Protecting Privacy of Patients’ Electronic Health Records with the ABTTP Scheme

Raed M. Salih and Leszek T. Lilien (adviser), Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008

Introduction

The digital form of healthcare information is becoming more and more widespread in healthcare information systems, replacing “paper” medical records with Electronic Health Records (EHRs) or Electronic Medical Records.

The use of EHRs has a number of goals: (i) improving safety, quality, and efficiency of healthcare; (ii) reducing healthcare costs; and (iii) enriching healthcare research and public health monitoring.

However, facilitating data exchange via use of patients’ EHRs can increase privacy threats due to easier copying and dissemination of these EHRs among more entities (health insurance companies, federal or state government agencies, and research centers).

We define user privacy as a user’s right to protect and control her data. As a special subcase, patient privacy deals with data that include patient’s healthcare-related or personal (SSN or home address) data.

Problem Statement

Protecting patient privacy is a major challenge in healthcare information systems. Fig. 2 illustrates EHR dissemination as an example.

The hospital represents the main guardian for a patient’s EHR. The hospital might send a copy of the patient’s EHR to other guardians. For example, a clinic (Guardian 4 in Fig. 2) receives from the hospital (Guardian 1) a copy of a patient’s EHR. In turn, the clinic (Guardian 4) may distribute the patient’s EHR to multiple other guardians (like Guardians 5, 6, and 7).

Such EHR dissemination increases the risk of disclosing (or leaking) private patient’s information to unauthorized parties.

The Proposed Solution: ABTP

An active bundle (AB) is a software construct (Fig. 3), which bundles together the following three components: (i) sensitive data, (ii) metadata; and (iii) a virtual machine (VM).

The ABTP (Active Bundles with a Trusted Third Party) scheme combines active bundles with trusted third parties (TTPs). A TTP in ABTP maintains and provides to ABs information on the trust levels of visited hosts.

Sensitive data: data to be protected from privacy violations

Metadata: describing sensitive data and prescribing their use; including a privacy policy for the sensitive data, as well as the rules for AB dissemination

Virtual machine (VM): makes its AB active by controlling and managing how the AB behaves; the essential task of the VM is enforcement of privacy and other policies specified by metadata

1. EHR flow for a patient visiting a clinic for the first time. (Fig. 4)

a) AB’s verification activities:
   - Checking visited host’s trust level (Item 7 in Fig. 5/6)
   - Checking AB’s integrity (Item 10 in Fig. 5/6)
b) AB’s enforcement activities:
   - Evaporation destroys irretrievably portions of the EHR that the visited host is not authorized to access. (Item 2 in Fig. 6).
   - Apoptosis destroys irretrievably the entire AB in cases when: (i) a visited host’s trust level is not sufficient (Item 1 in Fig. 6), and (ii) integrity check fails (Item 2 in Fig. 6).
   - Full or partial EHR disclosure (Item 13/End 3 in Fig. 5/6).

Conclusion and Future Work

We propose a solution to protect privacy of patients’ EHRs. Our future work will focus on developing the Agent-Based Active Bundle (ABAB) scheme to protect EHRs in healthcare information systems, as well as patients’ privacy in healthcare cloud computing.