Beyond E-mail:
Enterprise Integration Issues for Mobile E-Commerce

Brenda Lewis

Abstract

Many pages have been written on the challenges IT managers must address in preparing enterprise mission critical systems for business to business (B2B) electronic commerce, but few writers have addressed the issues surrounding the preparation and protection of these same enterprise systems for mobile e-commerce. This paper examines the history of remote access to enterprise e-commerce systems and attempts to identify the specialized issues and challenges mobile B2B e-commerce presents.

Specifically, mobile e-commerce has some specialized issues relating to separation of wireless user access from secure data because of multiple air interfaces in use. The issue of speedier and more secure transmission of corporate data over relatively slow wireless links is being addressed by a new group of tool builders developing applications which are network resident or especially designed to be accommodated on small wireless form factors. The issues of developing an audit trail for billing and non-repudiation of transactions appear more complicated than in traditional remote access over wireline networks. However, they are being addressed both by more user authentication and location profiling which is a byproduct of real-time call rating.

Brenda Lewis is Principal of Transactions Marketing Inc., Greenwich, CT.

Introduction: An Overview of Commercial Transactions

To evaluate enterprise integration issues for mobile e-commerce, first let's look at long-established IT solutions for commercial transactions via remote (fixed) access over public networks:

1. Secure data storage and transactions processing, separate from computers accessed by remote user;
2. Robust password, authorization and encryption techniques;
3. Bypass networks (virtual or hard wired) to permit reliable data throughput and reduced latency;
4. Remote access monitoring to identify compromised devices, decayed connections and network overload; and
5. Individual transactions identifiers to create audit trail for billing and allow non-repudiation of transactions;

Enterprise e-commerce existed long before 1994, when the Internet was made accessible for broad commercial use through the World Wide Web and the advent of browsers. The first remote access -- on-line, real time, non-military data communications -- is believed to have taken place in 1940. This is when Professor George Stibitz of Dartmouth Medical School in Hanover, NH sent answers via a computer over the public telephone network to problems posed by colleagues at a meeting of the American Mathematical Society in New York City. Hard on the heels of this historic transmission came a number of private, closed end user groups exchanging commercial transactions in real time over telex, X.25 and satellite networks: SWIFT in the banking industry, IVANs in the insurance industry, Reuters in foreign exchange and SITA in the airline industry.

In these global networks, remote access was easy to secure. Computers lived in locked, window-less, air-conditioned rooms accessible to only a handful of people:

1) Authorized users were few in number and known to each other;
2) Networks were privately owned, maintained and constantly monitored by employees of the owners;
3) Data load was relatively small and predictable and speeds slow, allowing nearly immediate detection of system penetration; and
4) Network topology was a hub and spoke model so an authorized remote device run amuck could be isolated and contained.

The arrival of IBM's 360 mainframe opened the door to what we now know as distributed networking. Software became portable and programmers trained by IBM began to move into corporate enterprise. American Airlines partnered with IBM in 1964 to invent roll-on, roll-off processing, the granddaddy of all non-stop, real time transactions processing. The SABRE system tracked inventory of airline seats available in real time. SABRE is arguably the first public B2B e-commerce network, linking American Airlines with third-party travel agents and later with corporate travel departments across the world. Again, remote access was a controlled affair based on a hub and spoke system, an owner-managed network with a known universe of terminals.

In 1967 the FCC handed down the Carterfone decision permitting non-Bell devices to interconnect to the public switched telephone network . Remote access began to present new issues as non-Bell dial-up modems proliferated in private enterprises in the late-1960s. Passwords and authorizations which had been central office-resident migrated to private enterprises and became user specific. A key remote access issue became how to verify the identity of the authorized user. Still unresolved after 30+ years, the authentication issue has been largely addressed by the use of passwords, encryption and public key infrastructure.

Fast Forward to the Early 1980s.

Along with the proliferation of desktop PCs and distributed networks came the first public wireless data networks. Financial services institutions were again in the lead, trying satellites, then FM sub-carriers and eventually CDPD to deliver information and later to execute wireless securities trades. Many of the techniques employed in these early networks are in use today: Aether Systems delivers Reuters financial data from a secure server with a hard-wired connection to its NOC (Network Operating Center)**,** where wireless users queries are received. Security, load balancing, billing and transactions processing are separated.

