Security Threats in Auto Vaccination Architecture Implemented in Handheld Device

Maricel O. Balitanas*, Min-kyu Choi*, Farkhod Alisherov*,
Seok-soo Kim*, Taihoon Kim*
*Dept of Multimedia Engineering, HanNam University
e-mail:jhe_c1756@yahoo.com

Security Threats in Auto Vaccination Architecture Implemented in Handheld Device

마리셀 바리타나스*, 최민규*, 박호드 알리셀로브*, 김석수*, 김태훈*
*한남대학교 멀티미디어공학전공

Abstract

This study focuses on the security issues of a handheld technology in auto vaccination scenario. Handheld or palm-based computing technology, commonly known as personal digital assistant (PDAs)are having tremendous impact in many personal, educational and business settings, the potential is particularly compelling for healthcare, specifically in the clinical settings. By exploring the development of the technology and its application, as well as the issue of its security would provide a better understanding of this technology

1. Introduction

People have become more and more mobile. One big thing that really got a boost in 2008 was mobile broadband. The technology particularly, lead people to do their jobs outside the companies secure parameters. This trend could ultimately lead to catastrophic data leakage that is if it is not prevented by good policies and encryption. This study focuses on the security issue of a mobile handheld technology in auto vaccination scenario.

Vaccination is the administration of a vaccine to stimulate a proactive immune response that will prevent disease in the vaccinated person it contact with the corresponding infectious agent occurs subsequently [1]. Thus vaccination, if successful, results in immunization: Vaccination is a highly effective method of preventing certain infectious diseases. For the individual, and for society in terms of public health, prevention is better and more cost-effective than cure. Vaccines are generally very safe and adverse reactions are uncommon.

1.1 Problem

Due to fast pace of civilization in most countries, the family as the basic unit of our society has an increased necessities and to be able to provide the needs, the father has become not the only sole provider in this unit but the mother as well. However with the demand of work to working mothers the effect would lead to

less time for children and attention to their health needs. Thus, with this pressing issue my proposal is to address one of the health needs of an infant to his/her childhood in terms of vaccination and less the burden to a working mother in dealing and setting appointments to the child's pediatrician to have vaccination shots.

If we keep vaccinating now, parents in the future may be able to trust that diseases like polio and meningitis won't infect, cripple, or kill children. Vaccinations are one of the best ways to put an end to the serious effects of certain diseases.

Most parents have realized the need of administering vaccinations to children. Vaccinations come in different stages and in different age levels. Despite there are catch-up vaccination schedules at different age levels worst is high risk is around the corner. Thus it is just convenient and practical for parents to have a digital aid that will do the appointments with their children's physician instantaneously because parents have tons and tons of work loads and have become preoccupied in their work these days.

With this pressing issue in vaccination, the issue of security comes along with it. In developing even a simple application security issues should not be left unconsidered. Latest IT security threats plugging the corporate office are actually clipped to the belt and purses of a company's mobile workforce. Wireless devices that can send and receive e-mail are emerging as serious cooperate threats because they have become so advanced and widely accepted, yet are so thinly secure, that cyber criminals are targeting them as a path to corporate data.

2. Related Studies

Childhood Immunization Schedule, This immunization schedule is based on the 2008 Childhood and Adolescent Immunization Schedule recommended by the Advisory Committee on Immunization Practices (ACIP), the American Academy of Pediatrics (AAP), and the American Academy of Family Physicians (AAFP). This schedule provides generally recommended dates for immunization based on your child's birthdates. Some diseases or treatments for disease affect the immune system. For children with these diseases or for children receiving these treatments, the recommended immunization schedule may need to be modified. If you have questions or concerns, consult your child's physician or other healthcare professional for advice about your child's immunization schedule.[5]

Another related study to vaccination planner is the eMedCheck; it is an electronic medication screening form that can be run on a PDA. Using this software, POD staff record basic information about family member. The software uses decision rules to determine which medication each person should receive. It also records the results for later analysis. [6]

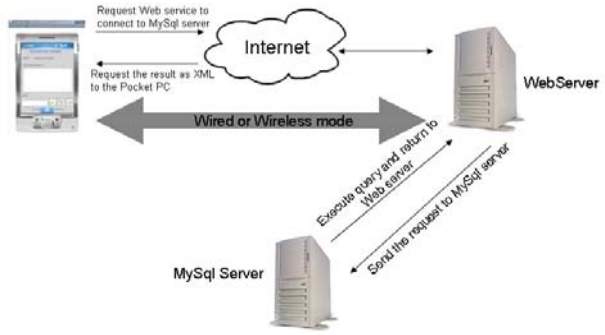
3. Vaccination Planner Architecture

The general architecture of vaccination planner is depicted on figure 1. The objective of this research is to develop a decision support tool that will help parents to automatically received vaccination shots appointment for their children ages 0-6 years old from their Pediatricians. However, it will not only be a conventional type of vaccination schedule from the Pediatrician because as an additional feature it will be able to filter the personal planner of the parent using the mobile device as shown in the Software Representation Diagram of figure 2 and be able to displayed as a blocked calendar in the end of the Web Server. This blocked calendar will be the basis of filtering an amenable schedule both for the parents to bring their children in the clinic for vaccination shots and the child's schedule base on the its vaccination planner schedule in the Pediatricians portal.

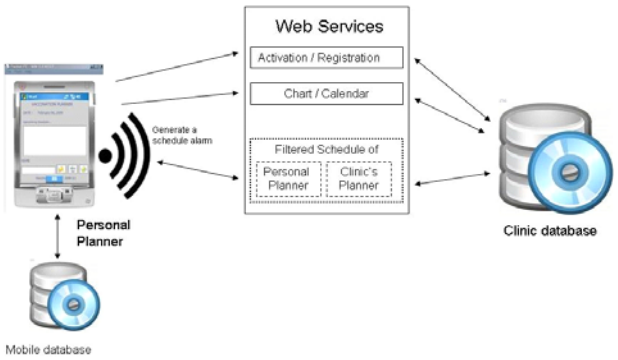
We are exploring applications of personal digital assistant technology to a range of medical

applications.

