Research Journal of Applied Sciences, Engineering and Technology 7(12): 2583-2588, 2014
DOI:10.19026/rjaset.7.571
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 31, 2013 Accepted: September 10, 2013 Published: March 29, 2014

Research Article

Secure Architecture for m-Health Communications Using Multi-agent Approach

Mohd Fadhli Abdul Jalil and Rossilawati Sulaiman
Faculty of Information Science and Technologi, School of Computer Science,
National Universiti of Malaysia, 43600, Bangi, Selangor, Malaysia

Abstract: In this study we propose a security architecture for mobile Health (mHealth) communications. mHealth is a term used for medical-related services or communication, delivered using mobile devices such as mobile phones, tablet computers and PDAs. Communication in the health-related field often involve sensitive information (e.g., an email about a patient's illness is sent between doctors), which is transmitted over the Internet. However, although the Internet greatly facilitates the communication, it is undeniable that the threats to the Internet are becoming more prevalent. A multi-agent security architecture is presented in this study to provide a secure environment for mHealth communication. Agents are skilled in order to handle the communication processes at both sender's and recipient's side. This includes the security processes, which make use of cryptography protocols to secure data at both sides.

Keywords: Cryptography protocols, m-health, multi-agent system, security

INTRODUCTION

Smartphone features have already been introduced to the world since 1993 by IBM Simon (Steve, 2011). The term Smartphone was first applied to Ericsson concept phone GS88in 1997 (Steve, 2011). From the continuous evolution of the Smartphone across decades, we can see how Smartphone have been playing important role in information exchanges. Nowadays, making calls is not the most used function anymore. Everything goes mobile from checking and replying emails to reading news and socializing. However, with the rapid growth of mobile technologies, the threats to the technologies also come in equal. Mobile devices are becoming daily needs not only to typical consumers, but also needed in other domains or sectors such as military, healthcare, business and education (Joseph and Jennifer, 2012; Pedro, 2012; Kosie, 2011). As mobile devices gain the popularity, they also lure attackers, which are targeting this platform.

Every domain has its own type of sensitive data to be exchanged during a communication session. In the healthcare domain for example, sensitive data such as clinical data and healthcare information need to be secured to avoid exploitation by the wrong hand (Ganthan *et al*., 2010). Even if we feel that the data is safe, the attackers out there will seek forever possible chance to get the information. All kind of actions that breach the availability, confidentiality and integrity of the sensitive information, will be classified as threats. If a threat occurs in the healthcare communication, it will involve the risk of individual's life. That is why we need a secure architecture for mobile devices to secure the sensitive data from threats. The next section discusses about threats on mobile phones.

Mobile threats: While the possibility of mobile devices being exposed to threats increases, nothing can hold these devices from becoming the fastest growing consumer technology. There are various threats that affect mobile devices. We categorize these threats into several categories such as application-based threats, web-based threats, network-based threat and physical-based threats.

Application-based threats occur from applications that have been downloaded or installed in mobile devices. An application can be specifically designed as malicious or exploited for malicious purposes. Malware, Spyware, Privacy Threats and Vulnerable Applications (Lookout Mobile Security Blog, 2011) are examples of the application-based threat.

Web-based threats occur when mobile devices connected to the Internet are using web-based services. These threats have been historically known problem for PC users since long ago before its affect mobile platform. It can be split into three categories: Phishing Scams (David, 2013), Drive-By Downloads (Meridith, 2012) and Browser Exploits (Yu *et al*., 2008).

Network-based threats affect mobile devices which support cellular networks and local wireless network. These two network features are built-in in every Smartphones. Two types of network threats are known as Network Exploits and Wi-Fi Sniffing (Lookout Mobile Security Blog, 2011).

Corresponding Author: Mohd Fadhli Abdul Jalil, Faculty of Information Science and Technologi, School of Computer Science, National Universiti of Malaysia, 43600, Bangi, Selangor, Malaysia

For physical threats, since mobile device are portable and designed for daily use, its physical security is also important. Mobile devices are also exposed to theft where it often happens because of user carelessness.

The commonly used security protection for mobile device that uses wireless LAN are user authentication and encrypted wireless network such as Wi Fi Protected Access (WPA) (Ahmad, 2003; Bowman, 2003; Johari, 2009). In addition SSL is also used on wireless devices to provide transport level security (Gupta and Gupta, 2001; Marti *et al*., 2004).

