Protecting Users' Privacy in Electronic Prescribing Systems with Active Privacy Bundles

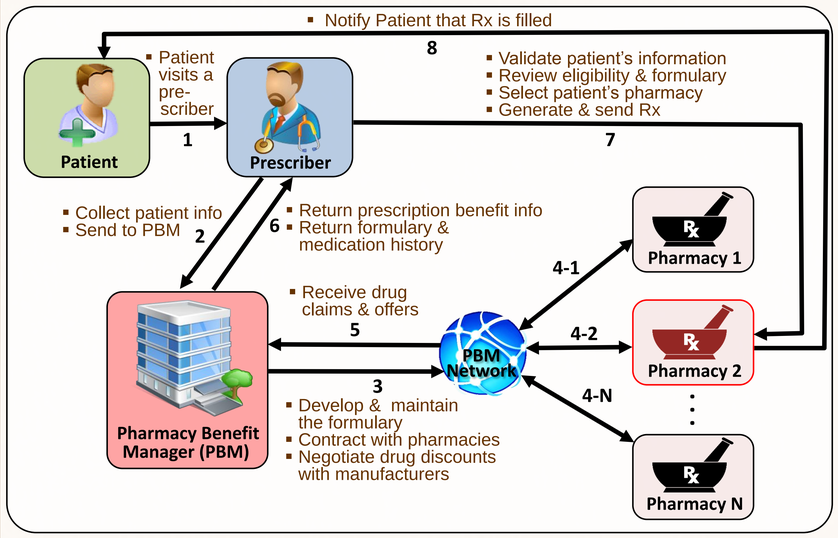
Raed M. Salih (Adviser: Dr. Leszek T. Lilien)
Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008

Introduction

➢ ***Electronic prescribing (e-Rx) systems*** — record and transmit *electronic prescriptions* among *prescribers, pharmacy benefit managers,* and *pharmacies*

- ***Prescriber*** — the subject (e.g. a physician) who writes prescriptions (Rx) for a patient
- ***Pharmacy benefit manager*** (***PBM***) — a third-party administrator responsible for developing and maintaining the formulary, contracting with pharmacies, and negotiating discounts and rebates with drug manufacturers
  - Also responsible for processing and paying prescription drug claims

➢ **The current *e-prescribing workflow***

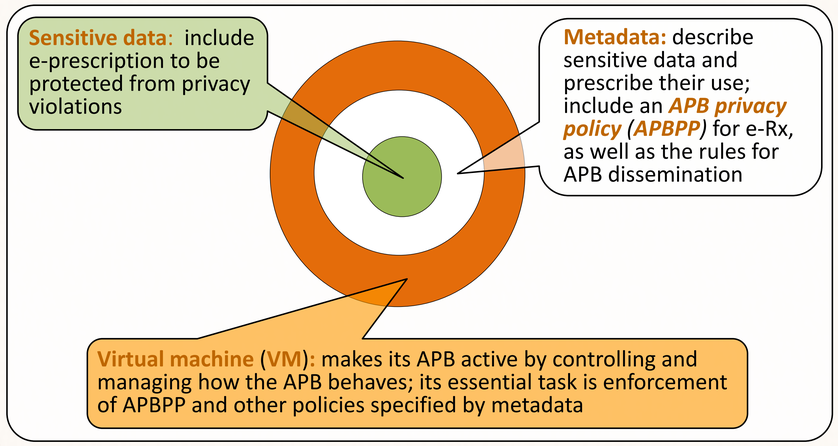


➢ ***User privacy*** — a user's right to control what information she reveals about herself, and who can access that information

- ***Patient privacy*** (a special subcase of user privacy) — deals with data that are or include a patient's healthcare-related data (incl. Rx data)

➢ ***An active privacy bundle (APB)***

- A software construct



Motivation and Problem Statement

➢ **Data privacy in an e-Rx system** — a critical challenge

- Users must be sure that the e-Rx system does not disseminate or share their private data (e.g., name, home address, names of mental illness medications) to unauthorized entities
- Users do not know who/what controls their data physically
  - Do not know where data are sent in an e-Rx network, and who manages them
  - Some companies profit from selling physician's prescribing routines to pharmaceutical companies

