Declarative Privacy Policy

Peifung E. Lam[1], John C. Mitchell[1], Andre Scedrov[2], Sharada Sundaram[3], Frank Wang[1]

[1]Stanford University, [2]University of Pennsylvania, [3]Symantec Corporation

Problem

The emergence of Electronic Health Records with Health Information Exchange holds promise for more effective and affordable health care.

However, the regulations and policies surrounding Electronic Health Information are complex, making compliance very difficult. Therefore, there is a great push to increase awareness and enhance systems to allow for secure storage and exchange of this information.

Approach

- Use logic programs, such as Prolog, to formalize privacy laws (HIPAA).
- A finite model of a representative hospital can illustrate how the law applies in all scenarios.
- Generate an access control policy using this formalization.
- Apply attribute-based encryption (ABE) to encrypt and decrypt data to allow access only to individuals who have the correct credentials using generated policy.

Applications

- Healthcare organizations can automate policy compliance.
- Finite model can support new education and policy development and refinement.
- System allows any policy-encrypted data to be placed on untrusted cloud servers, such as Dropbox (not just medical data).

1 – Encode HIPAA Law

HIPAA Law

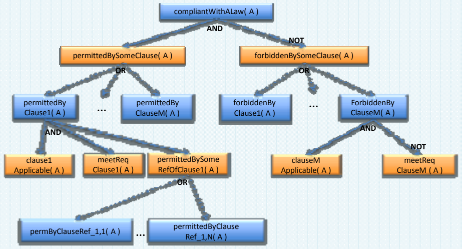
§ 164.502 Uses and disclosures of protected health information: general rules.
(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.
(1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:
(i) To the individual;
(ii) For treatment, payment, or health care operations, as permitted by and in compliance with §164.506;
(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §164.502(b), §164.514(d), and §164.530(c) with respect to such otherwise permitted

...010110...

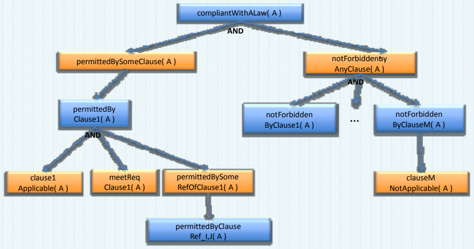
```
>|
%%Standard rules for "uses and disclosures"
permitted_by_164_502_a(A) :-
  is_from_coveredEntity(A),
  is_phi(A),
  (permitted_by_160_C(A);
  permitted_by_164_502_a_1(A);
  required_by_164_502_a_2(A)).

permitted_by_164_502_a_1(A):-
  permitted_by_164_502_a_1_i(A);
  permitted_by_164_502_a_1_ii(A);
  permitted_by_164_502_a_1_iii(A);
  permitted_by_164_502_a_1_iv(A);
  permitted_by_164_502_a_1_v(A);
  permitted_by_164_502_a_1_vi(A).
```

2 - Compute Policy Graph

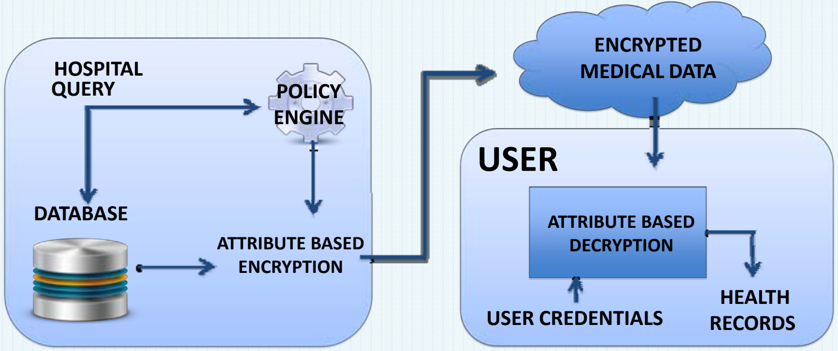
Compliance Tree



Search Tree


compliantWithALaw(A)
AND
permittedBySomeClause(A)
notForbiddenBy AnyClause(A)
AND
permittedBy Clause1(A)
notForbidden ByClause1(A)
...
notForbidden ByClauseM(A)
AND
clause1 Applicable(A)
meetReq Clause1(A)
permittedBySome RefOfClause1(A)
clauseM NotApplicable(A)
permittedByClause Ref_I,J(A)

3 – Encrypt Healthcare Record



HOSPITAL QUERY

POLICY ENGINE

DATABASE

ATTRIBUTE BASED ENCRYPTION

ENCRYPTED MEDICAL DATA

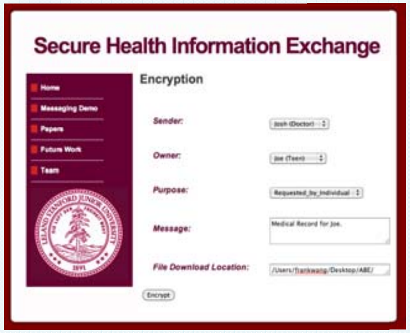
USER

ATTRIBUTE BASED DECRYPTION

USER CREDENTIALS

HEALTH RECORDS

Prototype



Secure Health Information Exchange

Encryption

Sender: Josh (Doctor)

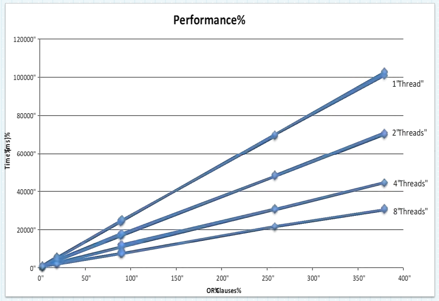
Owner: Joe (Teen)

Purpose: Requested_by_Individual

Message: Medical Record for Joe.

File Download Location: /Users/frankwang/Desktop/ABE/

Performance



For a given policy, more subpolicies, represented as OR-clauses, lead to longer encryption times. Decryption depends on the ordering of subpolicies.

Future Work

- Develop direct support for parameterized roles in ABE.
- Unique identifiers needed for attributes (i.e. define specific doctors in relation to specific patients).
- Declarative Privacy Policy: Finite Models and Attribute-Based Encryption. P. Lam, J. Mitchell, A. Scedrov, S. Sundaram, and F. Wang. IHI 2012.
- We thank Ellick Chan for his help with design and implementation.