INFSCI 2955 Special Topics on Security Assured Health Informatics

Attribute-based Access Control in Health Informatics Domain

Runhua Xu
Department of Informatics and Networked Systems
School of Computing and Information
University of Pittsburgh
runhua.xu@pitt.edu

Outline

- Access Control Review
  - *From DAC/MAC/RBAC to ABAC*
- Attribute-based Access Control
  - *Conventional ABAC*
  - *Crypto-based ABAC*
- Attribute-based Encryption
  - *From PKC to ABE*
  - *ABE Introduction*
- Applications in Health Informatics Domain

Access Control Review

from DAC/MAC/RBAC to ABAC

Security Terms

Authentication

“Who are you”

hat

hat you have

hat you are

Authorization

“What can you access”

ccess ontrol

Accounting

“What you have accessed”

Auditing

“Monitor/Verify what you have accessed”

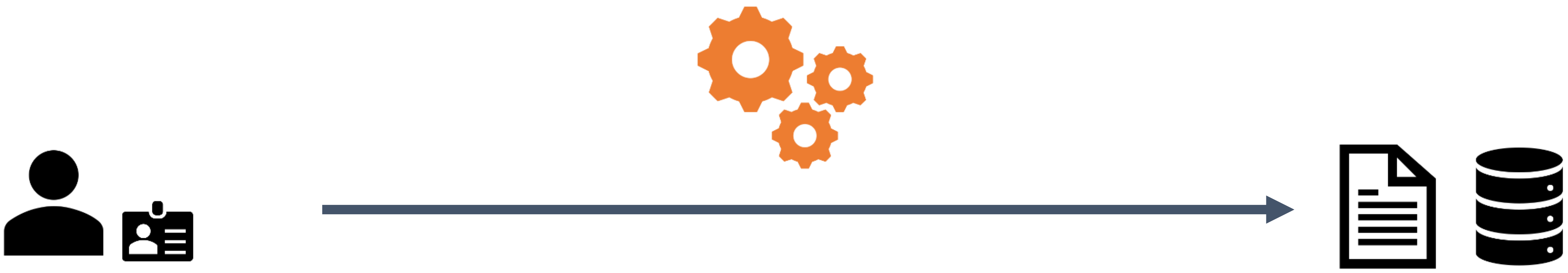
Cryptography

“Secure Communication”

