Student attendance monitoring at the university using NFC

Balázs Benyó*, Bálint Sódor*, Tibor Doktor* and Gergely Fördős*
*Budapest University of Technology and Economics
Department of Control Engineering and Information Technology,
Magyar Tudsok krt. 2, H-1117 Budapest, Hungary
{bbenyo, sodorb, doktort, fordos}@iit.bme.hu

Abstract—There are several complex business processes in the higher education. As the number of university students has been tripled in Hungary the automation of these task become necessary. The Near Field Communication (NFC) technology provides a good opportunity to support the automated execution of several education related processes. Recently a new challenge is identified at the Budapest University of Technology and Economics. As most of the lecture notes had become available in electronic format the students especially the inexperienced freshman ones did not attend to the lectures significantly decreasing the rate of successful exams. This drove to the decision to elaborate an accurate and reliable information system for monitoring the student's attendance at the lectures. Thus we have developed a novel, NFC technology based business use case of student attendance monitoring. In order to meet the requirements of the use case we have implemented a highly autonomous distributed environment assembled by NFC enabled embedded devices, so-called contactless terminals and a scalable backoffice. Beside the opportunity of contactless card based student identification the terminals support biometric identification by fingerprint reading. These features enable the implementation of flexible and secure identification scenarios. The attendance monitoring use case has been tested in a pilot project involving about 30 access terminals and more that 1000 students. In this paper we are introducing the developed attendance monitoring use case, the implemented NFC enabled system, and the experiences gained during the pilot project.

Index Terms—Near Field Communication (NFC) technology, Education related business processes automation, Secure and reliable person identification, contactless card technology, embedded system with wireless access

1 Introduction

Due to the increased number of students in the higher education institutions there is a high demand for the automation of education related business processes in Hungary. This way we can reduce the cost and complexity of the administration and increase the efficiency of the education. The potential business processes to automate cover the whole spectrum of the education related tasks starting from the lecture or examination administration toward the integrated electronic examination. Even though, there are already some tasks supported by information systems but these are mainly administration related ones such as electronic student and lecture administration systems (Neptun [1], ETR [2], etc.). The automation of complex tasks, like examination is not common as they require sophisticated and reliable student identification. Previously we have presented the concept of a contacless university examination (CUE) system [3] which aims to support the whole examination process. In the CUE system we suggested to use the Near Field Communication (NFC) technology for the implementation of the fast and secure identification and data exchange features.

It is a growing challenge in several higher education institutions, as well as at the the Budapest University of Technology and Economics (BME), to incorporate the students in the teaching process as more and more information especially, lecture notes becomes easily available in electronic format via the internet. In order to ensure a healthy participation from the students in the lecture rooms such incentive process was introduced like making the students presence at lectures as perquisite of the examination. However, taking manually attendance reports during lectures can be tedious and hard to maintain task which consumes valuable in-class time.

Our current research task at the BME was to elaborate the business use case of the attendance monitoring and develop an autonomous monitoring system. The primary goal of the work was to provide an efficient way for measuring the students participation in the teaching process. Even though our long-term goal was to implement an NFC capable IT platform for further education related tasks, and to set up the fundamentals of the contactless university infrastructure.

2 Requirements

In this section we present an overview on the basic requirements of the monitoring system outlining the security requirements at the end of the section. During the identification of the requirements we had taken into account two main goals. The first goal is to provide reliable enough attendance data which can be used to

978-1-4577-0580-9/12/$26.00 c2012 IEEE

sanctioning the students. According to the university ethical codex if a student does not visit a predefined percentage of the lectures he fails the possibility to enter the exam at the end of the semester. The second goal driven by both the availability of the NFC technology and also the spreading of NFC enabled mobile equipments in the market is to prepare the system to be used with NFC enabled mobile phones as well as NFC capable smart cards.

Functional requirements

The fundamental consideration is that the student has to prove his presence in a given time window before and after each lecture. If the student meets the above requirements his presence at the lecture is confirmed.

As an average lecture at the BME is held for more then two hundred students it is necessary to provide an easy and straightforward opportunity for presence indication. To meet this requirement an average registration process should consume less than 2 seconds. Furthermore the monitoring system should provide high robustness and reliability as the main output the attendance report is used for allow or deny the possibility to the students to absolve the specific curse.

In the start-up period around 1000 students participated in the automatic attendance monitoring. The students had 8-10 lectures on a week which take place in 10 lecture room in two different buildings. An average lecture is held for 200 students. Taking into account the size of the lecture rooms a lecture can be held for maximum 500 students. As the time passes more and more students and lecture rooms will be involved in the attendance monitoring procedure. The above specification outlines a highly distributed environment where even in one lecture room the collimation of the attendance checking process is expected.

