A MOBILE SERVICE GATEWAY FOR MOBILE ACCESS TO ENTERPRISE DATA AND SERVICES

Xueshan Shan
Avaya Labs Research, 233 Mt. Airy Rd., Basking Ridge, NJ 07920, U.S.A.

Keywords: Wireless and mobile computing, Mobile access to enterprise services, Web services

Abstract: We present the architecture of an enterprise mobile service gateway for secure mobile access to distributed, autonomous, and heterogeneous enterprise data and services using browser-based thin-client. Our goal is to address key issues associated with mobile access to enterprise information, while minimizing the cost of service integration by leveraging existing infrastructure and business applications. Our approach achieves high extensibility and interoperability through Web Services based integration scheme and modularized device and gateway adaptation. The security and firewall issues are addressed through the loose coupling between the mobile service gateway and enterprise applications, the separation of mobile proxy and presentation server, and the two-way access control. The combination of home-deck browsing, notification, click-to-dial, and speech access interaction paradigms alleviates the limitations of small keypad and display and brings mobile users rich and personalized user experience. A prototype system has been implemented to demonstrate the significance of cost-effective mobile extension of enterprise services using our approach.

1 INTRODUCTION

With the advent of new wireless technologies and enterprise networks over the past a few years, the convenience of mobile access to distributed data and services over the enterprise network has become prominent. Enterprises are eager to extend their wireline services to mobile environment to improve the productivity and the efficiency of communications and collaborations. Enabling integrated and transparent mobile access to distributed, autonomous, and heterogeneous enterprise data and services is crucial for mobile workforce. Currently mobile operators offer services allowing corporate clients to access certain corporate services, such as e-mail and calendar, through mobile phones. However, the services are limited and not adequate for delivering highly confidential business information. Solutions that allow enterprises to extend customized services to mobile devices with full control over access to their networks would benefit enterprises significantly.

There are technical challenges in building service platforms to provide secure access to enterprise data and services using mobile devices. Firewall and security issues need to be resolved hence data can remain secured between LAN's and mobile devices. The cost of service integration, the cross-platform interoperability, and the service extensibility across varieties of devices, networks, and applications present practical challenges in the design and implementation of such systems. In addition, the service interaction and delivery mechanism needs to be very efficient to overcome the restrictions imposed by the limited on-device resources and the narrow bandwidth of mobile networks.

In this paper we present a cost-effective enterprise mobile service gateway, MiGate, for secure mobile access to enterprise data and services. It bridges the wireline services and wireless services in enterprise environment by leveraging existing infrastructure and business applications. We address the security and access control issues through the Mobile Proxy Server (MPS), the separation of mobile proxy and presentation server, the loose coupling between service logic and service delivery, and the two-way access control. The Web Services (W3C, 2003c) based integration scheme provides seamless cross-platform integration with existing and new services. The rich functionality of the service platform complements browser-based thin-client terminals, providing low-end device users with full access to information and services. The real-time data replication makes the system highly scalable and eases the setup of redundant servers to

Shan X. (2004).
A MOBILE SERVICE GATEWAY FOR MOBILE ACCESS TO ENTERPRISE DATA AND SERVICES.
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 197-202
DOI: 10.5220/0001386701970202

avoid the single-point-of-failure. The event-triggered backend synchronization mechanism enforces the data consistency between service gateway and enterprise applications. Moreover, the service access through all possible communication modes available on mobile terminals provides anytime access for mobile workforce and makes mobile phone an always-in-synch PDA.

The remainder of the paper is organized as follows. Section 2 reviews the related work in mobile access to enterprise data and services. Section 3 introduces the MiGate approach to addressing the issues brought up in this section and briefly describes the implementation of a prototype system. We conclude in Section 4.

2 RELATED WORK

There are a number of efforts that focus on various aspects of building service platforms for mobile access to enterprise data and services.

