Demand of present smart device is increasing very rapidly. Smart-phone user is reaching in 20 million in domestic at 2011. Smart-phone can offer mobility and convenience to user but we don't have smart device security problem solving method at now. So, we can expect four security threats in smart devices as following:

1) Device forgery or variation
2) User individual information masquerade
3) Steal of communication data
4) Data masquerade

In addition, we described in front 4 main security threats but more threats exist. Evil purpose have user can distribute malignancy code or denial of service attack against of right cloud service.In some cases, it is the Contact Volume Editor that checks all the pdfs. In such cases, the authors are not involved in the checking phase.

2.2 Public-key Encryption Keyword Search schemes

Passing the late 1970s, PEKS proposed by Rivest, Shamir and Adleman to offer data confidentiality check and guarantee against of difficult environment that support security service about confidentiality by using encrypt algorithm directly [7]. Reference paper [11] proposed Homomorphic encryption algorithm that is possible to approach on PC and communication environment of internet. And reference paper [8, 9, 10, 12, 13] explain and develop application may be possible in latest communication environment. This can offer convenience to confirm confidentiality services compare with traditional encryption algorithm.

2.3 Authentication Services

Kerberos algorithm started from a variety of authentication techniques have been developed by many computer security engineers. The user authentication scheme to ensure identification of the proposed technique that proposed for using computers and Internet in the environment. In recent years, a variety of methods based on PKI is used mainly.

But this paper is based on the environment of Smart-phone. Therefore, a conventional PKI- based authentication technology is difficult to accept for many. So, We suggest of authentication method that based on a quick and easy PEKS to perform user authentication to the plans.

3 Proposal Schemes

3.1 Structures of Proposal System

We design structure of Proposal system that we will call AESSUHEA. It can offer confidentiality and integrity service using AES-256 and MD-5 algorithm. Figure show about it. As appear to figure 1, AESSUHEA that propose has 3 components. First, communication module exists in first layer. We design to call and appropriate library of communication device of general smart devices.

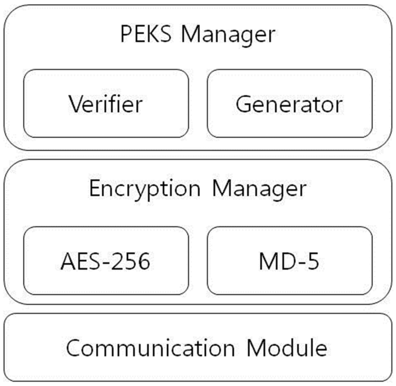

Fig. 1. Structure of AESSUHEA

Our proposed system (AESSUHEA) has three major components. The first component of the proposed system to easily retrieve information from the user to verify the verifier for the user to generate a token for authentication to a constructor has a PEKS manager. The second component has two components. To enable encrypted communications between users to provide confidentiality services. It is a Encryption Manager. That was composed of modules consisting of AES-256 encryption module and to guarantee the integrity of the MD-5 module. The third element is usually smart-phone hardware to provide telecommunications services between communication devices. It has a many communication module.

As above, a general manager to offer two kinds of communication structures mounted on top by confidentiality and integrity of communications services to provide powerful, as well as the process of providing these security services for internal users easily without direct involvement were able to handle.

3.2 Procedures of Proposal System

AESSUHEA designed for smart device communication between other devices via formality of 6 steps. Figure 2 show about it. The formality is as following:

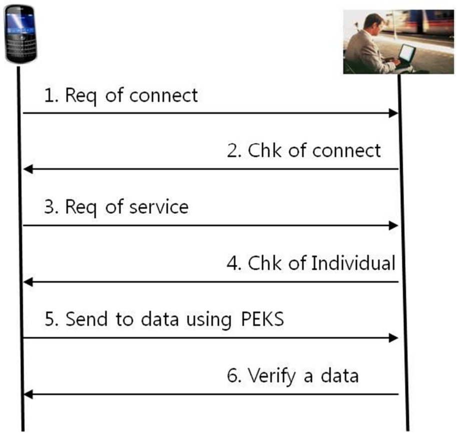

Fig. 2. Procedure of AESSUHEA

1) Request of connect: smart device sends together random information that use device discernment number and present sight through communication module to other device.
2) Check of connect: Transmit response number about device discernment number and own discernment information that other person sends to other person by confirmation process about communication request.
3) Request of service: After finish device discernment, request cloud service.
4) Check of Individual: Confirm user discernment information and information that receive at device discernment process to confirm about user required service.
5) Send to data using PEKS: Sender transmits together simplification information for verification about information that wishes to transmit using PEKS Manager after encipher information that wish to transmit using Encryption Manager.
6) Verify a data: Information that listener receives whether assurance about security service is available using PEKS Manager inspect.