In this research the researchers used a Connected Device Configuration (CDC) since this is for devices with much greater memory, processing power and network connectivity such as smart phones, set-top boxes, internet, and embedded servers. CDC is defined as a specification that has passed through Java Community Process (JCP). The CDC is known as Java Specification Request (JSR) 36.



[Fig. 1] Vaccination Planner Architecture



[Fig. 2] Software Representation Diagram

The CDC specification is much smaller document than the CLDC specification because the CDC is much closer to a Java 2 Standard Edition (J2SE) runtime environment than the CLDC. The specification defines four things in particular: [8]

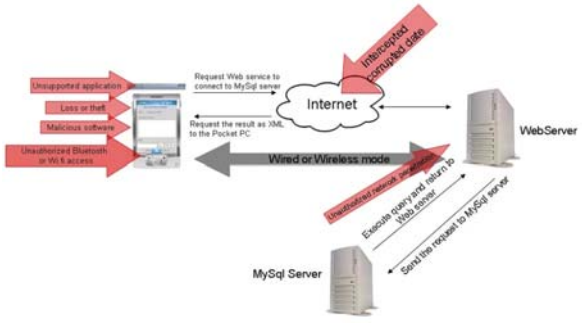
- The capabilities of the Java virtual machine (VM). Unlike the CLDC, the CDC VM is a full-featured VM
- A subset, much larger than the CLDC's, of the J2SE 1.3 classes.
- The same API's (application programming interfaces) that are new to the CLCD
- Support for file-and datagram-based input/output using both the GCF and the familiar java.io and java.net classes

4. MobileSecurity Threats

Mobile powered devices and software offer a potential benefit, including lower operating costs and greater productivity.[9] However, organization that deploy mobile solutions need to make security a priority. Illustrated in the following figure is the possible security threats to auto vaccination planner implemented in a handheld device.

Malicious software : Viruses, Trojan horses and worms are familiar threats to traditional workstations and laptops. While mobile devices have not yet become a significant target, there is a growing consensus among security experts that mobile devices will be a targeted. Even malicious software not designed to deliberately inflict damage may have unintended consequences such as data disclosure or corruption

Loss of sensitive data : Some organizations consider mobile devices a security risk only if they have a business application installed. Other organizations consider the loss of calendar and contact information a security risk. Consider the potential consequences if an executive's e-mail inbox or calendar, full of meetings and briefings, were retrieved by a competitor. Contact information can also cause problems if it falls into the wrong hands, as recent high-profile incidents have demonstrated. Organizations need to protect the data on their employees' mobile devices.



[Fig. 3] Security threats to a network that supports mobile devices

Device loss or theft : Losing a device to mishap or theft can cause lost productivity, data loss, and potential liability under data-protection laws. Thousands of mobile phones and networked handheld devices are lost or stolen every year. As sales of mobile devices increase, the negative effects of device loss and theft are sure to increase accordingly.

Unauthorized device connectivity : An employee device connecting to a personal device to exchange Active Sync may bypass security settings and applications required on a corporate device

Unsupported or unsigned applications : Older applications that are no longer supported, while they may still work, are dangerous because they may be vulnerable to attack by new viruses. If an unsigned application is installed on a device it could make changes to device that would jeopardize it security.

Intercepted or Corrupted data : With so many business transactions taking place over mobile devices, there is always concern that critical data could be intercepted along the path through the Internet cloud, via tapped phone lines or intercepted microwave transmissions

Unauthorized Bluetooth or Wi-Fi access : Many mobile phone users employ hands-free Bluetooth headsets, potentially leaving hackers a hole for BlueSnarfing data on the device or BlueBugging to gain control of the device. Ad hoc wireless network connection can also lead to unauthorized device access.

Unauthorized device connectivity: An employee connecting a personal device to the Exchange Active Sync may bypass security settings and applications required on a corporate device.

Unauthorized network penetration: Because many mobile devices provide a variety of network connectivity options, they could potentially be used to attack protected corporate systems. Attackers who gain access to a mobile device may be able to impersonate a legitimate user and gain access to the corporate network.

5. Conclusion

The expected technological advances indicate the tremendous potential of Vaccination Planner technology. Several emerging technologies, promise further performance improvements. However, a number of challenging tasks should be further addressed in an effort to make this technology affordable, robust, secure, and easy to use. Further challenges include:

- Standards for wireless communication, messaging, and system support.
- Planner and automatic upload to support intermittent upload links to the medical server.
- Given the increasing number of user's familiar with the use of cell phones and PDAs, we expect wider user acceptance
- The catering of not just children vaccination in the system but as well as the vaccination for all ages.
- Outlining the features of security-enhanced mobile network and protocol for data encryption and device authentication

Reference

[1] Vaccination Schedule, http://www.wikipedia.org
[2] Vaccination Schedule, http://www.wikipedia.org
[3] The Children and Adolescent Immunization Schedule 2008, http://www.aap.org.
[4] http://www.cdc.gov/vaccines
[5] http://www2a.cdc.gov/nip/kidstuff/newscheduler_le/
[6] http://www.isr.umd.edu/Labs/CIM/projects/clinic/emedcheck.html
[7] Vaccination Schedule, http://www.wikipedia.org
[8] http://www.developer.com/java/j2me/article.php
[9] http://technet.microsoft.com/en-us/library/default.aspx