An enterprise mobile service platform, iMobile EE (Chen et al, 2003), allows enterprise mobile clients to securely access the Intranet information. A client-application communicates with the platform to establish a secure connection through either a wireless modem or a VPN. We speculate this approach is unsuitable for computing power-constrained low-end devices. Our approach focuses on secure access to enterprise data and services from browser-based thin-client to minimize the requirements for the functionality of terminals.

Another system, WMTIP (Chou, Shan and Li., 2001), enhances the security in enterprise service delivery by introducing a Wireless Secure Broker (Li et al, 2003) between the end user devices and the enterprise application server, providing another level of security. It ensures that sensitive data only stays on WSS for a pre-specified period of time to prohibit unauthorized access. Our platform offers anytime secure access through variety of communication modes and ensures that no sensitive data resides outside firewall either temporarily or persistently.

Some systems, for example, iMobile EE, use different protocols to accommodate the access to various information sources. It is not sufficient for data exchange with a large amount of heterogeneous information sources. Other systems use common data interchange formats to cope with heterogeneity of the resources. MDSS (Butrico et al, 2000) addresses the heterogeneity of devices and data sources and achieves interoperability by introducing the MDSP. However, a client-side adaptor is required to translate the client's data into MDSP and vice versa. A middleware-based architecture (Pissinou, Makki and Kong-Ries, 2000) provides a solution to allow access to distributed autonomous, heterogeneous information sources from mobile devices. CORBA (OMG, 2002) is used for data exchange, which is considered to be complex and rigid. Contrary to complex and rigid data exchange interface and non-standard data exchange format, we adopt Web Services and standard XML (W3C, 2003a) document format, providing a suitable platform for service extension and interoperability while keeping our assumption of thin-client intact.

A thin-client solution is proposed (Stajano and Jones, 1998) to give mobile users access to central resources through mobile phones, which benefits from functionality and portability at the same time. One of the limitations of the solution is that both phone and server initiated services rely on SMS (ICE, 2003), which is limited in size and not interactive. Our thin-client based approach also adopts mobile phone as access device to benefit from both portability and rich functionality. The key difference is that we provide interactive services through the combination of different communication modes and allow access to distributed services over the entire enterprise network.

3 MIGATE APPROACH

In this section we introduce the MiGate approach of secure mobile access to distributed, autonomous, and heterogeneous enterprise data and services. We overview the system architecture and discuss key issues addressed by our approach.

3.1 System Architecture

MiGate is a service gateway for enterprises to extend wireline services to mobile devices easily and securely. Figure 1 illustrates the system architecture and the data flows of the MiGate platform.

MPS resides in the DMZ of the corporate network. It authenticates users and redirects requests and responses to and from the Mobile Image and Presentation Server (MIPS), which is behind the firewall, to provide secure Intranet access for mobile users. The gateway adaptors connect MiGate to operator's networks to deliver various types of traffics over different bearers and networks.

MIPS server consists of three major components: Mobile Service Broker (MSB), Mobile Content Converter (MCC), and Mobile Service Images (MSI), which implement functionalities of service brokerage, content transformation, and mobile service image creation and storage, respectively.