E-health: According to the definition of e-health by Eysenbach (2001), e-health is an emerging field in the intersection of medical informatics, public health and business, referring to "..health services and information delivered or enhanced through the Internet and related technologies..". In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude and a commitment for networked, global thinking, to improve health care locally, regionally and worldwide by using information and communication technology. E-health can include a range of services or systems like Electronic Health Record, Telemedicine, Consumer Health Informatics, Health Knowledge Management, Virtual Healthcare Teams, m-Health, Medical Research Using Grids and Healthcare Information Systems.

m-health: Healthcare services that are supported by mobile devices are called mobile health or m-Health. The term m-Health refers to services that use mobile devices such as mobile phones, tablet computers and PDA to deliver health services and information. m-Health applications include the use of mobile devices in collecting community and clinical data, delivery of healthcare information to practitioners, researchers and patients, real-time monitoring of patient vital signs and direct provision of care (via mobile telemedicine) (Germanakos *et al*., 2005).

Interest in applying Multi-Agent System (MAS) in healthcare has been shown in Antonio (2010), Mayuri *et al*. (2011) and Sulaiman *et al*. (2009). The motivation of using MAS is based on the four factors. First, MAS is inherently distributed. Second, agents can coordinate their activities while keeping their autonomy and local data. Third, MAS is known as a dynamic and flexible distributed problem solving mechanisms and fourth, MAS can be used for personalization techniques (Antonio, 2010).

MATERIALS AND METHODS

This section discusses about agents, which covers its definition, related terms and applications that use agents for security purposes.

Agent and Multi-Agent System (MAS): Researchers define agents in the context of their research. For example, Bradshaw (1997) defines an agent as "a software entity which functions continuously and autonomously in particular environment". Agents can be categorized as single agent systems and multi-agent systems (Weiss, 1999). Single agent system, such as an online shopping agent, is launched to search for information based on the owner's preferences. However, single agent system is unsuitable for a distributed problem domain, because it does not improve in reducing the complexity of the problem. Agents need to interact with each other in order to achieve their goals, such as portrayed in MAS.

Oliveira *et al*. (1999) defined MAS as "a collection of, possibly heterogeneous, computational entities, having their own problem solving capabilities and which are able to interact among them in order to reach an overall goal". Each agent is skilled to do special tasks that help with the achievement of the system's overall goal. This characteristic makes the agents possible to handle problems that have multiple problem solving methods and entities (Jennings *et al*., 1998).

Agent-based modeling software can be used to develop agent-based applications. Examples of such software are ADK (Tryllian Agent Development Kit), SeSAm (Shell for Simulated Agent Systems) (fully integrated graphical simulation environment), ZEUS and JADE (Java Agent Development framework) (Nikolai and Madey, 2009). These software were known for its FIPA compliant but the only one that remains active is JADE.

MAS and FIPA: MAS has standardization that makes it easily be integrated with other systems. The Foundation for Intelligent Physical Agents (FIPA), is an organization that provides agent development standards and specifications, including agent communications and agent management (Bellifemine *et al*., 2007). The most widely adopted of the FIPA standards are the agent management and Agent Communication Language (FIPA-ACL) specifications.

MAS permits interconnection/interoperation of multiple legacy systems, that is, to integrate the existing systems with MAS, to add value to this system by utilizing the agents capabilities (Sycara, 1998). In addition, extensibility of the agent allows an agent to be instantiated with new functionalities and integrated to the existing system (Sycara, 1998; Debenham, 1999). Therefore, creating and removing agents can be performed without having to reconfigure the whole system. Examples of information systems with support from MAS can be found in Nguyen *et al*. (2008) and Zgaya and Hammadi (2006).

Agents in mobile devices: The use of MAS has become a well-accepted paradigm to support online

communication to exchange messages over the network. The agents are used to cater for the communication processes, as well as the security mechanisms applied to the message before transmitting the message to intended recipient (s). For example, the K4CareEuropean project aimed to provide a Home Care model, as well as to develop a prototype system, based on the Web technology and intelligent agents, that provided the services defined in the model (Antonio, 2010).

Other related works that were proposed were from MITCOE Pune, India (Mayuri *et al*., 2011) that used the multi-agent based mobile health, which include the combination of wireless medical sensor module with the data mining techniques. They separated the association rule into two data group that were real data sensory and historical data collected in past. These two data sources were compared to analyze patterns of patient's normal and emergency status. Their system architecture was divided into Body Area Network (where the sensor attached), Medical Server and Hospital System. Six main agents involved in this system such as Patient Monitoring Agent, Gate Agent, Supervisor Agent, Manager Agent, Doctor Agent and Decision Support System (Mayuri *et al*., 2011).