onfidentiality

.ntegrity

Access Control



Access Control Mechanism

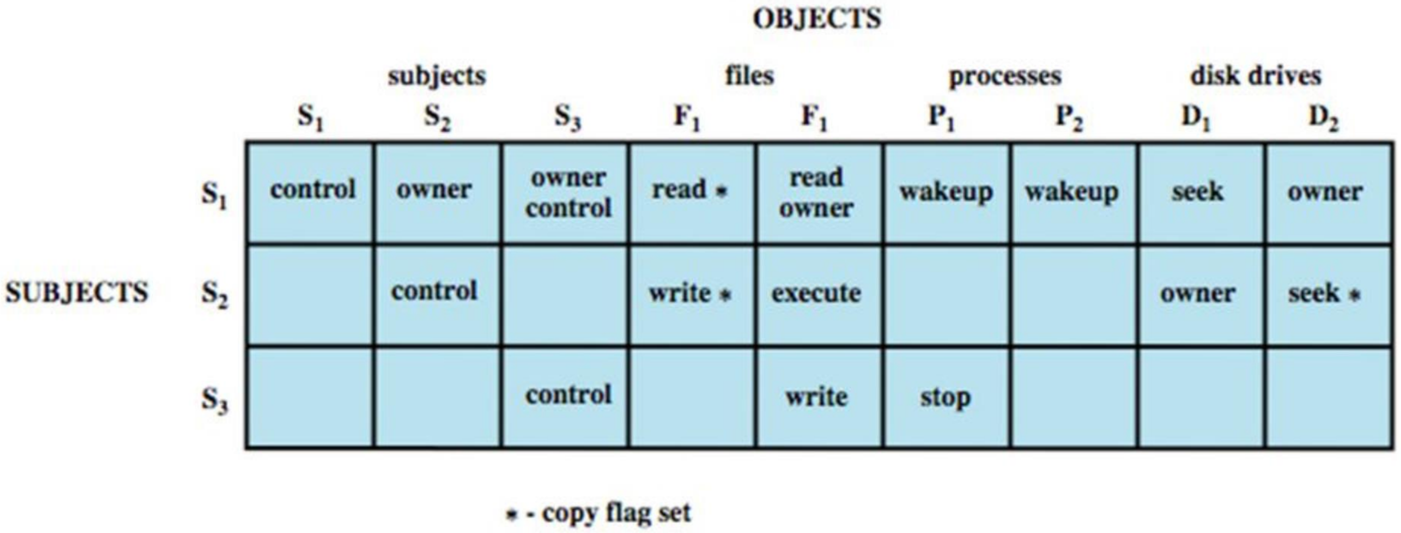
Subject
e.g., authenticated users

Object
e.g., file, data, resouruce

> *" A logical component that serves to*
> *i) receive the access for an Object from a Subject*
> *ii) and decide and enforce the access decision "*
>
> *a definition from NIST*

Discretionary Access Control

- DAC Model
  - *Owner's responsibility to define rights of each subject on the object*
  - *Key properties*
    - Decentralized – discretion of each individual owner
    - Permission rule are attached to object



		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_1	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

* - copy flag set

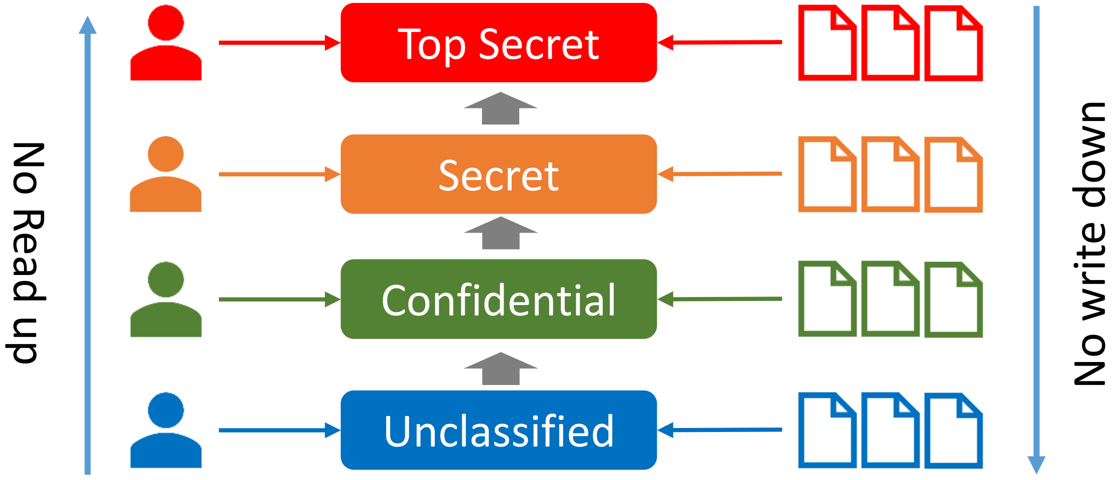
Typical example: HRU model

Access Control Matrix example

Protection State is defined as
a triplet: (S, O, A)