Furthermore the monitoring system should provide an efficient way for implementing extra services in the future. Such a service for example could be an interface where the students can follow his/her attendance status. The system could be extended in the future by functions aiding the examination process at the university [3] as well. This extension means services for aiding the examination registration process, aiding the student identification before examination or providing an interface where the students can examine his/her test results.

Security requirements

As pointed out earlier in this article the system should meet strict security requirements to provide a reliable attendance report. Based on this report the student are allowed to take the exam at the end of the semester a student is allowed to take the exam and complete the curse only if he appeared at more than a predefined percent of the lectures. To meet this goal the following major requirement groups were identified which the system should satisfy.

- Reliable identification: The system should accept identification and register the presence only if the student is personally present. To meet this requirement the system should prevent that one can register on behalf of another student or more students. As the students may be interested in misleading the system it may be a students interest to register his presence at a lecture in the system without personal appearance the application of paraphrases or any transferable tokens are insufficient. On the contrary a biometric identification mechanism which is more difficult to mislead consumes more time than it is expected.
- Reliable data storage and transfer: The system should provide a reliable way for storing and transferring the registration data. Especially such situations where registration data can be lost should be avoided.
- Data integrity and consistency on every components: It is essential to preserve the integrity of the registration data. If the registration data becomes corrupted then the result will be inappropriate to decide whether a student is accomplished the prerequisites of a curse.

Based on the requirements introduced so far we have implemented a distributed and highly autonomous system for monitoring the students attendance at lectures at BME. Hereinafter in this article we will present the implemented environment.

3 Implementation and results

Although a number of automatic attendance solution are known, from our point of view these systems has a several bottlenecks. From the previous requirements it is clear that the contactless infrastructure should be involved in the attendance monitoring system. The contactless technology (i.e. RFID, NFC) [4] [5] [6] could ensure secure and fast identification based on predistributed tags. As these tags are easily transferable among the students, an attendance system based on pure contactless technology can be easily circumvented. To eliminate the above weakness we chose to apply biometric identification along with the contactless technology. In our solution the personal data for biometric identification are stored distributively and serves as a binding between the appeared person and the student identifier used for registration.

For biometric identification we choose the fingerprint identification as it is wildly used and it is among the most cheapest ones. Although the central storage of personal biometric data raises both procedural and legal issues these can be avoided by storing it distributively. In our system the biometric identifiers are stored on the student cards. To eliminate the security risks which comes from the distributed storage, highly reliable and secure student cards are used.

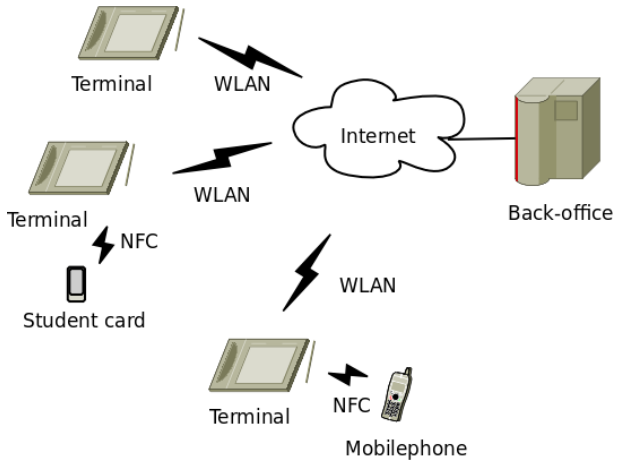

Fig. 1. Monitoring system architecture

System architecture

The implemented system is based on a number of distributed terminals managing the registration process and a central server collecting the registration logs form the terminals and implementing the presentation layer. The third main component of our system is the NFC capable student card used for registration at a terminal (Figure 1).

Student card

Every student involved in the attendance monitoring gets an NFC capable student card for attendance registration at lectures. Although there are many types of NFC cards from a number of different vendors available on the market [7] we choose the Mifare DesFire card due to its excellent safety features. In addition the Mifare DesFire card provides services for managing multiple NFC application independently on one card. The latter feature comes in handy as we expect to implement additional NFC based services in the future.