Agents to secure mobile devices: Besides the intelligence and flexibility of an agent, there is a potential for MAS to be used for securing mobile devices communication. In a research by Sulaiman *et al*. (2009), an approach called the Multilayer Communication (MLC), was used to determine the security processes, which uses cryptography protocols to secure data and communication channel in e-health. Agents are used to communicate between a mobile device (wireless) and a PC (wired), which exchanged sensitive information. Agents are skilled to perform certain tasks. At the Sender's host, agents interact with each other to secure a message to be sent to the Recipient, including encryption, digital signature and hash code. A mobile agent is used to carry the encrypted messages as well as the agent's code to the Recipient's host. MLC approach also provides mechanisms to verify the authenticity, confidentiality and the integrity of the code and data that arrived at the Recipient's host. The message and the code are authenticated; the code is executed to perform tasks to recover the plaintext (Sulaiman *et al*., 2009).

Other application example has been proposed by Wang *et al*. (2011) that used Self-Certified Proxy Sign cryption in protecting mobile agent. Mobile agent is an entity that is able to transport messages between nodes in a network. The self-certified is used to reduce storage space and communication overheads, computational cost and no key escrow problem. This type of protocol is suitable for mobile application because of limited storage capacities and computational resources.

As to our limited knowledge, we have not seen many researches that use MAS, to secure communication in mobile device apart from what have been discussed so far. The next section discusses our MAS security architecture to secure communications specific for mobile device communications.

RESULTS

We propose a secure MAS architecture for mobile devices communication such as depicted in Fig. 1.

Consider a scenario in the e-health domain, where a paramedic (Sender) at an accident spot needs to communicate and send information about patient (s) at the accident location with a staff (Recipient) at the hospital using smart phones. The Recipient could prepare a medical team at the hospital, while waiting for the patient to arrive. The information communicated may consist of patient's current condition, medication history such as allergy and current medication list, which is evidently very sensitive and must be protected.

Sender's side: From the figure, at the sender's side, there are Interface Agent (IA) and Security Agent (SA). First, IA takes a message composed by the user. Then, the message is sent to SA, where SA applied appropriate cryptographic protocols to the message, such as encryption, hash and digital signature (details of the protocols will be explained in the next section). After SA finished the task, the secured package is sent out to receiver.

Recipient's side: At recipient's side the only agent involved is Receiver Agent (RA). After the secure package is received, RA verifies the package whether it is from trusted sender or not. After the tasks are completed, the user at the recipient's side will get the original plaintext.

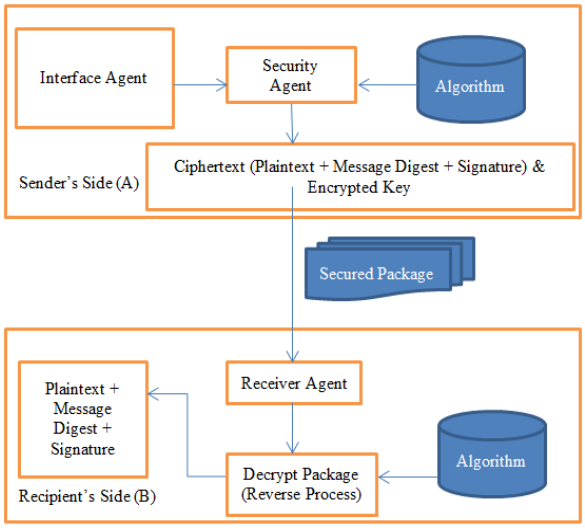

Fig. 1: Proposed architecture for sender and recipient side

Table 1: Notation and description

Notations	Description
A	Sender
B	Recipient
E	Encrypt
D	Decrypt
P	Plaintext
C	Ciphertext
S	Signature
Sig	Sign a plaintext
Ver	Verify
Hash	Hashing function
P_H	Message digest
K	Shared key
K_E	Encrypted shared key
$_{APRI}$	Sender's private key
$_{APUB}$	Sender's public key
$_{BPRI}$	Recipient's private key
$_{BPUB}$	Recipient's public key

The cryptographic protocol: We labeled the two communicating parties as "A" for sender and "B" for recipient. The following notations show the steps of proposed cryptographic protocols. Cryptographic protocols involved in this data exchange are symmetric encryption, asymmetric encryption, digital signature and hash function. Table 1 describes the notations and the corresponding description.

Sender's side (A): Every data exchange will start at the sender side or known as "A". There are five steps involved at this side. These entire five steps were handled by SA (Fig. 1). Assume that a shared key K, has been generated by A and assume that both sender and recipient has exchange their public keys.

