SIRS Project Topics 2016-2017

DISCLAIMER: in the designed and proposed applications, user interface concerns are secondary. The security aspects (such as functional and assurance) are the essential points where you should focus and will be main metrics to be considered in the grading of the work.

Revised on 2016-10-11

Available topics to be selected:

1. Medical Records database

Health care institutions gather and store sensitive information from patients with the goal of providing the best care. The medical history of a patient is essential to guarantee that the right diagnosis is achieved and help the clinic staff act in the shortest time possible. This information is highly sensitive and must be kept private for the responsible staff only. At the same time, the medical records should be accessible by any health care institution to ensure that a patient can be attended anywhere.

To guarantee data availability, health care institutions rely on data repositories accessible through the Internet. This exposes a threat since patient data can be accessed by unauthorized personnel. It is also extremely difficult to manage access to data using standard access control mechanisms due to the vast amounts of user, groups and patients and the constant adjustment in privileges that must be done to maintain patient's confidentiality.

Define a cloud based system to store medical records. The records are available for a wide range of users, so the system must provide an interface to manage access privileges to the records (consider using different access control models – e.g. ABAC, RBAC – and standards – e.g. XACML).

2. Remote document access

Collaborative office applications allow groups of users to create and edit documents remotely. In these applications a user, owner of the document, is able to select contributors to gain access to the document. Documents cannot be accessed by unauthorized parties. If an attacker accesses the servers storing the documents he must not be able to view the documents and if he tries to edit any document, there must be a way to detect the illegal modifications.

Design a cloud based solution that allows documents to be shared over a network in a secure fashion. This application should allow authenticated users to access local and remote files in a transparent way. Data confidentiality must be assured even in the case where an attacker gains physical access to the data storage devices. Illegal modification of the documents by unauthorized users must be detected.

3. Smart Restaurant

Consider a Smart Restaurant scenario where the overall goal is to improve the service quality and speed for regular customers of restaurants, by using a mobile app (e.g. Android).

The customer's phone should be located automatically inside the restaurant space (e.g. table) using indoor location technologies, like: QR code scanning, iBeacon detection, Wifi, LiFi, etc.

The customer should access the menu and make the food order using the app. Finally, the payment and invoice/receipt issuance should also be handled in a secure way.

There should be concerns regarding the privacy of the user, because food preferences can provide information about personal health and tastes.

4. Secure online auction website

Auction sites are a useful tool to promote the exchange of goods directly exploiting the demand and request needs of dynamic markets. The goal of this work is to create an on-line auction store, providing sellers and buyers a reliable website with all the mechanisms for the secure transactions of products and goods. The site must be secure against the threats like XSS and SQL injection and/or other attacks.

The solution should consider all layers explicitly, including: web layer, application server layer, database layer; and their respective servers. The network topology should be adequately designed having in mind the need functional and assurance requirements with security in mind.

A banking system can be considered as another secure website to be developed by the students or a simple server application (with the most basic interface and without security).

5. Smartphone as a security token

The smartphone is a digital companion for most people. This work should leverage its presence (proximity) as part of an increased security solution.

One idea is to use the mobile device for two factor authentication, i.e., the user should have the phone with himself to answer a security challenge posed by a web application. Consider the example of an academic management system (e.g. Fenix) that wants to ensure a stronger authentication for certain operations.

Another idea is the encryption/decryption of files (or directories) based on the phone's presence. A secret key is kept on the phone and then provided to the computer via Bluetooth/NFC (which may be simulated by any other type of channel, such as a WiFi connections) using a secure protocol. The computer will have service running that maintains the files decrypted only while it senses the phone; when the phone moves away, the directory is encrypted again.

6. Secure payments using SMS

SMS are still one of the most widely available messaging services. Given this, the goal is to develop an application for a smartphone (e.g., Android or simulated by a small program in Windows or Linux sending and receiving SMS-like messages via a UDP channel) that enables the exchange of SMSs in order to authorize bank transactions.

For this transaction the user must send the IBAN (2 characters and 23 digits) of the account where the money should be transferred to, the amount of money to be transferred (8 digits).

Mechanisms must be added in order to assure a secure order (i.e., taking into account security requirements such as integrity, confidentiality and authentication) considering SMS messaging constraints (with a maximum of 120 characters). Techniques such as cipher text stealing can be used to ensure that the message limits are respected. Consider the possibility of assuring non-repudiation.

You can consider that the phone is able to securely store and use a limited set of keys (private and/or secret).

7. Secure child locator

In this scenario, consider the problem of child localization in outdoor spaces.

Develop a service for smartphone users (e.g., Android) that enables the tracking of children using GPS (e.g., A-GPS) only by their authorized legal guardians (and not by anyone else).

The service to build should consider the secure tracking of the children. Both the children and the responsible adult should be considered as users of the system, and all stored and communicated data should take into account their privacy.

8. Secure Smart Home

In the Smart Home there are already emblematic products, like the Nest thermostat from Google, that provide a glimpse of what can be achieved when things are connected between them and to Cloud services.

There are also open devices and development kits, like the Arduino and Raspberry Pi, that can be used to develop new ideas in this domain.

The Smart Home gateway is a central component in a Smart Home system. It provides internal connectivity to the sensors, using specific network protocols; and external connectivity to the worldwide Internet, using IP.

The gateway can also play an active role: it can filter data to reduce data volumes and to safeguard the privacy of the people; it can also provide a management and monitoring console.

In this scenario, you should consider how to implement some of the described functions of the Smart Home gateway in a secure way.

9. Secure Smart Cars and Vehicular Networks

Software has been embedded in our vehicles in the past few years. Nowadays, several critical systems – like the brakes – are controlled by software and several components communicate between themselves using the internal car network. Furthermore, in vehicular networks, there communication vehicle-to-vehicle to detect road obstacles and avoid traffic accidents.

Both this uses of software pose security risks. These can be: exploitable software, malicious updates, or impersonation, privacy, or network disruption in the case of vehicular networks.

The goal of this project is to study one of the above problems, as well as the technology involved in the current solutions. You should develop a security solution that mitigates one such potential problem.

NOTICE that there is no need to simulate the full auto environment. e.g., if you develop a solution to manage the braking system, a message "breaks ok" in the console would be enough.

10. Truthful Emergencies

Emergency systems, in particular first responder ambulances are scarce resources in our society. Their usage should be carefully planned, and only triggered when really needed. Improper usage should be avoided, and careless usage should be penalized.

The goal of this project is to consider a scenario where a user requests help using a device (similar to dialing 112 on a phone) and the current emergency context – e.g. location – is captured and sent to a dispatch central for processing. Furthermore, users should be accounted for incorrect usage of resources and reckless behavior. You may want to consider certification, non-repudiation, and auditing mechanisms.