Collaboration and the Knowledge Economy: Issues, Applications, Case Studies
Paul Cunningham and Miriam Cunningham (Eds)
IOS Press, 2008 Amsterdam
ISBN 978–1–58603–924-0

Mobile Applications for Public Sector: Balancing Usability and Security

Yuri NATCHETOI[1], Viktor KAUFMAN[2], Konstantin BEZNOSOV[3]
[1]*SAP Research, 111 Duke, Montreal, Canada*
Tel: +1 613 262 1767, Email: viktor.kaufman@sap.com
[2]*SAP Research, Vincenz-Priessnitz-Str. 1, Karlsruhe, Germany*
[3]*University of British Columbia, 2332 Main Mall, Vancouver, Canada*

Abstract: Development of mobile software applications for use in specific domains such as Public Security must conform to stringent security requirements. While mobile devices have many known limitations, assuring complex fine-grained security policies poses an additional challenge to quality mobile services and raises usability concerns. We address these challenges by means of a novel approach to authentication and gradual multi-factor authorization for access to sensitive data. Using our mobile Framework that facilitates low-cost composition of rich applications, we have designed and implemented prototype software that provides secure access to information stored in dedicated online systems, such as Customer Relationship Management, collaboration support, and more for Public Sector workers. Usability of our solution has been confirmed by a first evaluation conducted by a group of volunteers.

1. Introduction

Public Sector organizations are increasingly leveraging mobile devices to support and equip business processes that take place outside. Many government employees work outside of their offices or spend time away from their desks [1]. Public Sector workers such as police officers, social workers, postal workers, employees performing various inspections such as fire, food, buildings, and environmental monitoring need mobile access to information. All these people can benefit from using secure mobile applications, connected to the back-end systems. For example, they could receive assignments and information updates in real time, review contact information before the visit, use maps and routing software in order to find places, and wirelessly submit information to the back-end databases.

In many cases, using a laptop is not appropriate, because of its weight, size, power consumption and WiFi connectivity requirement. Smart phone appears to be a more suitable device, as it is becoming equipped with powerful hardware and software technologies such as J2ME, Bluetooth, GPS, digital cameras, and more – all at a greatly reduced cost and with better infrastructure support. Mobile applications and services continue to be one of the most rapidly evolving areas of technology.

Mobility is especially important for Public Security workers. In order to perform a quality job, police officers, detectives, and forensic investigators would benefit a lot from any-time any-place access to back-end Information Systems.

For this category of workers security is one of the highest priorities. They need advanced capabilities for secure access to very sensitive information. Unfortunately, the high security level is often achieved at the expense of usability and utility. Frequently typing a password is not a convenient task, especially on the tiny keypad. Using multi-modal input capabilities can lead to better usability. At the same time, it can be used for multi-factor authentication and authorization. We propose to combine unique biometric

Copyright © 2008 The Authors

attributes such as user's voice and face image, password, and Bluetooth-connected security token to provide for enhanced security. In the following, we describe our research and a first application that simultaneously enables enhanced security and better usability.

2. Challenges in Design of Secure Mobile Applications

Mobile applications have, in general, to overcome many obstacles such as limited processing power, unreliable network performance, and limited data storage. Technologies used for desktop applications don't work well on mobile phones. Mobile applications for Public Security introduce additional stringent security requirements.

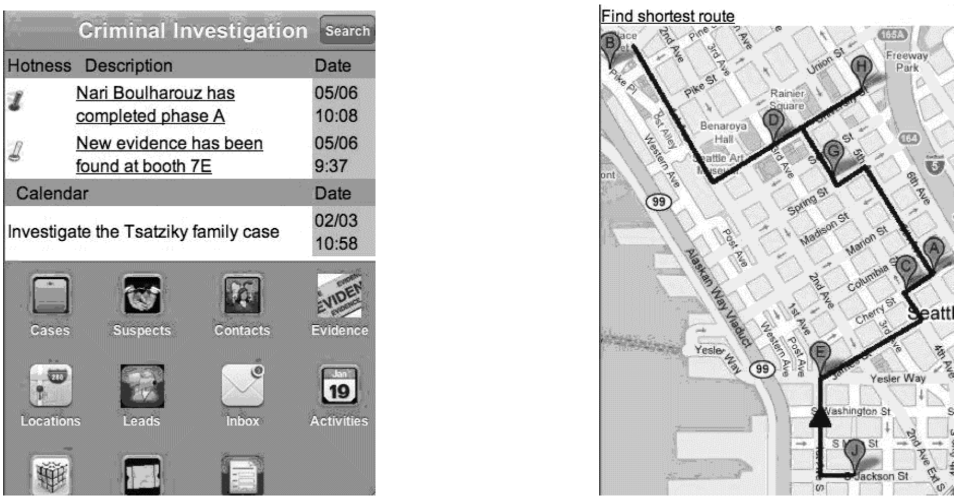
Designing applications ensuring secure mobile access to online Information Systems poses several challenges:

- Lack of control over physical location and environment of the user makes usurpation, physical tampering, and shoulder surfing attacks easier.
- Constrained input and output capabilities limit the choices for authentication and other security-related interactions via the device.
- Lack of common Operating System and common mobile-application platform implies use of custom or proprietary APIs and tools for secure application development.
- Relatively slow and intermittent connectivity prevents traditional approaches used to enforce fine-grained access control that relies on authorization verification on each access to the central server.

The state of the practice pervasively relies on password-based authentication and all-or-nothing authorization. A typical example is any application for Blackberry smart phones. It allows the user to use all the application functionality after a successful password-based authentication. For the applications where an extended level of security is required, the BlackBerry® Smart Card Reader connected to the mobile device by means of Bluetooth can be used. It prevents the use of the smart phone without proper signal from the reader. There are some international initiatives dealing with mobile security [2], but they mainly focus on mobile applications that do not require extensive information exchange with a central server. For business applications such information exchange implies the need for additional security measures.

3. Mobile Support for Public Security Workers

We have designed and implemented a prototype application using a back-end CRM system for support of Investigative Case Management, used by police investigators. The mobile application enables online and offline access to the Incident Reports, Leads, Cases and Contacts database etc.



Criminal Investigation

Hotness	Description	Date
	Nari Boulharouz has completed phase A	05/06 10:08
	New evidence has been found at booth 7E	05/06 9:37

Calendar	Date
Investigate the Tsatziky family case	02/03 10:58

Figure 1: Example Screenshots of Mobile Investigative Case Management Application

Copyright © 2008 The Authors

Incident Reports can be immediately assigned to investigators and sent to their mobile devices, together with location-based routing information, historical records relevant to the case (previous similar incidents, personal files of victims, suspects and witnesses, their connections). In the process of investigation, the officer can collaborate with his colleagues using emails, instant messages, voice, video conference, and shared media records [3, 4]. Real-time collaboration among mobile users leverages multi-media features of the phone such as camera and voice recording for documenting user activities. Forensic equipment could be used as well, by means of Bluetooth, to collect and analyze data.

3.1 Enabling Technology

We follow a systematic approach taking into account multiple requirements for the mobile solution, including timely, secure, robust and easy access to the back-end system; transparency between connected, occasionally-connected, and disconnected modes; easy application composition, development, and low total cost of ownership. This requires an innovative approach to Web Services invocation, data exchange and staging, and interfacing with the user, as well as enforcing security policies. The basic technologies that we find appropriate in this case include Service-Oriented Architecture, BPEL, semantic technologies (RDF, OWL), and others.

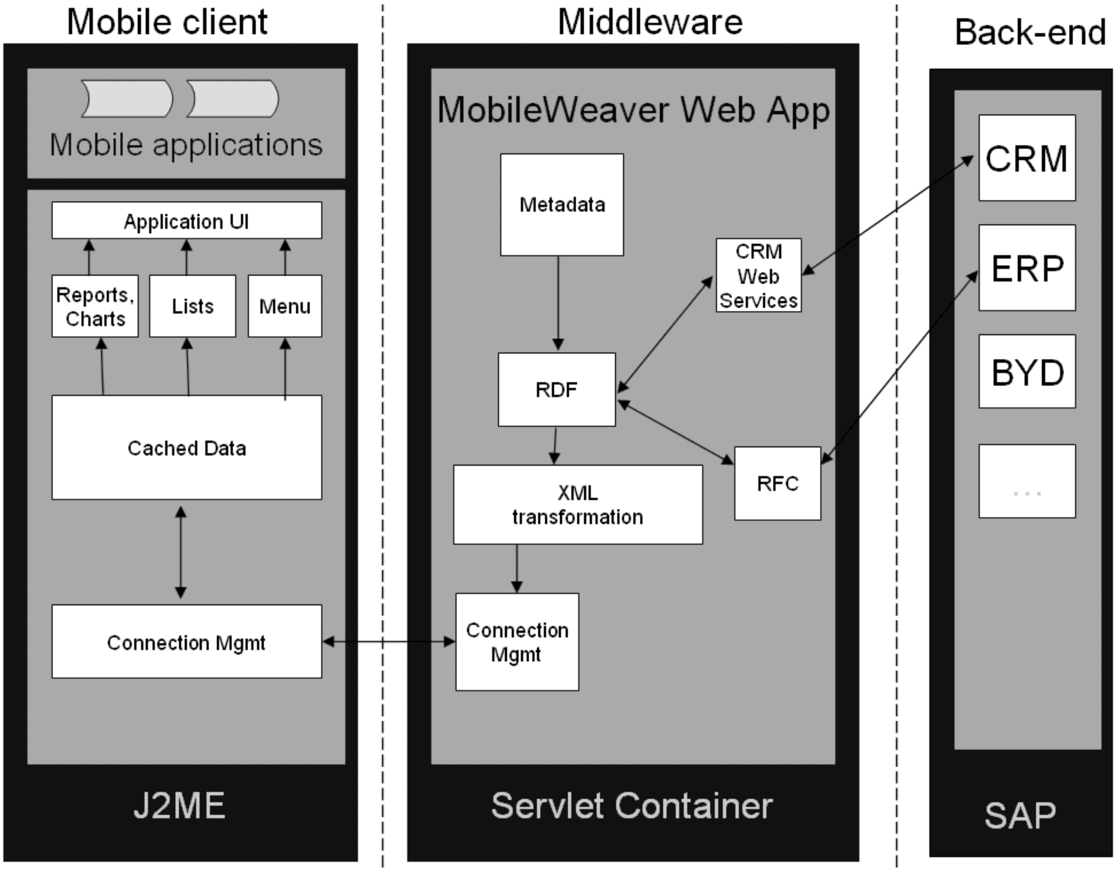


Figure 2: Framework Architecture

Our lightweight mobile service-oriented Framework [5] is designed to facilitate rapid development of rich mobile applications running on Java-enabled devices. In our Framework, the back-end business objects, such as Contact and Activity are being serialized, compressed, encrypted, and transmitted as by-design compact SOAP messages to the client side. The information is stored in the local persistent data store in a compressed and encrypted RDF format. This way, a significantly larger number of business objects as compared to a traditional file system or relational database can be stored. The cached

Copyright © 2008 The Authors

objects are decompressed and decrypted only when requested by an application. Asynchronous remote SOA-based invocation mechanism allows applications to fully function in the disconnected mode, and supports on-demand requests to the server as well as push notifications from the server.

In our solution, neither the business logic nor the user interface forms are hard-coded in the client application. Instead, the client application partially implements interpreters for open industry standards such as SOAP, OWL, RDF, BPEL, XForm and SVG. The application logic and the user interface can be modified or augmented at low cost.