Convergys, the largest wireless bill processor in the world, uses layers of security at the device, network, host and application or transactions level. These are augmented by a private key system, which active intrusion testing helps refine. But as Convergys President Bob Marino says, "the ideal would be the elimination of PINs and access codes altogether. Convergys favors voice recognition for future user authentication. In the interim, one of the most powerful tools to prevent fraud and secure mobile e-commerce is a byproduct of real-time rating of mobile calls. Real time call rating yields geographic data which can be processed on the fly to spot cloned cell phone numbers and illegal transactions, much as American Express profiles purchase patterns to prevent unauthorized card use.”

Compounding the issues of Internet latency and security, the enterprise IT manager dealing with mobile e-commerce must now consider the security and latency of the wireless networks over which transactions flow. In the US, this problem has multiple dimensions because there are 3 air interfaces in use in the public networks, GSM, CDMA and TDMA , as well as 3 packet networks, ARDIS, Mobitex and CDPD. Beyond slow speed (9.6kbps), GSM in particular has significant latency implications from an enterprise standpoint. As Carey Gray of the UK consulting firm Butler Group explains, unless a special digital connection to a remote access server in the carrier network is installed, the GSM data is modulated to analog for passage over the landline network. Passing through two codecs results in longer call set-up and modem handshake time.

Yet another set of latency issues arise in the presentation and adaptation of Internet data for display and processing on wireless devices. Websites combine presentation and content data and must be translated for wireless device use. Use of eXtensible Mark-up Language (XML) gets around that and widespread adoption of the Wireless Application Protocol (WAP) with its XML-compliant Wireless Markup Language (WML) has provided an interim solution. But conversion of WAP at a carrier's gateway poses a security risk for the enterprise. And while 3G wireless and wired broadband networks will ultimately use end-to-end IP protocol, enterprise solutions in the near term are likely to require middleware to ensure security and high throughput for transactions.

Remember middleware? That was software which tied together applications and the operating system. In distributed wired networks, Enterprise Application Integration (EAI) became the new middleware: a category of packaged solutions designed to tie together proliferating internal corporate applications into an interoperable system. But like fruit flies, this type of software began to multiply. ERP (Enterprise Resource Planning) pioneered by SAP, Baan and later Peoplesoft, was joined by SCM (Supply Chain Management) from Manugistics, i2Technologies and others as well as CRM (Customer Relationship Management) from Siebel Systems, e-Piphany and others. All *within* the same enterprise. Then along came the Internet and opportunities for cost savings through B2B e-commerce, which meant more integration with partners *outside* the enterprise, many of whom had different ERP, SCM and CRM software.

To implement inter-enterprise integration for e-commerce, or Internet Application Integration (IAI), a company may now choose from a vast array of packaged e-commerce integration software. Vitria Technology, Inc. is the market leader in this group. End–to-end solutions require at a minimum, a business process or workflow manager, preferably with a user-controlled, object-based GUI, a component integration manager (application server), a communications or messaging manager and a data transformation manager. It must also provide adapters or connectors to a firm's legacy systems and/or to its ERP, SCM and CRM software. In addition, to providing all of these elements, Vitria was also the first inter-enterprise e-commerce suite vendor to recognize the special issues involved in mobile e-commerce, partnering with Weblink Wireless to address mobile e-commerce transactions requirements.

The complexity of inter-enterprise systems and the speed with which they must be able to change has driven the need for scalable, reusable and easily maintained software. This means a greater dependence for all but the largest enterprises on third-party software components, application servers, EJB servers, COM and DCOM objects and systems. As Anup Ghosh, author of E-Commerce Security: Weak Links, Best Defenses (John Wiley & Sons, 1998) points out, “the more components in the system, the higher the possibility of unintended interactions between the various software components. The upshot is that the more complex the software system, the less reliable, predictable and secure the system will be. This means we need to do more due diligence into these types of complex systems before fielding them.” And as Cory Reid, President of NotimeWireless notes, the bad news is that you cannot debug these components and must live with the bugs and the third party vendor timelines. Even so, he believes that more, not less contract-based programming is the answer to unburden the development staff and achieve the component and code reuse needed for complex systems. In his experience, this approach more than makes up for the cost of building or licensing code from vendors.