The student card contains a student identifier which is used for registering the students presence at lecture in the attendance reports. The card contains two different fingerprints from the student which serves as a binding between the identifier and the real person itself. This binding prevents one from using student card other than his own for registration. The benefit of this approach is that no one of the components in our system stores sensitive personal data other than the student card. This eliminates the necessity of storing thousands of fingerprints in our system while the Mifare Desfire card is accepted as secure enough for storing sensitive data. The chosen card has 4k memory that is far enough for storing the student identifier and the two fingerprints. The fingerprints are stored on the card as compressed lists of detected so-called minuitaes generated by the NBIS minutae detect algorithm [8]. The size of an average fingerprint is less than 400 bytes, thus the 4k memory inside the card is enough even for storing other independent NFC applications in the future.

The card personalization is done by an administrator using a special terminal. The administrator verifies the identity of the student based on the the ID card. Next the personalization terminal reads and processes two different fingerprint form the student. The administrator has to supervise this process to ensure the validity of the fingerprints. The terminal writes the fingerprints and the allocated unique student identifier to the card. Finally the administrator sends the student card issuance event to the backoffice.

As the penetration of NFC capable mobile equipments is continuously increasing on the market we plan to involve these equipments into our system to replace the student card in the future. Although the NFC technology utilized in our system supports the option of involvement of NFC enabled mobile phones, the replacement of DesFire cards by mobile devices is not a trivial issue. While NFC chip-sets integrated in mobile equipments supports the emulation of classical Mifare cards in the operation system layer the DesFire emulation is not commercially available yet. There are some reference by the Gemalto [9] [10] and NXP [11] that they have solution for the problem as well as a published article dealing with DesFire emulation cardlet. As the earlier is not commercially available and the later rises performance questions we consider the DesFire card to be not suitable for emulation by mobile equipment. Despite this, we should like to use both DesFire cards and mobile equipments in our system in parallel. To meet this expectation the terminals has been built and prepared to support the different NFC reading procedure.

Terminal

The terminal serves as the main interface between the student and the attendance monitoring system. Its main parts are the graphical interface the NFC capable card reader and a fingerprint reader. The student can register the attendance by waving the student card in front of the terminal. The terminal reads the student id and the fingerprints from the card and registers the event. The terminal either accepts the attendance automatically or asks the student for biometric identification. If the biometric identification succeeds the attendance became registered, in other case the student has to register himself in person at a defined checkpoint. If the student fails with the biometric identification and does not appear in person at the checkpoint it results in retaliation.

The number and the locations of the terminal can be dynamically changed inside the attendance monitoring system. Each terminal works autonomously and independently from the other ones. However the terminals has a wireless communication interface for periodically checking the timetable status on the backoffice and sending the attendance report. This communication channel is not considered as a permanent and reliable one. In order to resolve this problem the terminals get the timetable and identification policy once in a semester

Fig. 2. Contactless terminal

and after that it manges the attendance checking process autonomously during the given period. The timetable contains the lectures held at the specific room while the identification policy contains the rules for every lecture. These rules contains the student list and as the biometric identification is applied randomly, this rules contains the biometric identification policy as well. Every terminal in the same lecture room gets exactly the same identification policy descriptors thus if a terminal requires biometric identification form a student at a specific lecture all other terminals at the same room will require the biometric identification. Obviously after the initial distribution of the timetables and identification policies further modifications can be make on the schedule during the semester. The terminals stores the attendance logs for a whole semester but when the backoffice is available via the communication channel it uploads the logs. The uploading procedures is initiated by the terminal periodically.

On Figure 2 the manufactured contacless terminal is shown with colour screen, NFC sensing area, and fingerprint reader. Figure 3 shows the activity diagram briefly describing the contactless identification process.

Backoffice

The backoffice generates the timetable and identification policies for the terminals and collects and stores the attendance data. Timetables contains the lecture dates for a specific terminal while the identification policy describes whether a biometric identification is required form a specific student at a specific lecture. Both the timetable and the identification policies are generated for a whole semester and distributed to the terminals before the starting. During the semester the timetables and identification policy descriptors can be modified by the backoffice as well.

