WIRELESS TECHNOLOGY INFRASTCTURE AND DECISIONS

Binshan Lin, Louisiana State University in Shreveport, blin@pilot.lsus.edu

ABSTRACT

The promise of wireless technology is captivating, but in practice it can be perilous. Successful wireless technology depends more on design and strategy than on amount spent on wireless technology itself. This paper analyzes an in-depth case study of underlying infrastructure and architecture for a wireless technology solution.

Keywords: Wireless Security, Public Key Infrastructure, Digital Signatures, Mobile Transactions, Architecture

INTRODUCTION

Since wireless technology solutions give users the ability to access the Internet from any location at nay time, the capability to pinpoint an individual mobile terminal user's location, and the functionality to access information at the point of need (7), it has the potential to reduce administrative overhead, increase efficiency, and distribute information more rapidly throughout organizations.

One major challenge to implement the wireless technology architecture is the ability to link diverse information systems to one another in a way that allows for timely and reliable transaction processing. Without the ability to react to changing circumstance, the merchant may find himself in a position where he is either leaving money on the table or is not generating business. The ability to dynamically generate offers stems from the combination of data warehouse and event management engine. Without such capability the most important aspect of mobile technology – the ability to adjust to a specific consumer situation – is lost for obvious reasons.

The promise of wireless technology is captivating, but in practice it can be perilous. Successful wireless technology depends more on design and strategy than on amount you spend on technology itself. This paper is organized as follows. Section 2 illustrates the underlying digital signing procedure of a case study. Section 3 analyzes mobile architectures of the case study. Section 4 presents and assesses mobile solutions success in three architectural decision steps. Section 5 concludes this case study with a summary and our wireless project experiences.

DIGITAL SIGNATURE PROCEDURE

Just like hand written signatures or fingerprints, digital signatures can be used to identify entities for legal proceedings with transactions and wireless transactions. A digital signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption. The concept is a alternative of today's PIN/TAN based transactions. The digital signature solution has to comply with the following three crucial requirements of security solutions:

- *Authentication*
- *Integrity*
- *Non-repudiation*

Suitable digital signatures have to fulfill the three requirements. These requirements are fulfilled by the solutions developed in the content of the wireless project for mobile devices. Confidentiality can also be achieved by using communication standards like Secure Socket Layer (SSL) for HTTP or Wireless Transport Layer Security (WTLS) for WAP.

Public key algorithms are normally used to generate digital signatures. This means that the signer who wants to generate a digital signature for a document has to be in possession of a pair of keys. The private key then is used to generate the signature, and the public key that is sent along with it is used by the recipient to check the rightfulness of the signature.

One possible method is for the originator of data to create the signature by encrypting all of the data with the originator’s private key and enclosing the signature with the original data. This procedure would fulfill not only the first three, but also the fourth requirement above. Anyone with the originator’s public key can decrypt the signature and compare the decrypted message to the original message. Since only someone in possession of the private key can create the signature, the integrity of the message is verified when the decrypted message matches the original.

MOBILE ARCHITECTURE CONCERNS

The required components of a mobile technology architecture are listed below:

- *Enterprise-level systems*, which include ERP functionality (finance & controlling or marketing & sales), customer relationship management, supply chain planning and execution.
- *Internet-based data sources* such as a necessary weather service for the restaurant in our example.
- *Mobile data warehouse*, which allows the storage, aggregation and mining of consumption variables and their values.
- *Collaborative mobile technology exchange* that is shared between different parties and likely is built and maintained by an independent third-party provider.
- An *event management* server, which provides the capability to detect events such as customer interest (through inquiry for example) or product pricing changes, milestones such as acceptable outside temperature, rules that specify how to handle an event and a logical processor that knows when certain events leave the boundaries of a given milestone and triggers an action.

When the consumer receives the unchanged or newly established price from the collaborative exchange he either accepts or rejects the offer. Should he accept the offer, the service center is informed immediately and now has to take precaution in that all required resources including a service bay, needed materials and service technician time are scheduled and reserved. This way, the service center is fully prepared when the customer arrives and will ideally already have information on the model and make of the customers vehicle. When the customer arrives, his car will be taken into service immediately and he can be back on his planned route shortly after deviating from it. In this briefly described process it becomes apparent that mobile technology allows for substantially enhanced marketing capabilities. The merchant has effectively served a real need, builds brand loyalty through this provision of an exceptional customer experience and ultimately creates satisfaction that leads to return customers. While the customer is waiting for his oil change, the merchant also has to opportunity to sell other products and services.

The wireless project was based entirely on open standards such as the Wireless Application Protocol (WAP) and the Hypertext Transfer Protocol (HTTP), and existing infrastructures. This makes the solution accessible for many partners and avoids problems associated with proprietary solutions.

Hardware Architecture

The application can be divided into three functional separated layers. The first layer is the smart card, which is used to generate the key. The smart card is interfacing the mobile device via a smart card reader. The mobile device is connected to the Internet via a wireless interface card. Communication with the back end components was established via a web server. For the Wap-devices a WAP gateway was used.

