

A Flexible and Reliable Architecture for Mobile Agent Security

Ghossoon M.W. Al-Saadoon

School of Computer and Communication Engineering, University Malaysia Perlis,
Kompleks Pusat Pengajian Seberang Ramai (Blok A), No. 12 and 14,
Jalan Satu, Taman Seberang Jaya Fasa 3, P.O.S. 02000 Kuala Perlis

Abstract: Problem statement: Wireless application protocol is a protocol that makes it possible to surf the Internet from a cellular phone or other handheld wireless. Many of us that surf the Internet from home with a 56 kbps modem think that it is slow and a cell phone only uses 9.6 kbps so WAP has to take the lesser bandwidth into consideration. For this reason, this study proposed a flexible and reliable system to be implemented by using the characteristic of agents "mobile agent" through wireless application protocol for identification of distributed Intruder. The problem appears when the limitation of data transfer when the distributed systems are used (which includes the heterogeneous database) through internet. For this reason the suggested approach will be the solution to the problem of WAP for mobile agent. **Approach:** The purpose of this study was to present the ability for dispatch mobile agent from a host to carry out operations directly to the remote point of interest, thus agent's scans provide an appropriate response which is faster than a hierarchical IDS that communicates with a central coordinator based elsewhere on the network. **Results:** The methodology was used in order to understand the mobile agent mechanism and will introduce the distributed computing mechanisms that are intended for large scale distributed systems. Since the distributed security agent models system was built using mobile agent and net, this will develop small applications for data stores, like sequential query language server. The method used the algorithms built refer to each part of the structure and the rules that implemented (users and the security agent system roles). The result was simulating the intended for business roles for both commercial and government modules, which included the solution to the problem and to architecture to be more flexible and reliable. **Conclusion/Recommendations:** One of main conclusion for the mobile agent used WAP protocol: To make this protocol secure when transmit the messages in the distributed system using agents chrematistics and Interaction with security agent is multi-mode providing hassle-free access to the user. Security agent alerted the users based on their alert rules. This study had new approach and idea in implementation, also presented the ability to dispatch mobile agent from a host to carry out operations directly to the remote point of interest, thus agent's scans provide an appropriate response which is faster than a hierarchical IDS that communicates with a central coordinator based elsewhere on the network.

Key words: WAP, GPRS, security in WAP, cookies and proxy

INTRODUCTION

Agents can model a problem, involving moving real-world entities or to follow a mobile user. In many cases, mobile agents are really mobile objects.

The aim of this study to be the structure more flexible and reliable using the General Packet Radio Service

Mobile agent security: The proposed approach used the Wireless Application Protocol (WAP) which refers to a group of related technologies and protocols widely used as a de-facto standard protocol in providing Internet access to mobile phones or other thin-client devices.

This study has built the Distributed Security Agent Models System (DSAMS) using Mobile Agent that developing small applications to store data in the SQL Server to simulate the roles for the governmental and commercial modules. General Packet Radio Service (GPRS) is a packet oriented mobile data service available to users of Global System for Mobile Communications (GSM) and IS-136 mobile phones. It provides data rates from 56-114 kbit sec⁻¹.

Literature reviews:

- The client-server mechanism is widely used and adopted by many applications. The server, which resides at a centralized site in the network, provides

a number of services to its clients. Along with the services, it also provides the resources needed for executing the request and program code (describing how to perform the service). Sebastian *et al.*^[2] show that the clients who in many cases have less computational resources than the server, request the execution of a service by interacting with the server. If the client has access to that particular service, the server performs the requested service and typically returns the result to the client^[2]