First of all, the Plaintext (P) will go through the hash function to get a message digest (P_H). P_H is needed later for comparison at the recipient side to verify the integrity of P:

$$A: P_H = Hash \{P\} \quad (1)$$

In the second step, the plain text will be signed by the sender, to provide a signature of the Sender (S). The plaintext will be signed using the sender's private key ($_{APRI}$):

$$A: S = Sig_{APRI} \{P\} \quad (2)$$

In the third step, Cipher text (C) will be produced. P, P_H and S will be encrypted together in one package using the shared key, K. This step resembles symmetric-key encryption:

$$A: C = E_K \{P, P_H, S\} \quad (3)$$

The K, is encrypted using the recipient's public key ($_{BPUB}$):

$$A: K_E = E_{BPUB} \{K\} \quad (4)$$

In the fifth step, C and K_E will be concatenated and sent to the recipient:

$$A \rightarrow B: \{C, K_E\} \quad (5)$$

Recipient's side (B): At the recipient's side, we assume that the submitted package is successfully received by the recipient. There are also five steps involved at this side. The entire steps here are actually the reverse steps of the one at the sender side. First, the recipient received C and K_E from the sender:

$$B: \{C, K_E\}$$

The recipient needs to get K, to decrypt the C. Therefore, K_E will be decrypted by the recipient's private key ($_{BPRI}$):

$$B: K = D_{BPRI} \{K_E\} \quad (6)$$

After K is successfully retrieved from K_E, it can be used to decrypt C, to get P, P_H and S:

$$B: \{P, P_H, S\} = D_K \{C\} \quad (7)$$

Afterward, S is used to prove that the plaintext is actually coming from the sender, by verifying S against the sender's public key ($_{APUB}$). If this is successfully verified, the whole message is considered authorized:

$$B: Ver_{APUB} \{S\} \quad (8)$$

Lastly, the recipient will need to make sure that the plaintext is not modified or changed during transmission. Again, a message digest is calculated by the recipient. This new message digests is then compared with the one that comes from the sender. If both are matched, no modification or change occurs during transmission, thus, P is considered genuine:

$$B: P_H = Hash \{P\} \quad (9)$$

DISCUSSION AND RECOMMENDATIONS

Our proposed secure MAS architecture utilizes agents to cater for the security processes as well as to handle the message exchange between Sender and Recipient. IA handles the interface between the user and the system, to get the message for the user and forward it to SA. SA applies cryptography protocols to the message and handles the communication between the sender and the recipient. At the recipient's side, RA waits for any connection and communicates with SA. RA also handles the cryptography protocols to authenticate SA. Based on the results of the security procedures applied on the message, SA decides whether to accept or discard the message.

As explained in the previous section, we use encryption, hash function and digital signature to provide confidentiality, integrity, as well as authenticity respectively. This protocol provides confidentiality to both sender and recipients by encrypting all messages using a shared key, K. Sender is able to prove his/her authenticity by signing the message with $_{APRI}$ so that Recipient can later verify it with the Sender's public key. Recipient can verify the integrity of the message by calculating a new hash message and comparing the hash it with the one received from Sender, P_H.

For our future work, we will be conducting an experiment to test the implementation of our security protocols in MAS and compare our MAS with the traditional non agent-based system, which both will be implemented on mobile devices.

REFERENCES

Ahmad, Z., 2003. Wireless security in health care. Proceeding of the 1st Australian Undergraduate Students' Computing Conference.

Antonio, M., 2010. On the application of multi-agent systems in healthcare. University Rovira I Virgili, Tarragona.

Bellifemine, F.L., G. Caire and D. Greenwood, 2007. Developing Multi-agent Systems with JADE. Wiley, NY.

Bowman, B., 2003.WPA Wireless Security for Home Networks [Electronic Version]. Retrieved from: http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.mspx.

Bradshaw, J.M., 1997. An Introduction to Software Agents. In: Bradshaw, J.M. (Eds.), Software Agents. MIT Press, Cambridge, MA, pp: 3-46.

David, W., 2013. Seven Steps to Avoid Being 'Phished'. Retrieved from: http://www.smh.com.au/small-business/seven- steps-to-avoid-being- phished-20130401-2h20y.html.

Debenham, J., 1999. An Adaptive, Maintainable, Extensible Process Agent. In: Bench-Capon, T., G. Soda and A.M. Tjoa (Eds.), DEXA'99, LNCS 1677, Springer-Verlag, Berlin, Heidelberg, pp: 636-645.