➢ ***Security* = confidentiality + integrity + availability (CIA)**

- This is a classical definition of security

➢ **Problem Statement**

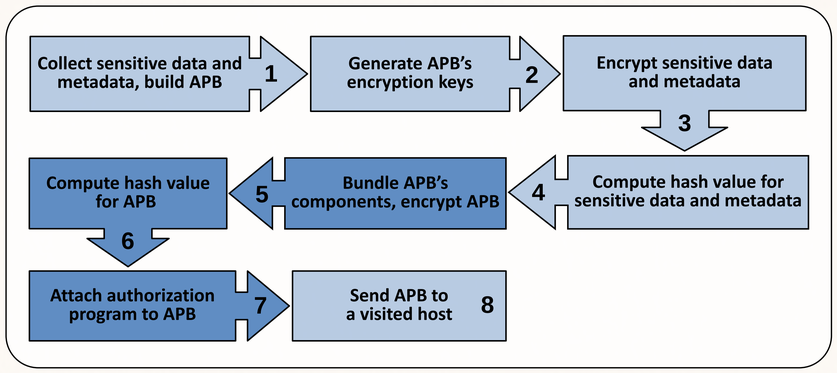
- Assure that an e-Rx system provides all 3 components of security
- Assure that private data are not disclosed to unauthorized parties by an e-Rx system

The Proposed Solution

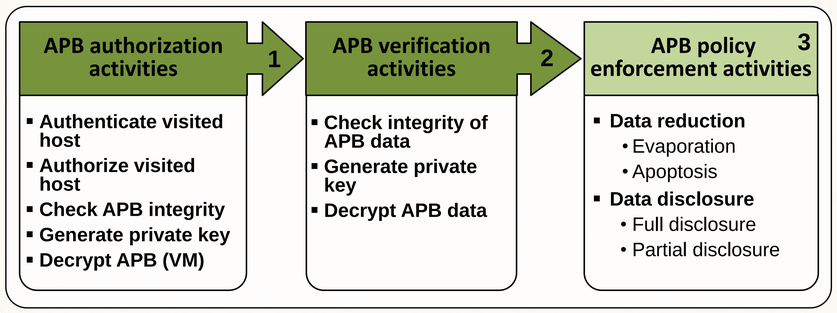
➢ **Modifications of the Active Privacy Bundle**

- Modified two **APB execution phases**

1) ***APB creation***: APB constructed in user space with APB creator software (either automatically or interactively)
   - The APB creation **steps**
     – Darker color indicates modified steps

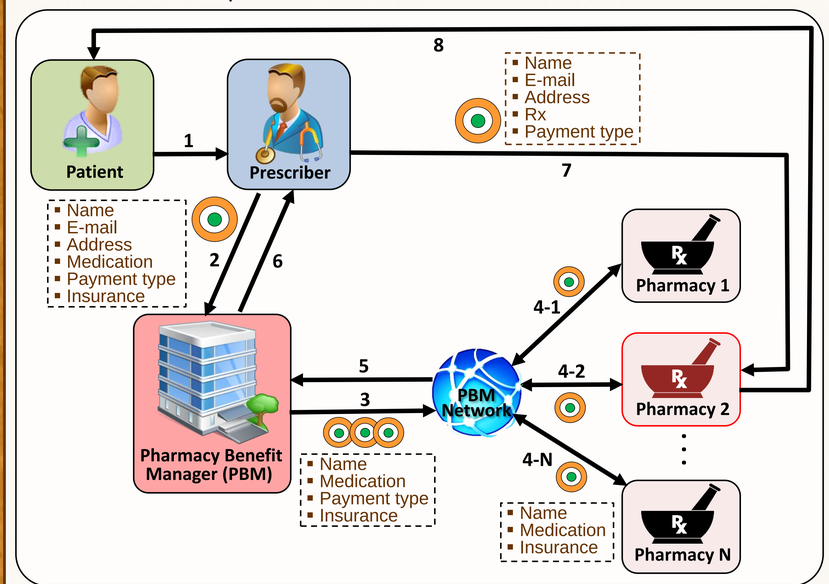


2) ***APB enabling:*** APB automatically enabled on the visited host
   - The APB enabling **steps**
     – Darker color indicates modified steps



➢ **The e-prescribing workflow with APBs**

- Analogous to „The current e-prescribing workflow" but ...
  - Activities (drawn as arrows) are not labeled below
  - Contents of APB data are described in the broken-line boxes shows
- Different APB sizes — due mostly to different sizes of APB's data and metadata components



➢ **Requirements for APB creation**

- Using domain names, addresses & associated certificates
- Key derivation
- Key stretching
- Detached signatures

➢ **Requirements for APB enabling**

- Message disposition notification (MDN)
  - Provides indications of message delivery (read or discarded) to the sender
- Using certificate authority (e.g., X509)
- Certificate discovery
  - Through DNS and LDAP
- Trust verification

➢ **Salient Solution Features**

- Attribute-based access control (ABAC)
- No need for trusted third party (TTP)

Work Status and Future Work

➢ **Status**

- Nearing completion of a pilot APB implementation
- Developing ***active privacy bundles with multi-agent system*** (***APB-MAS***)

➢ **Future work**

- Adding to APB privacy policy inclusion
- Adding to APB privacy policy verification
- Adding to APB automatic negotiation of privacy policies
- Using APB-MA for protecting patients' privacy in e-Rx systems