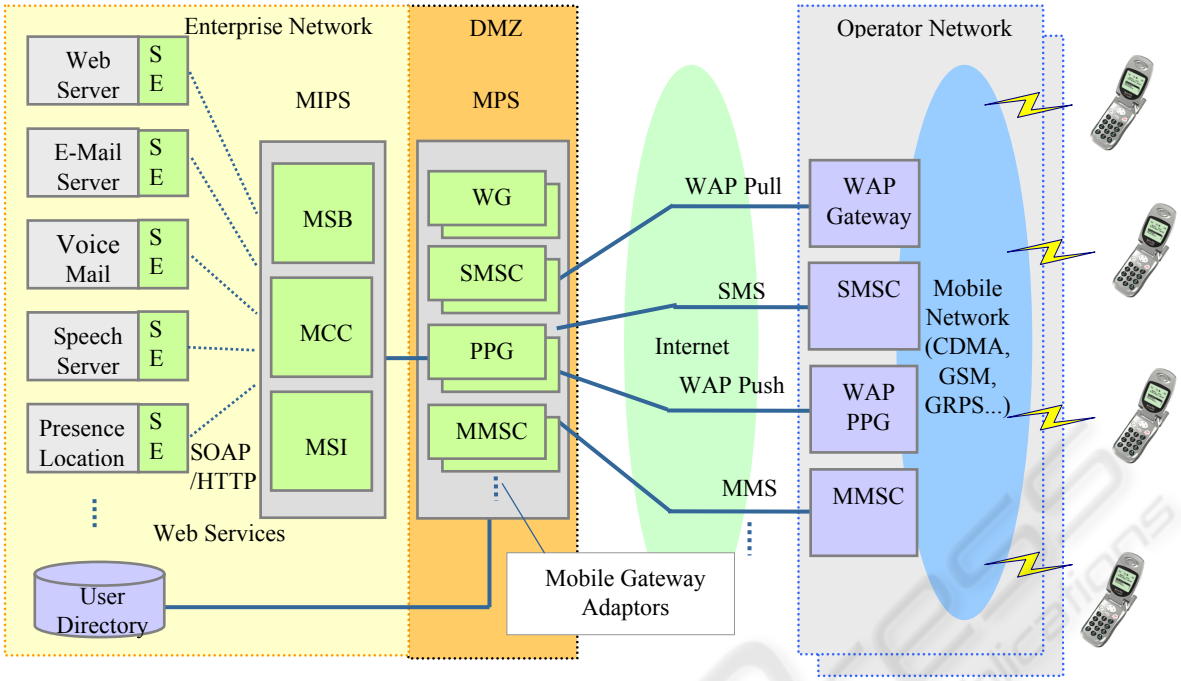

Figure 1: MiGate system architecture and data flows

Web Services interface loosely couples the distributed enterprise applications with MiGate. It further separates the service logic from service delivery, making the platform structurally extensible and interoperable. MiGate can be deployed in conjunction with any existing or new enterprise applications through a Service Extender (SE).

Figure 2 shows the major components of MIPS and the interactions among them. MSB interfaces with enterprise services and manages service access control, mobile service image creation, backend synchronization, and service coordination. The Service Access Control (SAC) matrix is built, as part of the service dispatcher (SD) initialization procedure, according to the registration information of users, devices, and services. It prohibits unauthorized access to mobile services from both mobile devices and enterprise applications. The Mobile Service Images (MSI) is created instantaneously from SAC in real-time therefore no MIPS data backup is necessary. Furthermore, MSB performs event-triggered as well as routine backend synchronization between enterprise applications and MIPS, updating MSI accordingly to maintain the data consistency.

When a notification or a service request arrives, SD checks for the accessibility against SAC and dispatches the service request to a particular service representative (SR). If the notification represents a triggering event, for example, a location change, SD chains the requests to other SRs to reflect the change. Each SR in turn invokes the corresponding Web Services to update the MSI. Finally SR relays the notification to the appropriate gateway connector. The delivery status, such as notification-sent, content-retrieved, is sent back to the service originators for reliability and session management.

MSI comprises all mobile service images that users currently subscribed. It caches service content for better performance and gets rebuilt upon service context changes. MCC transforms the service content into a format most suitable for the target device in real-time. The content rendering is governed by device profiles and user preferences gathered through registration, service activation (SA), and learning process. Adaptation to new devices is achieved by adding device adaptors.

A corporate user registers a mobile device with MiGate by providing the basic device information and personal preferences. Upon the completion of registration, an SA notification is sent to the newly registered device to confirm user's credentials and service subscription. A home-deck is in turn created on MIPS. The basic device profile is acquired from the header of the SA form. A more advanced form containing various fonts, images, and colour pallets is made available to users to further evaluate the device capabilities and the user preferences. In case WAP push (WAP Forum, 2001a) is not supported, the confirmation and evaluation will be performed through the home-deck browsing.

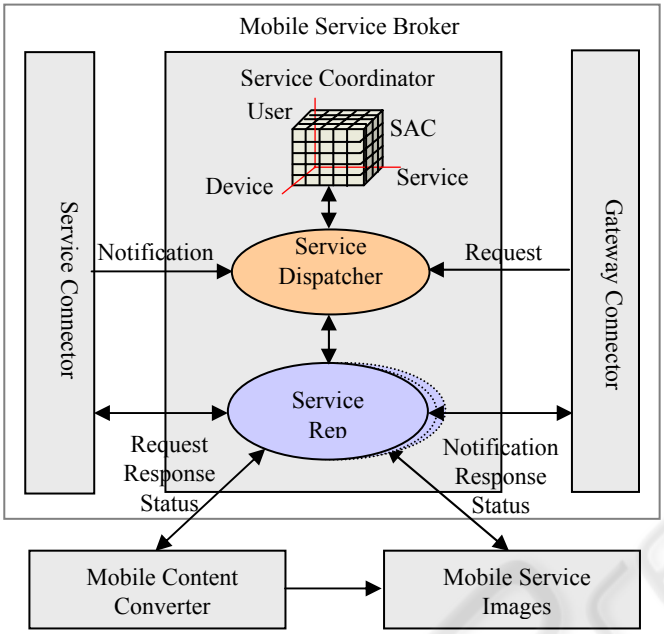

Figure 2: Major components of Mobile Image and Presentation Server (MIPS)

3.2 Security

Ensuring secure mobile access to corporate data is a primary concern for enterprises. Wireless data transmission and access to Intranet from mobile devices add another set of security issues to those in wireline services. Data needs to remain secured between Intranet and mobile devices while allowing data to pass through the corporate firewalls. Device-side security is also a major concern since mobile devices are prone to loss or theft.

In our approach, the separation of mobile proxy and presentation server enhances the security and the loose coupling between enterprise applications and mobile service gateway through Web Services adds an additional level of security. MPS serves as mobile proxy and firewall to authenticate users and to restrict users' access to certain services. MPS connects to mobile operator's gateways through SSL and provides secure browsing by redirecting requests and responses between enterprise applications and mobile users, effectively preventing intruders from accessing sensitive service content.

The SAC matrix provides two-way access control on per user, device, and service basis to prohibit unauthorized access from mobile devices and enterprise applications. The SA procedure enforces a logon-based confirmation through notification or home-deck. Notification is end-to-end secured if WAP 2.0 is enabled. In the case of SMS a brief notification is sent, which only reveals information regarding the readiness of the service content to ensure the privacy. The highly sensitive content can then be retrieved from the logon-enforced home-deck. The remote clear-cache operation on device after a specified time further secures the service content in case the device is stolen or lost.

3.3 Interoperability

Over the last decade, there have been numerous attempts in building application integration technologies towards interoperability. Those technologies were progressively evolved towards reducing the coupling between participating system components. Replacing of synchronous transfer of control with asynchronous message-based communications and relaxation of the rigid information exchange requirements by self-defining data formats were introduced for loosely coupled service-oriented architectures (He, 2003).

Web Services is a widely accepted industry standard for application integration. It leverages existing open standards, such as HTTP, TCP/IP, XML, UDDI (UDDI.org, 2003), WSDL (W3C, 2001), and SOAP (W3C, 2003b), and it is language and platform independent. A Web Service interface is a document, or a contract written in XML. The data exchanged can be any XML document such as text, images, e-mail, or any type of information. Contrary to the complex and rigid DCOM (MSDN, 2004) and CORBA interfaces, which try to capture

all of the application behaviour with assumption that all data being exchanged is of fixed format, the Web Services interface is simple and dynamic. The Web Services based architecture is loosely coupled and cross-platform interoperable, hence proving an excellent approach to transparent access to distributed and heterogeneous information sources.