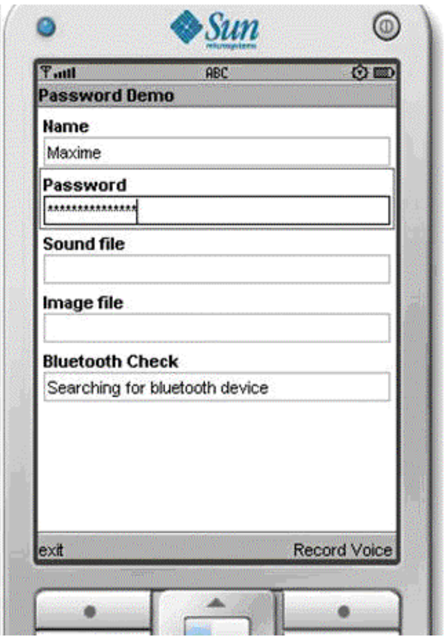
In this paper, we highlight our applied research relevant to Public Security. In particular, we use a novel approach for authentication to handle sensitive data, see Section 4; knowledge of business processes to minimize data transferred to and stored on the mobile device by means of semantic representation of use-case-specific knowledge shared between the client and the server; and flexible composition of business processes by leveraging Web standards [6].

3.2 Deployment Considerations

Our application supporting Public Security workers doesn't require special hardware or network infrastructure. The client application can be deployed on a wide range of mobile phones, supporting J2ME CLDC 1.0, including many mass-market models. It also works with the GPRS and EDGE networks – the advanced networking infrastructure deployed worldwide. Using existing handsets and networks provides for lower costs and faster deployment. Push notifications and compressing wireless traffic additionally reduce communication costs and guarantee almost real-time access to the information.

4. Fine-Grained Access Policy and Usability

Almost every data piece used by Public Security workers is confidential and requires protection of its integrity. Care must be taken in order to protect the data in the communication channel and on the device in case it is lost or stolen. For most user activities on the device, proper authentication, authorization, and audit are necessary.



Password Demo

Name

Maxime

Password

****

Sound file

Image file

Bluetooth Check

Searching for bluetooth device

Figure 3:Multi-factor authentication.

Multi-media features of the mobile devices provide a unique opportunity to use multi-factor authentication. Our application uses four factors: password authentication, hardware

Copyright © 2008 The Authors

security token connected to the phone by means of Bluetooth, and two biometric factors: voice and face recognition [7]. We provide for voice recordings and photo taking, and plan to call remote services like [8] to perform voice spectrum analysis and similar tasks.

As part of the login procedure, we can use any combination of password typing, voice sample capturing, and image taking. To prevent intruders from using eligible user's photo, randomly selected challenge is supported. For example, application can ask the user to close her left eye. In addition, the application checks if the Bluetooth token is in 10 meters proximity of the device. These four factors, in combinations, enable strong authentication.

Multi-factor authentication takes time and requires significant effort on the part of the user. Given that users often need access to only small pieces of information, which might be not very sensitive, employing all four authentication mechanisms would be redundant, error-prone, and would imply prohibitively high cognitive load of the users.

In order to find the right balance between the security and usability, we use adaptable security policies. All data accessible through the mobile device is being classified using several levels of integrity and confidentiality importance. Depending on the sensitivity level of the information that user attempts to access, different combinations of authentication means can be chosen. For example, in order to grant access to less confidential data, the system only checks that the Bluetooth token is in near proximity. However, if the user accesses more confidential data, voice or face authentication might be requested.

In our approach, we leverage OWL standard and store metadata describing required authorization level along with the business objects accessible through the mobile device. We thus classify all the objects in terms of the required level of identity assurance. We assume that using more authentication factors provides better assurance of the user's identity. If authorization thresholds are defined for both a generic business object and an inherited one, and possibly even its parts, we compute the required authorization level as a maximum of all relevant thresholds.

In order to overcome performance issues related to access validation with high level of access-control granularity and to facilitate offline access control, we "compile" security policies into a Finite-State-Machine graph on the server side. This machine tracks the current security level of the device usage. Authentication actions on the client lead to higher security levels, longer inactivity times reduce this level the same way as absence from a desktop computer leads to computer lock, see also [9]. On the client side, we determine the security state, validate user's permissions and decrypt requested objects accordingly.