Eysenbach, G., 2001. What is e-health? J. Med. Internet Res., 3(2): e20.

Ganthan, N.S., A. Rabiah and I. Zuraini, 2010. Security threats categories in healthcare information systems. Health Inform. J., 16(3): 201-209.

Germanakos, P., C. Mourlas and G. Samaras, 2005. A mobile agent approach for ubiquitous and personalized ehealth information systems. Proceedings of the Workshop on 'Personalization for e-Health' of the 10th International Conference on User Modeling (UM'05). Edinburgh, pp: 67-70.

Gupta, V. and S. Gupta, 2001. KSSL: Experiments in wireless internet security: TR-2001-103. Sun Microsystems Laboratories, Sun Microsystems Inc.

Jennings, N.R., K. Sycara and M. Wooldridge, 1998. A roadmap of agent research and development. Autonom. Agents Multi-Agent Syst., 1(1): 7-38.

Johari, J.A.Y., 2009. Securing Wireless Network. Retrieved from: http://blogs.iium.edu.my/jaiz/2009/04/17/securing-wireless-network/ [Electronic Version].

Joseph, E.M. and S.M. Jennifer, 2012. Evaluating Mobile Device Usage in the Army. Retrieved from: http://scs.org/upload/documents/conferences/autumnsim/2012/presentations/etms/7_Final_Submission.pdf.

Kosie, E., 2011. Mobile Devices in Education. Retrieved from: http://repository.up.ac.za/bitstream/handle/2263/16963/Eloff_Mobile%282011%29.pdf?sequence = 1.

Lookout Mobile Security Blog, 2011. Security Alert: Droid Dream Malware Found in Official Android Market. Retrieved from: http://blog.lookout.com/2011/03/security - alert-malware-found-in-official-android-market-droiddream/.

Marti, R., J. Delgado and X. Perramon, 2004. Network and application security in mobile e-health applications. Proceeding of the International Conference on Networking Technologies for Broadband and Mobile Network.

Mayuri, G., A. Snehal, P. Dipti and V.M. Wadhai, 2011. An intelligent architecture for multi-agent based m-health care system. Int. J. Comput. Trends Technol., 2011: 5.

Meridith, L., 2012. Mobile Malware: Beware Drive-by Downloads on Your Smartphone. Retrieved from: http://www.cio.com/article/702655/Mobile_Malware_Beware_Drive_by_Downloads_on_Your_Smartphone.

Nguyen, M.T., P. Fuhrer and J. Pasquier-Rocha, 2008. Enhancing e-health information systems with agent technology. Int. J. Telemed. Appl., Article ID 279091, 2009: 13.

Nikolai, C. and G. Madey, 2009. Tools of the trade: A survey of various agent based modeling platforms. J. Artif. Soc. Soc. Simul., 12(2): 2.

Oliveira, E.C., O. Stepankova and K. Fischer, 1999. Multi-agent systems: Which research for which application? J. Robotics Autonom. Syst., 27(1-2): 91-106.

Pedro, H., 2012. CDW Survey: Mobile Devices Boost Small Business Efficiency. Retrieved from: http://www.smallbusinesscomputing.com/News/ Mobile/cdw-survey-mobile-devices-boost-small- business-efficiency.html.

Steve, K., 2011. Here are all the Smartphone Features you Love so Much and who had them First. Retrieved from: http://www.businessinsider.com/smartphone-firsts-2011-8?op=1.

Sulaiman, R., D. Sharma, M. Wanli and D. Tran, 2009. A multi-agent security architecture. Proceeding of the 3rd International Conference on Network and System Security. Gold Coast, QLD, pp: 84-91.

Sycara, K., 1998. Multi agent systems. AI Mag., 19: 79-92.

Wang, C., Y. Han and F. Li, 2011. A secure mobile agent protocol for m-commerce using self-certified proxy signcryption. Proceeding of the 2nd International Symposium on Information Science and Engineering (ISISE). Shanghai, pp: 376-380.

Weiss, G., 1999. Multi-agent System: A Modern Approach to Distribute Artificial Intelligence. MIT Press, London, UK.

Yu, W.D., R. Gummadikayala and S. Mudumbi, 2008. A web-based wireless mobile system design of security and privacy framework for u-healthcare. Proceeding of the 10th International Conference on e-health Networking, Applications and Services (HealthCom, 2008), pp: 96-101.

Zgaya, H. and S. Hammadi, 2006. Assignment and integration of distributed transport services in agent-based architecture. Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology.