International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:12, 2014

On Adaptive, Auto-Configurable Apps

Prisa Damrongsiri, Kittinan Pongpianskul, Mario Kubek, Herwig Unger

***Abstract*—**Apps are today the most important possibility to adapt mobile phones and computers to fulfill the special needs of their users. Location- and context-sensitive programs are hereby the key to support the interaction of the user with his/her environment and also to avoid an overload with a plenty of dispensable information. The contribution shows, how a trusted, secure and really bi-directional communication and interaction among users and their environment can be established and used, e.g. in the field of home automation.

***Keywords*—**Apps, context-sensitive, location-sensitive, self-configuration, mobile computing, smart home.

I. Introduction

TODAY, mobile phones have become the most important accessory of most people especially of the young generation. Beside the communication functions (phone, SMS, chat, video-calls etc.), thousands of useful information can be obtained in various situations and locations using the permanently, almost everywhere available Internet access e.g. by fast 3G networks such as UMTS [1]. Apps have been originally developed to be small programs performing a single useful task for their owner [2]. Nevertheless, most apps are written to be applied by a wide group of users, are therefore quite general and offer a high amount of functions (which usually are not exploitable by one user). Taking these facts and the high number of apps is into account, it becomes clear that users are more and more overloaded by a plenty of information [3]. They can only use a few of them and feel unable to cope with the selection of the right alternatives.

More and more sensors of the mobile devices such as GPS sensors allow the determination of the location and the context of the user, i.e. the relevant constraints of its current situation, in a very detailed manner [4]. Other users in the direct neighborhood may be detected and recognized as well as time constraints, calendar entries, flight or hotel bookings, and so on. On the one hand, this may help the mobile device to limit the information presented to the user, on the other hand, a set of activities the user may meaningfully apply to influence its environment might be selected. In [5], a method has been introduced, how a user actively may influence the content of a website by adding or removing (authorized) objects to it, what significantly extends the possibilities known from the (preprogrammed) modification and configuration of a website. A few apps like [6] and [7] are able to control devices like RC helicopters and heater valves etc. via the Internet; however those applications are permanently assigned to the respective devices and therefore hard to change. For the necessary communication, another app, called Channel-Switcher, is introduced in [8] that is able to control the use of different communication channels in an intelligent way such that the available speed is maximized, costs are reduced and channels may be switched in a transparent manner to increase security. Nevertheless, an extended use of apps is difficult as they usually must be downloaded from fixed app-stores (are therefore not reprogrammable by a given user) and can rarely be programmed such that they can communicate with different local resources in a secure manner. Also, no secure authentication of the user and the merchant is possible.

Prisa Damrongsiri and Kittinan Pongpianskul are from the Faculty of Computer Engineering. of the Kasetsart University Bangkok, Thailand.

Dr.-Ing. Mario Kubek and Prof. Dr.-Ing. habil. Herwig Unger are with the Department of Communication Networks at the FernUniversität in Hagen, 58084 Hagen, Germany,(e-mail: kn.wissenschaftler@fernuni-hagen.de, phone +49 23319871155).

II. Ideas and Concept

To overcome the described problems, special protocols and re-useable software modules have been developed. The re-usable architecture framework requires (beside a mobile phone or tablet) at least one computer as a central server and a complete WLAN or GSM coverage of the whole facility. The already cited ChannelSwitcher [8] may allow an automatic switching to the fastest, cheapest and most stable connection (see Fig. 1).

Fig. 1 Screenshot of the proposed app "ChannelSwitcher"

While the merchant or the owner of the external system to be controlled is usually known and identifiable, the customer is rarely known. Differing from WLAN cards and their MAC addresses, the SIM cards of GSM systems are usually in all

countries well registered and can consequently be used for an authentication procedure, as for instance also suggested for the PayBox system in [9]. Therefore, a special registration procedure is necessary as shown in Fig. 2. It also includes an addition of a visual (face) record, which later may allow a double check for areas with a higher security level.

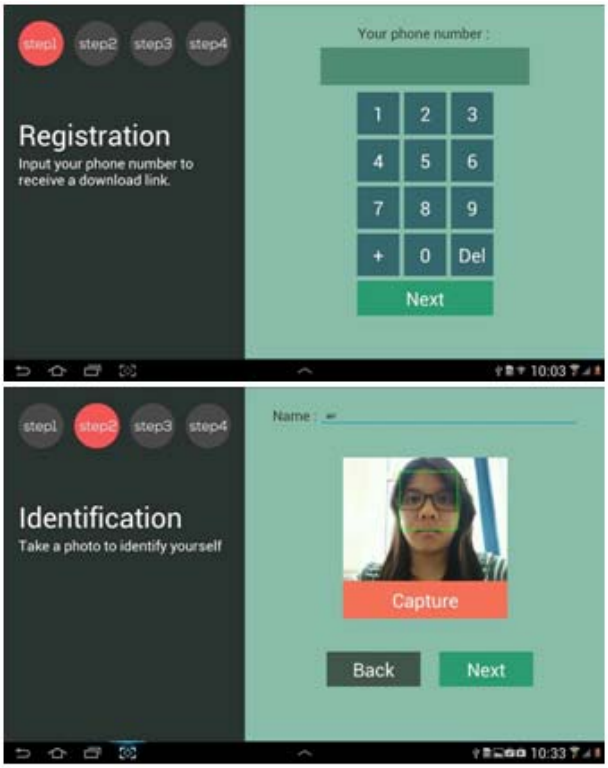

Fig. 2 Authentication process at the entry portal

After the successful registration, an SMS to the respective mobile device is sent with a link to download and install the app, which can also be configured and updated with the parameters for the respective user in advance. The respective protocol shall allow during its use

1. an automatic update of the app
2. a cancellation of the service
3. a change of rights initiated by the user and/or the administrator
4. the authentication of payment processes as well as
5. the execution of the location and context-depending functionalities (e.g. for an in-house navigation, Bluetooth marker buoys are used).

One application as an example showing clearly the advantages of such a new infrastructure is its employment in large hotels suffering form a lot of overhead to manage different bills, room keys and special orders etc. from their guests. It is our vision for this exemplary application that users may

- arrive and check-in the hotel automatically by identifying themselves at the reception with their mobile phone,
- obtain our new kind of application from the hotel
- are guided by this application through the building and will see only the currently available and suitable functionalities for which access is granted to them,
- obtain the rights to access localities (room, spa, …) depending on their booking,
- ask for additional services and
- be charged depending on their activities.

The realization of the described functionalities will transform the mobile end device of the user into a more universal n-in-1-multi-purpose device, which can increase the acceptance and ease of use of facilities and simplify logistics for both: customer and merchant.

III. Implementation

For the implementation of the server and the apps, JAVA is used to achieve a high degree of hardware independence. The exemplary initially built testbed contains light and door access solutions but may be easily extended to control other devices.

The protocol suite contains the following types of messages/message formats:

1. SMS messages to provide the registration and the exchange of key information to provide security for the remaining communications, see 2 and 3,
2. messages to control the respective environmental functionalities and
3. management messages to update customer rights and their statuses in the system or to request/revoke them from the administrator.

After the registration has been successfully completed, the process of building the user app is launched. Here, the special challenge is to automatically customize and configure the app according to specific users or user groups. For this purpose, a mechanism has been conceived that loads and injects user-specific code fragments and methods (according to the required app functionalities) from a database into the appropriate classes of the Java basis code. Then, the user app is built, signed and aligned using the command line tools of the Android Developer Tools (http://developer.android.com/sdk/index.html). The process itself is launched, monitored and controlled by another Java-based program in the server. Therefore, this process is highly dynamic in contrast to the normal (manual) app building process using an integrated development environment such as Eclipse.

After the building process has finished, the configured app can be downloaded. Depending on the position in the building, recognized using GPS or Bluetooth marker buoys, only functions, which are available, enabled and reasonable to use at the current location will appear on the screen of the app on the mobile end device of the customer.

Of course, the respective state of the system is presented on the screen to the user as well as on request to the administrator. As shown in Fig. 3, additional functionalities may be advertised, which the user currently cannot (not access rights granted) use but may be requested for (paid) usage from the administrator. The requested functionalities may also be automatically released (if advised from the administrator) or require a manual permission via a dialogue with the

administrator or super user (Fig. 4). This function may also be used to order services, e.g. a dinner menu in a restaurant.

A device controller supports at any time the status check of all devices/services as well as the manipulation of those statuses by the administrator (see Fig. 5). For a convenient functionality of the apps, a few more features are included in the code and the system:

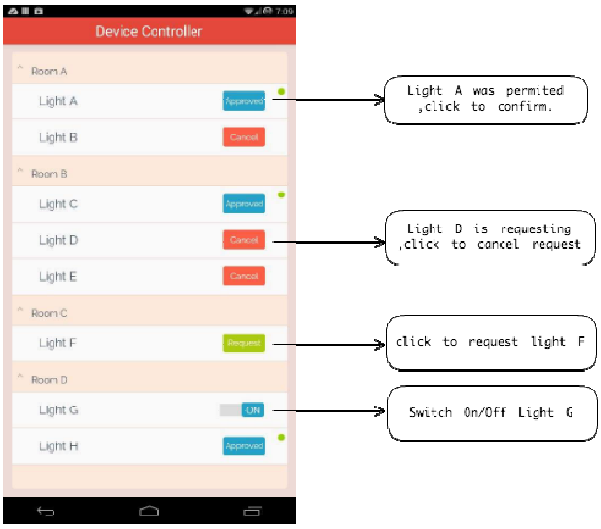

Fig. 3 User screen with room light functions

- The installed app has an expiration date and will delete itself from the customer mobile device of the respective deadline is not extended by an administrator on request.
- All messages are encoded to ensure a high information security. The keys for the password-protected WLAN will be transferred using a secure channel via GSM while all other keys for the information exchange are dynamically generated and coded into the app during the configuration process described before.
- At any time, an exchange of keys via a safe (second path) GSM-based transmission is possible without any notification of the user.
- The apk-code (Android application package, binary code of an Android app) is protected against copying by linking it to the mobile device hardware data.
- Paid services may request the transfer of additional PIN's or other security information.
- User information is transferred using a network separated from the control network of the devices/services. In a building, a transparent switching between different communication channels may, thus, increase information security even more.
- If needed, a transfer of applications at the registration desk may be limited to a wired (USB) or NFC-based transfer.

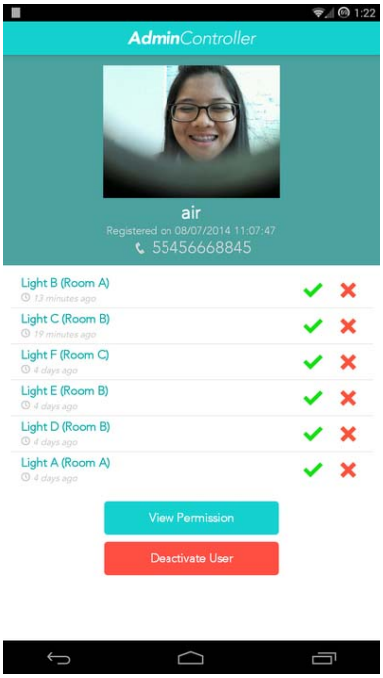

Fig. 4 Administrator screen with the presentation of the respective permissions and requests for a given user

Fig. 5 Administrator device control screen

It is an advantage of the described solution, that it may combine different network solutions. Furthermore, it is able to dynamically generate and support user-specific apps offering different functionalities whose access, in addition, can be controlled using grantable and revocable user rights. Therefore, these apps are adaptive to a great extent. Compared to existing, wired home automation solutions [10], it is also easily extendable and does not require any construction works in the buildings. Several standard solutions exist to realize the needed electric power switches controlled from mobile end devices. In the testbed solution, old Android-mobile phones have been successfully used for doing so.

IV. Conclusion

A concept for a new kind of flexible, owner-configurable and updateable apps is introduced which may transform the mobile end devices into universal, location and context-depending remote controls for the user. It is shown, which infrastructure must be implemented for this purpose and how this new kind of systems can reduce the information overload of the user by presenting appropriate choices depending on his/her current state and situation. Additionally, the memory load of the mobile device is reduced as only the needed functionalities in a specific context are downloaded.

Acknowledgment

The authors are very thankful that the 3 month internship of Prisa Damrongsiri and Kittinan Pongpianskul in Germany has been financially supported by a scholarship of the DAAD-IAESTE program. It significantly supported our cooperation and joint work in the area of mobile computing.

References

[1] M. Sauter, "*Communication Systems for the Mobile Information Society*", John Wiley, 2006.
[2] C. Anderson, M. Wolff, "The Web is dead. Long live the Internet", *Wired*, 2010.
[3] A. Marchick, "Information overload: The psychology of being connected 24/7", *Article on Mobile Commerce Daily*, http://www.mobilecommercedaily.com/information-overload-the-psychology-of-being-connected-247, last visited on Oct. 1st, 2014.
[4] N. D. Lane et al., "A survey of mobile phone sensing", *IEEE Communications Magazine*, Vol. 48, Issue 9, IEEE, 2010.
[5] M. Kubek, H. Unger, P. Hussein, W. Tiranalinvit, P. Chatpaiboonwat, "Contextual Rearrangement of Web Content", in: *Proceedings of the 3rd International Conference on IT and Intelligent Systems (ICITIS'2013)*, Bangkok, 2013.
[6] App "KNX Controller" in Google Play Store, https://play.google.com/store/apps/details?id=com.mhaspl.android.knx, 2014.
[7] App "i-Helicopter" in Google Play Store, https://play.google.com/store/apps/details?id=com.uprtek.rd2.icontroller.goldlight, 2014.
[8] M. Kubek, W. Suwanich, K. Wongyaowaruk: "Mobile Echtzeitkontrolle von Kommunikationskanälen", in: W. A. Halang and Herwig Unger: *Echtzeit 2014*, Springer, Berlin-Heidelberg, 2014.
[9] Paybox Web site: https://www.paybox.at/, last visited on Oct. 1st, 2014.
[10] H. Merz et al., "*Building Automation: Communication systems with EIB/KNX, LON and BACnet*", Springer, Berlin-Heidelberg, 2009.