MiGate adopts Web Services interfaces between MIPS and enterprise applications to achieve high extensibility and cross-platform interoperability. The event generator of SE traps the service event and relays the event to the Web Services wrapper (WSW). The XML generator retrieves the service content and converts it into a common format, XML document. WSW assembles the event and content in a deliverable form and sends them as SOAP messages over HTTP. Although all Web Services interfaces in MiGate are exclusively used for inner-corporate data exchange, additional security can be achieved at the SOAP level using authentication, digital signature, and encryption.

3.4 Device and Network Adaptation

The advances in mobile devices, wireless networks, and messaging technologies have been creating great opportunities to a vast range of new services for heterogeneous user environment. However, it also brings significant challenges for the design and development of new service platforms. A robust service platform should have the ability of adapting across different devices, networks, and applications. We achieve those objectives through modularized device and network adaptations.

Adding a new device adaptor allows MiGate to adapt to a new device with a different set of capabilities. The independence of content presentation is accomplished through the use of XML and XSLT. The service content received from enterprise applications is in the form of generic XML document. The content is then transformed in real-time to a format best suitable for the presentation on the target device.

MiGate gathers device profiles and user preferences from three different sources. The basic user and device information is collected during the registration. The device profile is retrieved from the request header in the process of SA. More subjective information is acquired in a learning-based query procedure. An evaluation form, with various fonts, images, and colour pallets, is provided to user through push or home-deck to learn more about device capabilities and user preferences.

Gateway adaptor layer extends mobile services across different mobile networks, different service providers, and different service types, such as SMS, WAP pull/push (WAP Forum, 2001b), MMS (3GPP, 2004). The gateway adaptor assembles the service information in a format suitable for a particular messaging technology and a particular network type.

3.5 Service Interaction and Access

The small keypad and limited on-device resources pose serious limitations on service interaction and access. Simple, intuitive, and personalized user interface and the ability of adapting users' mode of communications based on their need are key factors towards success. We adopt different interaction paradigms and combine notification, browsing, speech-access, and click-to-dial to accommodate enterprise users' extensive needs and to provide effective access to rich enterprise data and services.

There are several design considerations that lead to the enhanced user experiences. The one-handed user experience is achieved via data and voice channel switching. Two approaches, dialogue combined with content-push and click-to-dial, offer the capability of modality switching. Push notification delivers urgent information and services timely. The backend synchronization mechanism triggers home-deck to update upon changes of context, such as location, presence, calendar, tasks, etc., to guarantee the data consistency. A link to home-deck is pushed to the device for book marking during the SA to eliminate the needs for user input.

The proliferation of the mobile devices requires highly adaptable accessibility in mobile environment. Our browser-based thin-client solution bridges the gap between low-end devices and rich enterprise services. Simple messaging, such as SMS, combined with home-deck alleviates the requirements for device functionalities without compromising the service accessibility. This approach, thin-client complemented by rich server-side functionalities, promises low-end device users a similar user experience as high-end device users and provides access to the same information and similar services from low-end devices.

3.6 Implementations

We implemented and deployed a prototype system and two mobile enterprise services to demonstrate how enterprise services can be flexibly and securely extended to mobile environment and how mobile users access those services efficiently via different interaction paradigms. We adopt Microsoft Mobile Information Server (MIS) as MPS. WAP-over-GPRS is used as bearer for both browsing and notification traffics. We created a mobile service for

corporate e-mail and an extension that allows speech access to corporate e-mail.

4 CONCLUSIONS

In this paper, we identified the key issues and technical challenges in the area of mobile access to enterprise and proposed the architecture of a mobile service gateway, MiGate, with the aim of bridging distributed, heterogeneous wireline enterprise services to mobile devices securely and effectively. The security and firewall issues are addressed through MPS and the separation of mobile proxy from the presentation server, which keeps user information and enterprise data behind firewall. The loose coupling of enterprise applications and MiGate provides an additional level of security. The two-way access control blocks unauthorized access from both outside users and enterprise applications. We adopt Web Services as our integration scheme to achieve high interoperability across platforms and languages. The advanced device and gateway adaptation add to the system great flexibility and extensibility. The backup-free data replication scheme facilitates high scalability and fault tolerance. The event-triggered backend synchronization scheme guarantees the data consistency. The thin-client solution, enabling different modes of access to enterprise data and services, makes MiGate a general mobile service platform for a wide range of mobile devices.