Certification that detail with upside is available as well as discernment and certification for smart device through 6 formality and with discernment about service. And fast and uncomplicated processing is thought to be possible by using PEKS way without verifying all about transmission of a message or data that receive between smart devices.

4 Analysis of our proposal system

We know that AESSUHEA can fast and easy access compare wtih existent PC based encryption algorithm when consider structure and procedure. So, we show that our proposed AESSUHEA can support process speed about more ten times and provide security service against of existent RSA encryption algorithm.

Table 1. Analysis of our proposed system

	IOS based device	Android based device	Proposal
Confidentiality	AES-256	None	AES-256
Integrity	None	None	MD5
MITB	None	None	Possible
Speed	Slow	None	Fast
Complexity	Complex	None	Easy

As appear in table 1, existent Android based smart devices are no preventive measure for security threats. Individual development to provide suitable security service to own device in the company such as present Blackberry is progressing. Similarly, IOS based smart devices are applying AES-256 that is password algorithm of open height base but the processing speed is slow and smart-phone or tablet unit has very complicated output to apply and the efficiency is low.

However, we apply PEKS techniques for web service and using AES-256 and MD-5. And we designed so that the processing speed and calculation complexity may be low. And we designed our proposed system can provide device integrity service for smart device applying MD-5. AESSUHEA is possible confrontation to meson attack by second.

AESSUHEA runs authentication for smart device before use cloud service to Site-Based, and apply PEKS and run authentication about service itself. Therefore, is expected to keep away being killed by meson attack that occurrence is possible.

5 Conclusion

Smart-phone makes user's business environment very conveniently in cloud service environment by mobility. But it is difficult to provide security service for smart device. Smart device have low-speed, low-save capacity and user complaint about delay. So, user doesn't support strong security services.

But, Smart-phone using recommend is increasing very rapidly and malicious code or security attack is increasing. So, user's damage becomes serious gradually in smart device. we proposed to apply AES-256 and MD-5 algorithm and PEKS technique for resolving about this problems.

We propose AESSUHEA that could correspond in safety and integrity, man-in-the-middle attack running device authentication for smart device and authentication about service beforehand and examined about this. Additional research may be gone to act fast and easily applying PEKS techniques.

References

1. Byron Acohido, "New Security Flaws Detected in Mobile Devices", http://www.mobile-tech-today.com/story.xhtml?story_id=022001KSER0E&nl=8.
2. Eric Lundquist, "Security in the Borderless Enterprise", http://www.informationweek.com/news/global-cio/interviews/232601452
3. Stuart Sumner, "New Android malware can remotely control phone", http://www.computing.co.uk/ctg/news/2166409/android-malware-remotely-control-phone
4. Gareth Morgan, "Mobile security incidents costing firms nearly $500,000 a year", http://www.v3.co.uk/v3-uk/news/2154670/mobile-security-incidents-costing-firms-nearly-usd500?wt.mc_ev=click, 2012.2.23.
5. Molly Bernhart Walker, "NIST Security controls update addresses privacy, mobile, cloud", http://www.fiercegovernmentit.com/story/nist-security-controls-update-addresses-privacy-mobile-cloud/2012-02-29?utm_medium=nl&utm_source=internal, 2012.02.29.
6. George V. Hulme, "Mobile security threats are heating up: criminals, security researchers, vendors and even investors are now taking mobile security more seriously", http://www.csoonline.com/article/691043/mobile-security-threats-are-heating-up?source=CSONLE_nlt_update_2011-10-06, 2011.10.05.
7. Rivest, Adleman, Dertouzos, "On data bank and privacy homomorphisms", Proceedings of the 19th Annual Symposium on Foundations of Secure Computation-FSC, pp. 169-180, 1978.
8. J. Domingo-Ferrer, "A New privacy homomorphism and applications", Information Proceeding Letters, Vol. 60, No. 5, pp. 277-282, 1996.
9. Craig Gentry, "Fully Homomorphic encryption using ideal lattices", In proceedings of the 41st ACM Symposium on Theory of Computing – STOC, pp. 169-178, 2009.
10. Pascal Paillier, "Public-key cryptiosystems based on composite degree residuosity classes", Advanced in Cryptology-Eurocrypt(LNCS1592), pp. 223-238, 1999.
11. Dan Boneh, Giovanni Di Crescenzo, "Public Key Encryption with keyword Search",
12. Dawn Xiaodong Song, David Wagner, Adrian Perrig, "Practical Techniques for Searches on Encrypted Data",
13. Yong Ho Hwang, Pil Joon Lee, "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", LNCS4575, pp. 2-22, 2007.