- Saarinen^[3] shows that WTLS (Wireless Transport Layer Security) protocol was designed to provide privacy, data integrity and authentication for wireless terminals. The protocol is currently being fielded and it is expected that the protocol will be contained in millions of devices in a few years
- Even though the WTLS protocol is closely modeled, but after the well studied WTLS protocol, which identified a number of potential securities problems in it. This note has described a chosen plaintext data recovery attack, a datagram truncation attack, a message forgery attack and a key-search shortcut for some exportable keys^[3]
- Ceska *et al.*^[4] discussed the “Wireless Usability Software Agent” (WUSA). The agent applies these criteria to WAP sites and generates metrics that allow evaluation of the state-of-the-art regarding WAP sites. Current solutions can test single sites, but neither the implementation of a comprehensive usability catalog nor an extensive data collection possible with an agent has been done and publicized so far. With these results, common problems and errors can be pointed out giving developers the chance to avoid and correct them^[4]
- An increasing number of computer systems are being viewed in terms of autonomous agents. Ghossoon^[5] shows that the benefit of using framework agent model Security Agent Distributed System (SADS) that based on using special Agent Platform (AP) in distributed system and its implementation in a simulation model of E-Government heterogeneous Data Bases (DB) network

The Security Agent Distributed System (SADS) uses statistical models to correlate and analysis data and take the decisions to control both local and global agent's data bases perceptively, also adopts the security problem authentication and authorization by providing a secure distributed agent system using .Net. A whole family of security terminology needs to be imported for agents (authentication, authorization and access control list), that are used in the proposed system (SADS)^[5].

The problem definition: Certainly Handheld devices and mobiles are much simpler than desktop pc and laptop in using and accessing database to implement mobility and to provide flexible movement in critical sites like warehouses for example. The identification of distributed intrusions requires cooperation of different sensors so it is advisable to consider mobile devices as a challenge to intrusion detection. To distribute intrusion detection it is possible to use mobile and intelligent agents.

The way of programming needs typing a lot of code for WAP. The business objects class, database update code and database reading code. This is a tedious work that had to be redone whenever there is a modification to the database or the business design.

The beginning of the solution is the creation of a simple ASP page that prepared for using by PDA devices. (PDA) would result less code typing to update an object. All I would do is to add much type of pages that handle by different type of handheld devices.

The proposed system: In this research there is no need to use pure ASP and XML statements to access the business site and had to stick with WAP. The old system used to create a dozen of pages to update all the projects, also be aware of pages size to support multi type of mobile devices. The proposed system suggests some new features used in visual Studio 2005, the development environment is solve this problem and there is no need to build pages for each type of devices, all what to do, is to build one page for all types of mobile.

The proposed system comes up with the idea of creating pages and applies all the roles of security agent, so that it can access the database. Also it will use all the roles that applied before of the user who access the system by PC. From now on to update the code after a change in the solution, just change the interface and keep the authorities roles and business objects.

The proposed system intends to be more flexible and reliable architecture. The main two properties are used (mobility and proxy), mobility: The ability to transport itself from one environment to another. Proxy: the ability to act on behalf of someone or something.

The architecture of the proposed system is depend on: Security in WAP (users will be able to, security administer agent), system architecture after adding handheld devices (global administering agents, local administering agents), cookies and General Packet Radio Service (GPRS) is a packet oriented mobile data service available to users of Global System for Mobile Communications (GSM) and IS-136. It provides data rates from 56 up to 114 kb.

System architecture and results: WAP stands for Wireless Application Protocol. The point of this standard is to serve internet contents and internet services to wireless clients, WAP devices, such as mobile phones and terminals. Instead of html a WAP site uses WML; it stands for Wireless Markup Language. The proposed system contains many of embedded parts used in the Distributed Security Agent Models System (DSAMS) these are:

Security in WAP: The secure transmission is between the two endpoints; this mean there is a secure transmission all the way. In the WAP gateway the packet has to be unpacked and here we may have a security leak. It is obvious that security issues have to be taken care of in the gateway to ensure a secure transmission in the end-to-end system, as shown in Fig. 1.

WAP applying with security administer agent system: Web Access and Email are the most preferred communication medium for business across the whole system and providing secure and pervasive access to it is the key to increase productivity of any successful business. Security Agents provide intelligent mobile access to Database, all business roles, Email and contacts directory.