The implementation of a prototype system and two mobile services demonstrates the feasibility and effectiveness of the MiGate approach.

ACKNOWLEDGEMENTS

The author would like to thank Xiao Ma for his contributions to the implementation and deployment of the initial prototype system, and Lookman Fazal, Terak Warraky, and Eniko Kovacs for the assistance in network planning and server deployment.

REFERENCES

3GPP, 2004, *Multimedia Messaging Service (MMS),* Retrieved from http://www.lebodic.net/

Butrico, M., Cohen, N., Givler, J., Mohindra, A., Purakayastha, A., Shea, D., Cheng, J., Clare, D., Fisher, G., Scott, R., Sun, Y., Wone, M. and Zondervan, Q. 2000, *Enterprise Data Access from Mobile Computers: An End-to-end Story,* Proc. of IEEE 10th International Workshop on Research Issues in Data Engineering, pp. 9-16.

Chou, W., Shan, X. and Li, J. 2001, *An Architecture of Wireless Web and Dialogue System Convergence for Multimodal Service Interaction over Converged Networks,* Proc. of IEEE ICCCN, pp. 69-74.

Chen, Y., Huang, H., Jana, R., Jim, T., Hiltunen, M., John, S., Jora, S., Muthumanickam, and Wei, B. 2003, *IMobile EE – An Enterprise Mobile Service Platform*, ACM Journal on Wireless Networks, vol. 9, no. 4, pp. 283-297.

He, H. 2003, *What is Service-Oriented Architecture?* Retrieved from http://webservices.xml.com/

ICE, 2003, *Wireless Short Message Services (SMS)*, Retrieved from http://www.iec.org

Li, J., Chou, W., Shan, X., Liu, F., Wong, E. and Rathi, N. 2003,*An Adaptable Architecture for Secure Delivery of Converged Services,* Proc. of IEEE ISADS, pp. 45-52.

MSDN, 2004, *COM, DCOM, and Type Libraries,* Retrieved from http://msdn.microsoft.com

OMG, 2002, *CORBA/IIOP Specifications*, Retrieved from http://www.omg.org

Pissinou, N., Makki, K. and Kong-Ries, B., 2000, *A Middleware-Based Architecture to Support Transparent Data Access by Mobile Users in Heterogeneous Environments,* Proc. of IEEE 10th International Workshop on Research Issues in Data Engineering, pp. 63-70.

Stajano, F. and Jones, A., 1998, *The Thinnest of Clients: Controlling It All via Cellphone,* ACM Mobile Computing and Communications Review, vol.2, no. 4, pp. 1-8.

UDDI.org, 2003, *UDDI Version 3 Specification*, Retrieved from http://www.uddi.org/

W3C, 1999, *XSL Transformations (XSLT),* Retrieved from http://www.w3.org/TR/xslt

W3C, 2001, *Web-Service Description Language (WSDL)*, Retrieved from http://www.w3.org/TR/wsdl

W3C, 2003a, *Extensible Markup Language (XML),* Retrieved from http://www.w3c.org/XML/

W3C, 2003b, *Simple Object Access Protocol (SOAP)*, Retrieved from http://www.w3c.org/TR/soap

W3C, 2003c, *Web Services Architecture*, Retrieved from http://www.w3.org/TR/ws-arch/

WAP Forum, 2001a, *Push Architectural Overview*, Retrieved from http://www.wapforum.org

WAP Forum, 2001b, *Wireless Application Protocol Specification*, Retrieved from http://www.wapforum.org/