SIRS Proj Proposal Topics '15'16

Proposals

1. Medical Records Database

Medical records typically involve a rich set of authorization requirements that have a natural description in terms of sets of credentials. A credential defines a principal to be a doctor; a credential defines a doctor to be qualified in a certain specialty that gives access to certain records; a credential defines a doctor to be associated with a hospital; a credential associates a doctor with a given patient; and so on.

Define a system in which such authorization requirements can be stated and enforced. Your system should not implement a fixed policy, but rather should enable the policy to be specified dynamically. You should also provide example policies that are realistic. For example, an allergist probably does not need access to psychological records; an emergency room doctor needs access to the record of someone who has not previously declared this physician her doctor.

For your solution, consider different access control models – e.g. ABAC, RBAC – and standards – e.g. XACML.

2. Remote document access

Documents are crucial for collaboration between people. Many times they have to be accessed remotely.

Design a solution – server and client – 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.

Consider different document hosting possibilities, including Cloud providers.

3. Secure Scheduler

Electronic calendars are very convenient for setting up appointments and then having them accessible in multiple devices like smartphones and computers. However, there are privacy risks in using them. Some personal information can also be leaked when setting an appointment with another person or a group of people.

Design a solution to schedule meetings with privacy.

For increased usefulness, consider using actual calendar data – Google Calendar, Outlook.com - that can be accessed using APIs.

4. Shuttle reservation system with user reputation

Consider an on-line shuttle bus reservation system that could be accessed by users to book bus seats.

You have to consider special rules for assignment (e.g. book places only in the hour before the shuttle, persons with disabilities should have priority, teachers with lectures should have some pre-assigned sets, etc.

A reputation system should be implemented – e.g. based on the Credence system – to recognize and reward good user's behavior. Likewise, users that reserve and to not appear should be penalized.

5. Secure sales site

Create an on-line sales website with areas of different access levels to allow sales or other online services. 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 service layer, application server layer, database layer. The network topology should be adequately designed for protection with security in mind.

6. 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 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 using a secure protocol. The computer has a service running that maintains the files decrypted only while it senses the phone; when the phone moves away, the directory is encrypted again.

Another idea is to use the mobile device for two factor authentication, i.e., the user should have the phone with her 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.

7. Electronic notary

A notary is a trusted third party thus providing additional trust for documents related to transactions e.g. a real-estate sale/purchase.

In this work, you should implement a digital notary. The project includes investigating information about what a digital notary is and does. Digital signatures and secure timestamping are relevant mechanisms that should be used, as well as careful certificate management. Studying the XAdES signature levels will also provide more insight into the technical challenges.

8. Secure messaging using SMS

SMS are still one of the most widely available messaging services.

Develop an app for smartphone (e.g., Android) that enables SMS exchanges in a secure manner (i.e., taking into account security requirements such as integrity, confidentiality and authentication, if possible) considering SMS messaging constraints. Techniques such as cipher text stealing can be used to ensure that the message limits are respected.

9. Secure child locator

Develop an app for smartphones (e.g., Android) that enables to track children using GPS (e.g., A-GPS) but assuring privacy and the secure tracking of children. Both the children and the responsible adult should be considered as users of the system.

Other tracking technologies can also be studied and considered for use.

10. Secure Smart Home

The Internet of Things is a technology trend where all useful devices can get connected to the Internet and allow for data collection and remote control. Some illustrative examples of such devices are smart locks, thermostats, smart appliances (e.g. fridge, washing machine).

In this work, you should consider how to implement the management console for a smart home system. Moreover, you should consider the secure design of the network (e.g., firewall) to control the data flows.

The privacy of the home owner should also be safeguarded. For example, it is necessary to ensure that the collected data is only shared outside the home with the explicit consent of the owner.