Users can access Security Agent through any mode/device of their choice to read, reply, compose and forward emails and attachments. Further, Security Agent integrates with enterprise database and all modules, contacts directory and enables users to notify contacts, as shown in Fig. 2.

Results: So the Users can access their accounts using:

- Fixed telephones (with or without touchtone facility)
- Mobile phones/pagers, (GPRS can be used for services such as Wireless Application Protocol (WAP) access, Short Message Service (SMS), Multimedia Messaging Service (MMS) and for Internet communication services such as email and World Wide Web access
- Wireless Application Protocol (WAP) enabled mobile phones

Internet enabled handhelds. Users are alerted through SMS, paging and voice push about the arrival of new mails based on their preset rules with self-configurable details. On calling the Security Agent access number provided by the service provider/enterprise.

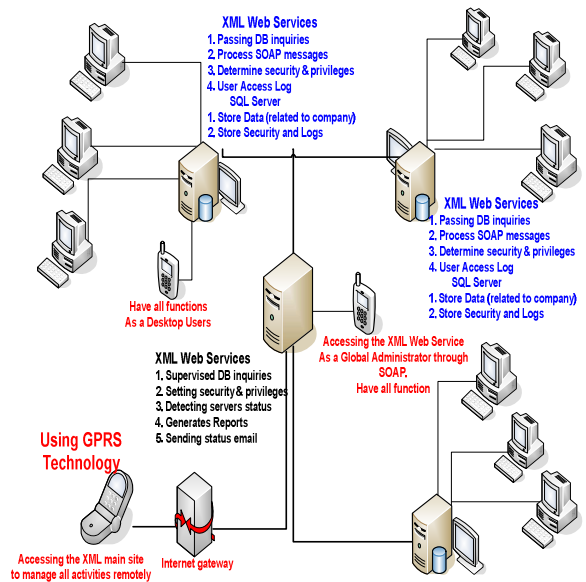


Fig. 1: Ghossoon M.W. security architecture using remote mobile agent

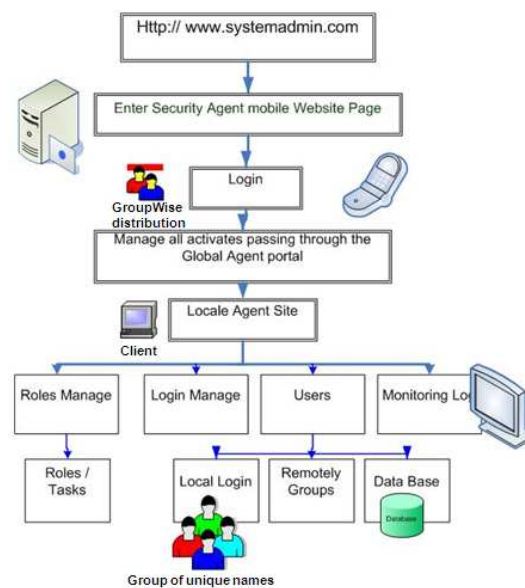


Fig. 2: Ghossoon M.W. system architecture using handheld devices (mobile agent)

Algorithms: The following algorithms refer to each part of the structure and the rules that implemented (Users and the Security Agent system Roles). Users will be able to:

- Access business database and show multiyear of reports
- Read, reply or forward the received emails with attachments

- Compose a new mail and send it to email id(s) in the contacts directory
- Delete mails
- View attachments: Plain text/HTML/Microsoft Word attachments
- Call contact: Users can call/conference the sender of the mail or any user from the contacts directory or any others by providing the contact number, without logging out of the Security Agent system

Security administrator agent:

- Synchronizes with MS outlook
- Integrates with MS-exchange server
- Integrates with enterprise contact directory

System architecture after adding handheld devices:

The proposed architecture is represented in Fig. 2 and can divide the administrator agents into Global and Local agents as the following:

Global administering agents: Administer can Access all the policies which can accessed through the web site by his handheld device:

- Manage users authorities and permission from their mobile
- Update users information
- Review and trace the log
- Send emails and SMS
- Manage database information and permissions

Local administering agents: Administer controls, manage and configure every user activity and database access within the site.