For initial login, user only needs the Bluetooth security token, the most convenient and usable factor. It provides basic level of security. Most of the non-confidential information is accessible on this level. However, if user requests access to data with higher security requirements, the application would ask for additional biometric or password-based authentication. The security level is being increased until it is high enough in order to get required data. This relatively simple approach enables reliable security avoiding unnecessary hurdles for the user and without overloading her with security checks.

Finally, all communications between the server and the client are encrypted. In the case of mobile devices, there always exists an additional risk of the device being lost or stolen, so that all data is encrypted as well. A major problem for mobile secure applications is that the asymmetric key encryption scheme works very slowly if the computational power is limited, as is the case for most mobile devices. We chose a compromise solution using asymmetric encryption for most sensitive information and symmetric key encryption for all other data. This approach is also used by the well-known PGP software. The symmetric key is generated once a session and is sent to the client using the asymmetric key.

Copyright © 2008 The Authors

5. Outlook and Conclusion

We are further looking into using advanced biometric sensors connected to the phone by Bluetooth etc. and into different algorithms to assure security. While we currently manually define security policies, we hope to take a closer look at a possibility of centralized security policy management. We also hope to perform extensive usability testing. Our first evaluation with a group of few volunteers showed higher level of satisfaction with multi-factor authentication procedure and general secure navigation in our application for Public Security workers in comparison to traditional procedures. In particular, we have given the volunteers a set of ten relatively simple tasks such as finding and viewing certain contact information. Using advanced logger component that records time spent by users during each step, we measured effectiveness (number of tasks performed in a limited time), and satisfaction (perceived level of comfort).

We believe that our innovative approach based on previous works of authors will help to solve many annoying usability problems in the area of enterprise mobile applications. We have implemented a proof of concept solution based on our approach and learned a lesson that secure access to Enterprise information doesn't have to sacrifice application simplicity and usability. Our experiments confirm that we can significantly improve security/usability ratio and should continue working in the direction of flexible security policies for mobile devices.

In conclusion, we proved that it is possible to largely overcome known limitations of mobile devices even in the case of complex additional security requirements in specific domains such as Public Security. To achieve good quality of mobile services we used and improved our mobile Framework based on service-oriented approach and descriptive design approach. Descriptive design and multi-factor authentication turned out to facilitate both usability and secure access management. Furthermore, good quality of service could be achieved by means of limiting the data and services capabilities of a comparable desktop application to those explicitly required in the supported use-cases.

References

[1] T. Virki, Global cell phone penetration reaches 50 pct, Reuters, 2007. Online.

[2] GSM Association Mobile Application Security Initiative. Online. Available: http://www.gsmworld.com/using/security/mobile_application.shtml .

[3] Y. Natchetoi, V. Kaufman, L. Hamdi, A. Shapiro, Mobile Web 2.0 Browser for Collaborative Social Networking. ECSCW 2007 Workshop. [Online]. Available: http://cscwlab1.informatik.unibw-muenchen.de/Main/Ecscw2007Ws .

[4] ECOSPACE Project. Online. Available: http://www.ip-ecospace.org/ .

[5] Y. Natchetoi, V. Kaufman, A. Shapiro, Service-Oriented Architecture for Mobile Applications. To be published in ICSE companion workshop proceedings, 2008.

[6] F. Hirsh, J. Kemp, J. Ilkka, Mobile web Services. Wiley, 2006.

[7] H. Nakasone, B. D. Steven, Forensic automatic speaker recognition. In: ODYSSEY, 2001.

[8] VoiceVault. Online. Available: http://www.voicevault.com/ca.aspx .

[9] J. Crampton, W. Leung, K. Beznosov, The secondary and approximate authorization model and its application to Bell-LaPadula policies. In: Proceedings of the eleventh ACM symposium on Access control models and technologies, SESSION: Access control model, ISBN:1-59593-353-0. ACM, NY, USA, 2006.

Copyright © 2008 The Authors