Application Server and Legitimiation Server

For the prototype, the backend system consists of two components: an application server and a legitimiation server. The server runs on a Sun machine under the Solaris operating system. The software is mainly written in Java and makes use of Common Object Request Broker Architecture (CORBA) components architecture. The Application server and legitimating server run on the same machine. The application server provides the HTML and WML forms to the mobile end-devices for the business to business (B2B) and business to consumer (B2C) processes. The pages are dynamically generated using Java Server Page technology.

WAP Gateway and WEB Server

For the HTTP webserver, the opensource Apache-server is used. This server supports HTTPS encryption and is run on the same machine as the application server (SUN). Different WAP Gateways are used, namely the Materna gateway and the Ericsson gateway, according to the devices (IC35 and Wireless Wallet).

End Devices

During the pilot phase of the project, three types of mobile end devices were used.. These comprised Siemens organiser IC35, Ericsson's wireless-wallet, and pocket-PC devices with Microsoft's operating system

Smart Card and Smart Card Reader

The private key required to create the digital signature is located on a standardized Smart Card in check card format. These cards comply with the global standard of Identrus and are independent of the mobile end-device. The use of the Smart Card as a carrier for the certificate allows for great flexibility (5). Multi-functional Smart Cards can be used in a mobile environment, and are also suitable for use with existing Point Of Sale (POS) systems, terminals or PCs.

Architecture Interfaces

The basic architecture for all solutions in the wireless project consists of three basic elements.

- SmartCard Reader
- Client applications (Browser)
- Backend

The backend means the remaining architecture including gateway, application server etc.
There are two main interfaces between these components: The Interface 1, located between SmartCard reader and hardware driver and Interface 2, located between browser and backend. The following subsections discuss the interface architecture of the Microsoft Pocket PC devices in detail.

Client Application

The client application on the pocket PC is implemented as standard HTML pages for the Pocket PC's Internet Explorer. Additional components on the client are using ActiveX controls.

ARCHITECTURE DECISIONS

Macomber (2) suggested three fundamental architectural decisions to make when design a mobile technology solution. These include:

- Targeted mobile device
- Software model
- Connectivity mechanisms

First, while many devises exit, most mobile technology solutions have four candidate devices for considerations: Palm, Pocket PC, RIM (Blackberry), or WAP phones. These are the primary mobile devices used by the target audiences. Each device has advantages and disadvantages when it comes to mobile architecture implementation. Launching a mobile application can be done on one of these four devices, or more risky, one can support multiple devices simultaneously. In general, mobile solutions targeted to corporate users will be positioned on a single platform, as the corporation can dictate the hardware for users.

Second, two models exist for developing mobile applications. One is a Web-based model, where HTML or clipped-HTML is generated by a server, then forwarded to the mobile device for rendering. The other is an application model built to run natively using language such as C++, Java, or Visual Basic.

The third architectural decision is connectivity mechanism. Two different mechanisms exist: real-time wireless networks, or synchronization models that store and retrieve data sets between mobile devices and desk-top systems at regular intervals. Each approach has advantages and disadvantages. In general, collecting and manipulating large data sets on a mobile device requires a synchronization approach. Large data sets don't easily pass through today's low-speed wireless networks.

CONCLUSION

In this article we have described a case study of mobile technology infrastructure. This paper makes several contributions. First, we analyzed the hardware and software components of the applications. The hard and software architectures make use of standard components, which were assembled in a way to support mobile and fixed Internet transactions.

Second, we gave an in-depth analysis of the digital signature procedure. Digital signatures were used to sign a contract and to legitimate a transaction. The ability to sign documents and authorize transactions will definitely evolve in the near future. This evolution makes the use of existing applications more convenient and secure in a mobile environment. Furthermore, signatures have the potential to secure payments with credit cards and replace the transmission of the serial number with the transmission of a certificate or signature, which makes the identification of users easier.

Third, we reviewed three fundamental architectural decisions. Based on our case study, we derived some crucial guidelines to decide the best way to build a mobile technology solution. The next step is to assess its functionality and performance on real- world applications. We also plan to address open issues such as protected logging for durability, query execution on encrypted data and maintenance as well.

REFERNCES

1. Fox, D, (2000), ”Data Encryption Standard (DES), *”DuD-Datenschutz und Datensicherheit*, p736.
2. Macomber, C. (2001) ”Mobile Solutions: Success in Five Steps,” *e-Business Advisor*, Vol.19, No.5, pp.24-26.
3. Mustafa, N, and Koeltzsch, T., (2000), ”MoSign-Praktischer Einsatz Mobiler Digitaler Signaturen“, *SecuMedia Verlags-GmbH*, pp.40-43.
4. Bluetooth, (2002) www.bluetooth.org.
5. Petersburg, C., Yen, D.C., Lin, B. and Chou, D.C. (2002) “Smart Cards in the Internet Commerce Era,” *Journal of Internet Commerce, forthcoming*.
6. RSA Security (2002), www.rsasecurity.com.
7. Siau, K., Lim, E. and Shen, Z. (2001) “Mobile Commerce: Promise, Challenges and Research Agenda,” *Journal of Database Management*, Vol.12, No.3, pp.3-10.
8. Trustcenter, (2002) ”TC Demo Chipcards CardOS / M3+M4” by TC TrustCenter”, www.trustcenter.de.