Mandatory Access Control

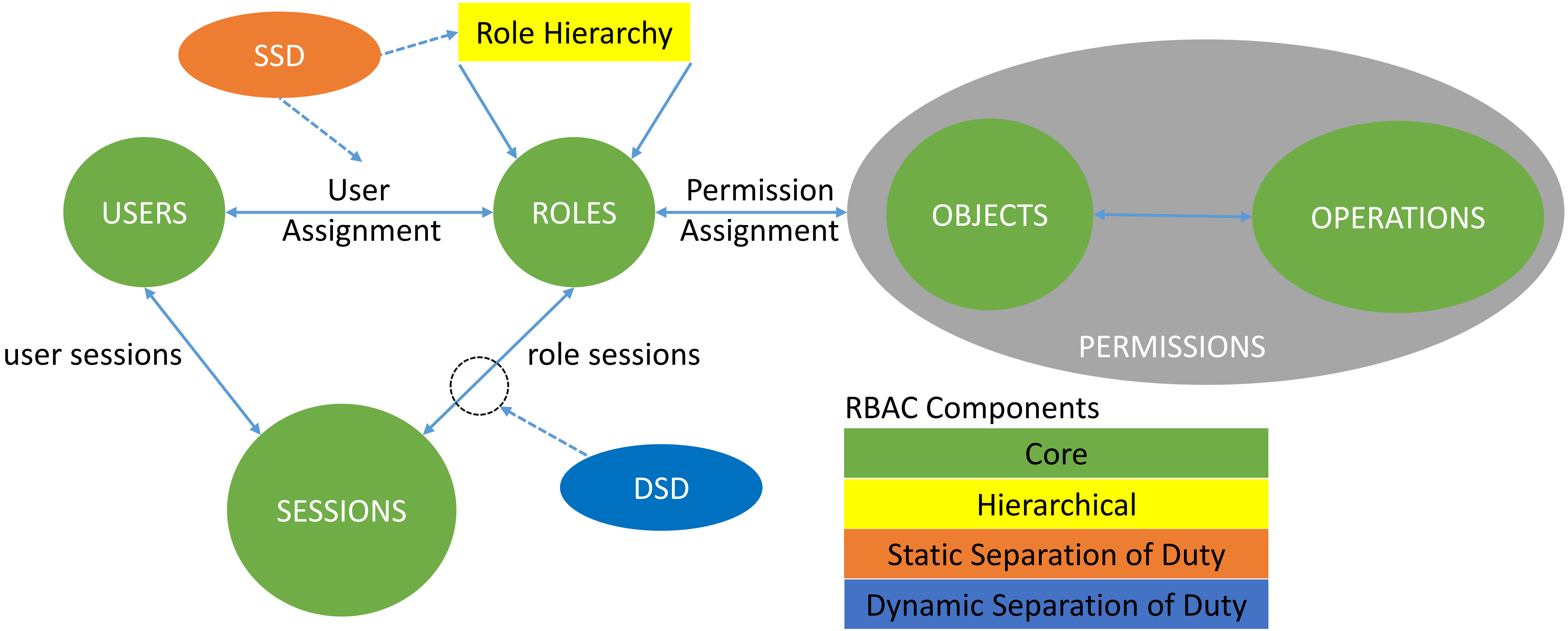
- MAC Model
  - *Access decision are take and enforced by the security system*
  - *Key properties*
    - Centralized
    - Most restrictive model – military style model
    - Adopted in highly sensitive application scenario



Typical example:
Bell-LaPadula, BIBA, Chinese-Wall etc.

Role-based Access Control

Subjects are assigned **Roles** which have predefined associated **Permissions** to perform certain **Operation** on the **Objects**.



SSD

Role Hierarchy

USERS

User Assignment

ROLES

Permission Assignment

OBJECTS

OPERATIONS

PERMISSIONS

user sessions

role sessions

SESSIONS

DSD

RBAC Components

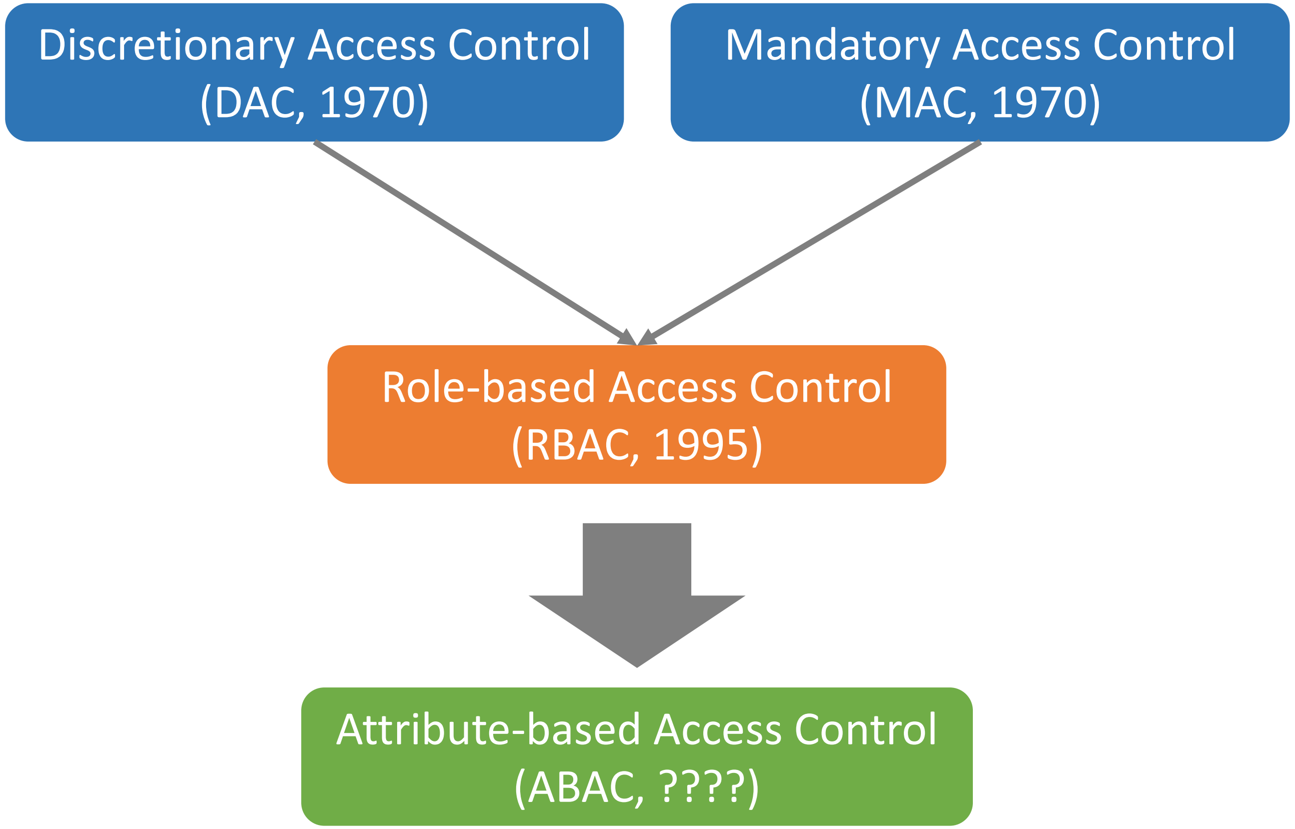
🟩 Core

🟨 Hierarchical

🟧 Static Separation of Duty

🟦 Dynamic Separation of Duty

Access Control Review



Discretionary Access Control (DAC, 1970)

Mandatory Access Control (MAC, 1970)

Role-based Access Control (RBAC, 1995)

Attribute-based Access Control (ABAC, ????)