The other main role of the backoffice is to collect the attendance data form the terminals and generate the attendance report for both the university staff and the

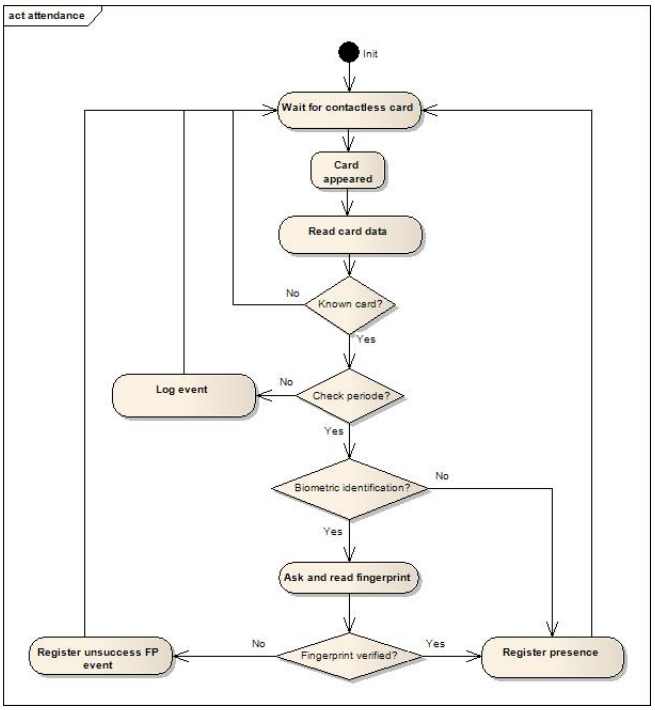

Fig. 3. The contactless identification process

students. The attendance data is collected periodically every day. As the terminals has far enough storage space for storing attendance data for the whole semester, even after successful transition to the backoffice the attendance data remains stored on the terminal as well. After collecting the attendance data the backoffice generates the attendance report for every student and provides an interface for visualizing it.

4 Conclusion

We have implemented the above described autonomous student attendance monitoring system at the BME. The monitoring has been lunched at the beginning of the last semester involving around 1100 first year students and 8 curses in 7 different lecture room. The system operated during the whole semester almost without any failure. During the semester our system accepted more than 200.000 card identification with more than 20.000 biometric identification. From the 1100 students around 100 was prohibited from accomplishing certain courses.

During the introduction period of the monitoring system there was not any successful and registered attack against it. Two weeks after the installation the students accustomed to use the system properly and the registration process became an essential activity.

5 Summary and Further Work

This article is introduced an autonomous student attendance monitoring system implemented and used at the BME. We gave a brief overview on the requirements of such a system and presented the architecture along with

the operation of the implemented system. The system has been used during the last semester to indetify first year students who does not appear regularly at the lectures.

As a further work we identified two main tasks. First we will involve NFC capable mobile phones in the identification process which requires both the implementation of the mobile application as well as the configuration of the contactless terminals. Later on we are going to develop further business process in the university education like electronic examination management system. This processes will be implemented over our contactless platform.

ACKNOWLEDGEMENTS

This work was supported by the National Office of Research and Technology grant id: Diad_NFC (project no. TECH_08-A2/2-2008-0093) and in part by Hungarian National Scientific Research Foundation, Grants No. T80316 and T82066.

REFERENCES

[1] Bme neptun portal. [Online]. Available: http://www.neptun.bme.hu/
[2] Elte etr portal. [Online]. Available: https://etr.elte.hu/etrweb/login.asp
[3] G. Fordos, T. Doktor, B. Benyo, and B. Sodor, "Building a contactless university examination system using nfc," in *Proc. IEEE Intelligent Engineering Systems (INES), 2011 15th IEEE International Conference on*, Szlovákia, 2011, pp. 57–61.
[4] W. Webb, *Wireless Communications: The Future*. John Wiley & Sons, 2007.
[5] A. Vilmos, G. Fordos, B. Sodor, L. Kovacs, and B. Benyo, "The stolpan view of the nfc ecosystem," in *Proc. IEEE WTS 2009, 8th Wireless Telecommunications Symposium*, Prague, Czech Republic, May 2009, p. 5, paper 1569183809.
[6] B.Sodor, G.Fordos, L. Kovacs, A. Vilmos, and B. Benyo, "A generalized approach for nfc application development," in *Proc of WIMA*, 2010.
[7] N. Forum. Nfc forum type tags. [Online]. Available: http://www.nfc-forum.org/home/
[8] M. D. Garris, E. Tabassi, C. L. Wilson, R. M. McCabe, S. Janet, K. Ko, and C. I. Watson, *User's Guide to NIST Biometric Image Software (NBIS)*. National Institute of Standards and Technology, 2006.
[9] Gemalto. [Online]. Available: http://www.gemalto.com/
[10] Gemalto, *Worlds First: Gemalto Integrates DESFire Transport Card into NFC Mobile Phone*. John Wiley & Sons, 2007.
[11] Nxp. [Online]. Available: http://www.nxp.com/