In the environment like the government, the local agent is administering of users and data in the size of ministry.

Cookie and WAP: Many WAP mobiles have no support for cookie technique today, only new WAP2 mobiles may have this support. Without cookies the session handling in your WAP application may be difficult or impossible, because the web container cannot write and receive the Session ID (via HTTP) from the WAP mobile. Session ID must be written on the mobile phone or WAP gateway to keep track of the HTTP session towards the Web container, so the session ID in the cookie can then be mapped to the session object in the web container.

CONCLUSION

Using Wireless Application Protocol will give the Flexibility and reliability for the hybrid system. This

gives the power to the proposed system and makes it easy to use. We can extend this idea by using mobile system by adding a proxy to the proposed system.

- The mobile agent used WAP protocol will make this protocol secure when transmit the messages in the distributed system using agents chrematistics
- Interaction with Security Agent is multi-mode providing hassle-free access to the user. Security Agent alerts the users based on their alert rules
- GPRS can be used for services such as Wireless Application Protocol (WAP) access, Short Message Service (SMS), Multimedia Messaging Service (MMS) and for Internet communication services such as email and World Wide Web access. GPRS data transfer is typically charged per megabyte of traffic transferred, while data communication via traditional circuit switching is billed per minute of connection time, independent of whether the user actually is using the capacity or is in an idle state

REFERENCES

1. Steffen, L. and K. Birgit, 1999. Using mobile agents in telecommunications networks-a simulative approach to load balancing. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.25.9767>
2. Abeck Sebastian, Kppel Andreas and Seitz Jochen, 1998. Management Architecture for Multi-Agent Systems, smw -abck.
3. Markku-Juhani Saarinen, accessed on 20 May 2008. Attacks Against The Wap Wtls Protocol, University of Jyväskylä, P.O. Box 35, FIN-40351, Finland. http://www.m-js.com/doc/saarinen_wtls.pdf
4. Tobias C., Stefan Kuhlins and Holger N`osekabel, 2003. Evaluation of Wireless Usability with a Java Software Agent. <http://www.wifo.uniannheim.de/~kuhlins/paper/wu sa.pdf>.
5. Waleed, M. Ghossoon, November 11, 2006. A Framework proposal for security in Distributed Agent system, Informatics institutes for postgraduate studies, PhD. thesis.
6. Richardson R., 2000. Mobile CT: The call of the wireless web. *Comput. Telephony*, 8: 140-153. <http://portal.acm.org/citation.cfm?id=349046>
7. Scott VanSickle, 1999. Wireless application protocol forum selects the open group to develop test suite for new wireless internet standard. <http://www.opengroup.org/press/22nov99.htm>

8. Thomas Peterson, 2000. WAP gateway. <http://www.student.nada.kth.se/~d95-tpe/school/wap.pdf>
9. Weiß Gerhard and Dillenbourg Pierre, 1998. Chapter 4: What is 'multi' in multi-agent learning? <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7640>
10. Affan Ahmed and Adeel Abbas, 2001. Wireless application protocol, EE-419 (communication system project report). <http://www.openmobilealliance.org/wap-210-waparch-2001>
11. Anderson Ross J., 2001. Security Engineering: A Guide to building Dependable Distributed Systems. 1st Edn., Published by John Willey, ISBN: 10: 0471389226, pp: 640.
12. WAP, 2008, Wireless application protocol and WAP architecture. <http://www.javvin.com/protocolWAP.html>
13. OASIS, 2002. WAP Wireless Markup Language Specification (WML). <http://xml.coverpages.org/wap-wml.html>
14. Robin Cover, 2001. The open mobile alliance Ltd.,
15. Gürer D., V. Lakshminarayan and A. Sastry, 2002. An intelligent-agent-based architecture for the management of heterogeneous networks. http://dpnm.postech.ac.kr/papers/DSOM/98/gurer_denise_27.pdf
16. Craig Thompson, 1997. Agent technology glossary. Revision 0.1.