The New Toolkits

Companies like Thin Web and its subsidiary NotimeWireless are developing toolkits and new network resident software solutions especially designed for use in mobile e-commerce. The current set of handsets and wireless networks have a number of shortcomings, including slow data transfer rates, small screen sizes, low battery life, underpowered CPUs and difficult data input mechanisms. Each of these will improve over time, but until that happens the model for delivering applications and data to the device will be network resident. This model relies heavily on scalable, high transaction throughput servers that manage most of the computational work for the entire system as well as communicate with existing legacy systems and back office databases. The servers are also responsible for supporting multiple client types, converting all information to a form that each client understands, e.g. WML data conversion for WAP clients.

The network resident model mirrors the current Internet model of service deployment, in that, unless Java or ASPs are used there is very little advantage taken of the powerful desktop computation ability. As more powerful wireless devices and device operating systems, e.g. EPOC, KVM are rolled out, some of the computing can be off loaded to the device to avoid network latency and to achieve the goal of an always-connected device .

To reduce latency, the start-up Marbles, Inc. has developed patented server-based software for accessing and managing real-time, interactive applications on mobile computers across Wide Area Networks (termed “slow links” by the firm). Initially targeted at Palm OS, WinCE and Win32 devices, the Marbles protocol enables speedy delivery of graphically rich content independent of the network it is running on. And wireless devices operating Windows and Microsoft Office applications for mobile e-commerce are about to become smarter, faster and capable of running longer. In January, 2000, after nearly 5 years under development, Transmeta Corporation demonstrated its low power, lightweight smart microprocessor, purpose-built for “all day computing” in the field.

As wireless devices become smarter, faster and more powerful, they pose a new enterprise security risk: they will be exchanging not only voice and data, but also executable code. Anup Ghosh notes: “Distributed object frameworks support remote invocation of code. As mobile IP, distributed object frameworks and mobile code technologies like Java and Jini merge in the future, we will have new security and privacy risks.” Cory Reid agrees: “ We can already exchange applications and data between Palms. The Bluetooth standard relies implicitly on wireless transfer between Bluetooth-enabled devices. On the Java front there is going to be more emphasis put on delivering “trusted” mobile classes so authentication can easily be verified. Cross enterprise and cross application Java security will become a very prevalent issue. Validation as it happens today for applets, signing, will have a similar home in the new mobile application world.”

Yet even as we worry over security of code in mobile e-commerce, we are well on the way to solving how to verify or authenticate the identity of the authorized user. This is especially important given the high theft rate of portable devices equipped for wireless remote access. Biometric identification techniques (fingerprints, voiceprints and eyeprints) are rapidly falling in cost. As Pete Bianco, President of BioNetrix Systems Corporation explains: “In the old world, ID tokens, smart cards and passwords were surrogates for the real user. Even digital certificates are only representative of identity; whereas voiceprints and eyeprints are direct personal assurance products. BioNetrix actually makes an authentication platform that is network agnostic, device agnostic and supports all the leading authentication technologies. It is designed to allow migration from old to new security systems.“ In the wireless arena, BioNetrix has a contract with Drugemporium.com, one of the nation’s leading online drugstores, which has developed a system permitting physicians to enter a prescription from any wired or wireless device, provided that it is authenticated with biometrics.

Conclusion

In summary, mobile e-commerce has some specialized issues relating to separation of wireless user access from secure data because of multiple air interfaces in use. The issue of speedier and more secure transmission of corporate data over relatively slow wireless links is being addressed by a new group of tool builders developing applications which are network resident or especially designed to be accommodated on small wireless form factors. The issues of developing an audit trail for billing and non-repudiation of transactions appear more complicated than in traditional remote access over wireline networks, but are being addressed both by more user authentication and location profiling which is a byproduct of real- time call rating. Finally, that old problem of user authentication in a portable device equipped for wireless access seems within striking distance of a solution, albeit a still expensive one in the near term. Does this mean that we've got all the issues involved in B2B mobile e-commerce solved? Unlikely. Hackers appear to be one of the most endemic species in our information age. We can be sure that without constant vigilance on the part of all participants in mobile e-commerce transactions, new problems will surface we cannot yet anticipate.