Fixed Policy

Administration Driven

Enterprise Oriented

Flexible Policy

Automated Adaptive

Beyond Enterprise

SO FAR: numerous other models, but only 3 successes

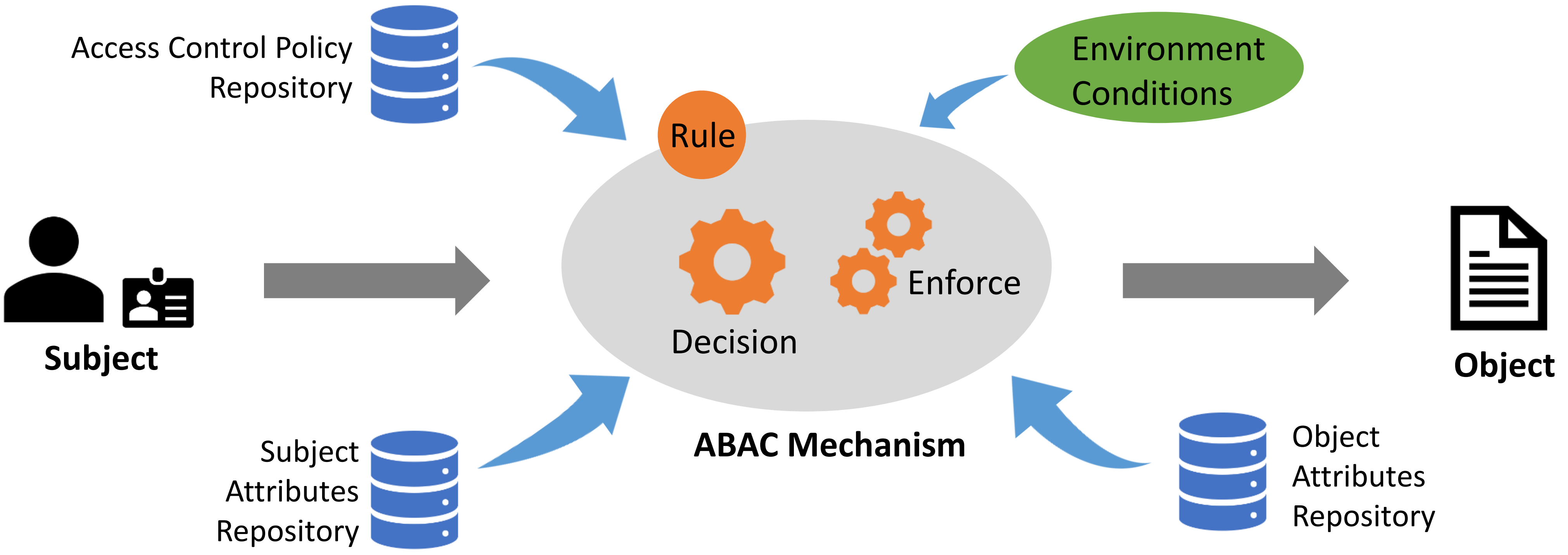
Attribute-based Access Control

from Conventional ABAC to Crypto-based ABAC

Attribute-based Access Control

"An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions"

-- a definition from NIST


Access Control Policy Repository
Environment Conditions
Rule
Enforce
Decision
Subject
Object
ABAC Mechanism
Subject Attributes Repository
Object Attributes Repository

Why ABAC – RBAC/DAC/MAC vs. ABAC

+

ABAC model

- ***Dynamic*** *– access control permissions are evaluated at the time of actual request is made*
- ***Contextual*** *– environmental conditions may be considered*
- ***Fine grained*** *– attribute based, so detailed rules can be formed*

Traditional AC model

- ***Static*** *– access control permissions are predetermined*
- ***Limited context*** *– environmental conditions are not fully considered (time, location, environmental roles, etc.)*
- ***Coarse*** *– classification is done at high abstraction level*

−

Why ABAC – An Intuitive Example

Access Policy:
Managers of the auditing department in Pittsburgh can inspect the financial reports from the current financial year within office hours.

What will RBAC do with this case? -- role explosion

Subject

- Identity
- Position
- Location
- Department

Object

- Type
- Date
- Label

Environment

- Device Type
- Timestamp
- System State

Action

- Action Type
- Amount

Managers of the auditing department in Pittsburgh can inspect the financial reports from the current financial year within office hours.

Why ABAC – Key Features of ABAC

Access Policy:

Managers of the auditing department in Pittsburgh can inspect the financial reports from the current financial year within office hours.

