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.

Figure 1. Change from paper-based records to 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.

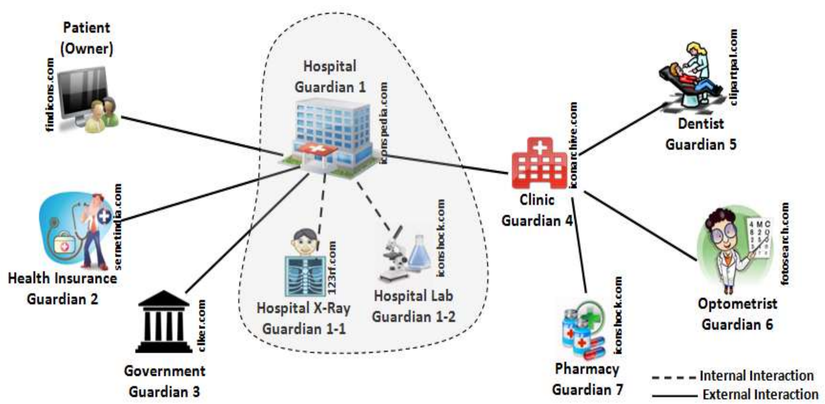

Figure 2. EHR dissemination example.

The Proposed Solution: ABTTP

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

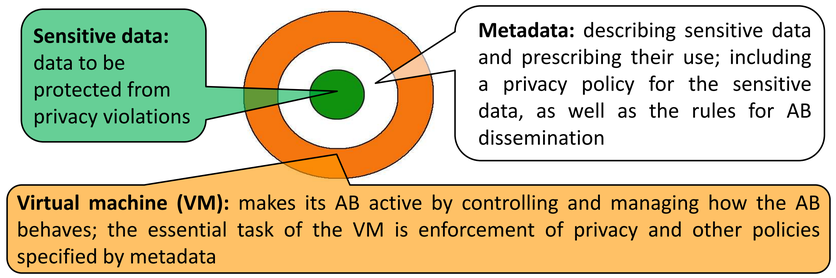

Figure 3. The structure of an active bundle.

The following simple scenario shows how ABTTPs can protect EHR for a patient visiting a clinic for the first time while his most up-to-date EHR is located in a hospital (cf. Figure 4):

1-5: The clinic EHR system (CES) searches for the patient 's EHR.
6-12: The CES asks the hospital EHR system (HES) for the patient's EHR since it is not in the CES database; HES searches for it and responds.
13-17: CES updates EHR in the CES database.
18-25: The patient meets a physician, who orders tests, and updates EHR in the CES database.
26-34: Tests results and diagnosis are obtained, and EHR is updated.
35-40: EHR update is sent to HES, and HES updates it in its database.

In the scenario, the EHRs exchanged between the clinic and the hospital (Steps 6,12, and 35) are protected by ABs.

The AB lifecycle consist of two phases:

1) *AB creation* (at HES): AB encapsulates its sensitive data, metadata, and the VM.
2) *AB enabling* (at CES): AB's VM performs these activities:

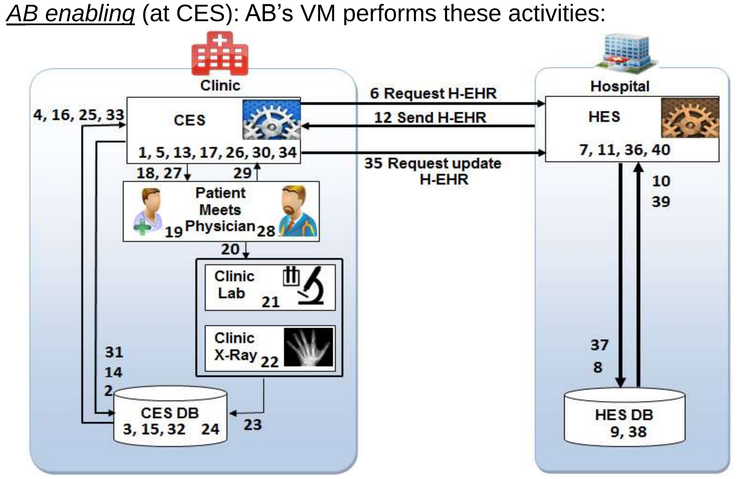

Figure 4. EHR flow for a patient visiting a clinic for the first time.

a) AB's verification activities:
- Checking visited host's trust level (Item *7/7* 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 *End 3* in Fig. 6),
- *Apoptosis* destroys irretrievably the *entire* AB in cases when: (i) a visited host 's trust level is not sufficient (Item *End 1* in Fig. 6), and (ii) integrity check fails (Item *End 2* in Fig. 6).
- Full or partial EHR disclosure (Item *13*/*End 3* in Fig. 5/6).

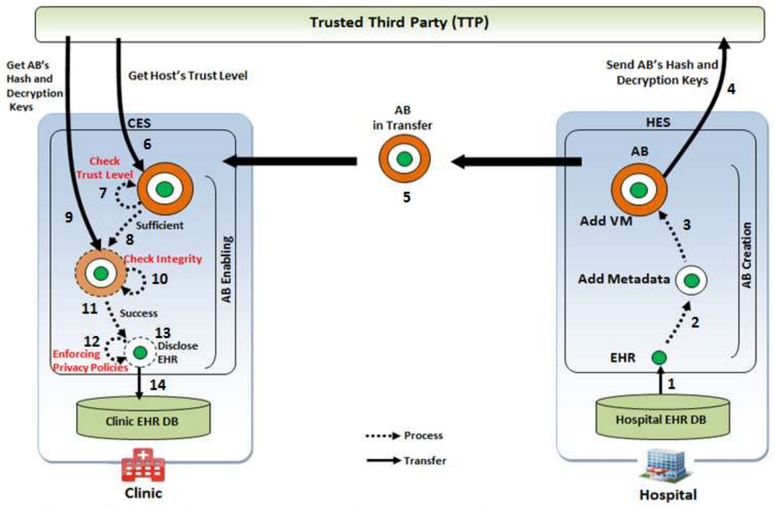

Figure 5. The AB lifecycle for a patient's EHR in the absence of an attack.

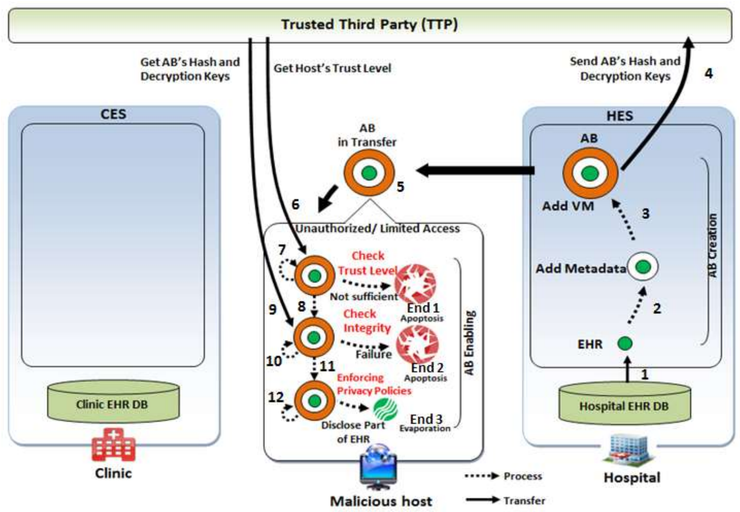

Figure 6. The AB lifecycle for a patient's EHR in the presence of an attack.

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.