Subject

Object

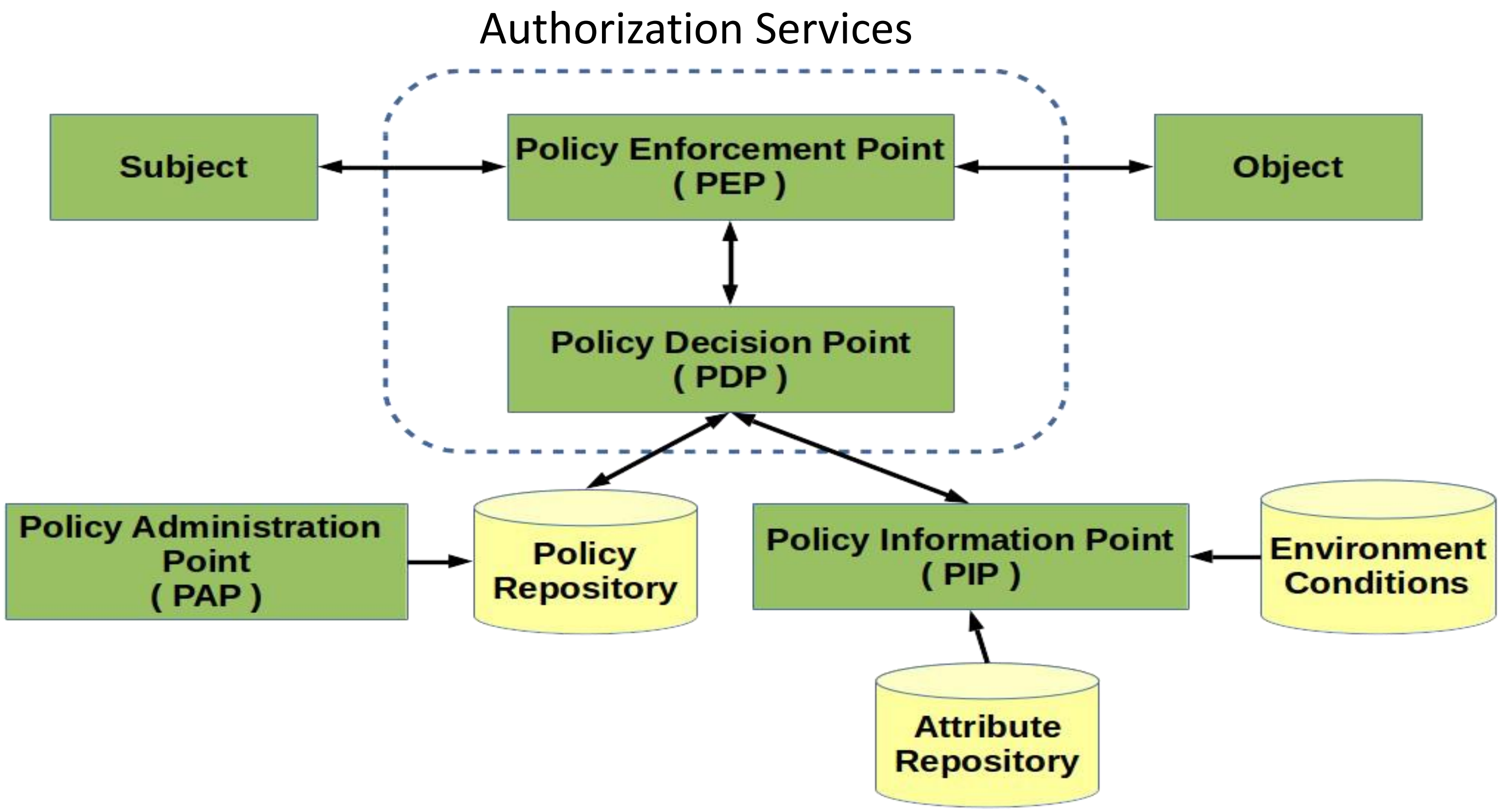
Environment

Action

- Fine-grained access control
- Context-aware access control
- Dynamic access control

Conventional ABAC Framework

A framework of ABAC mechanism

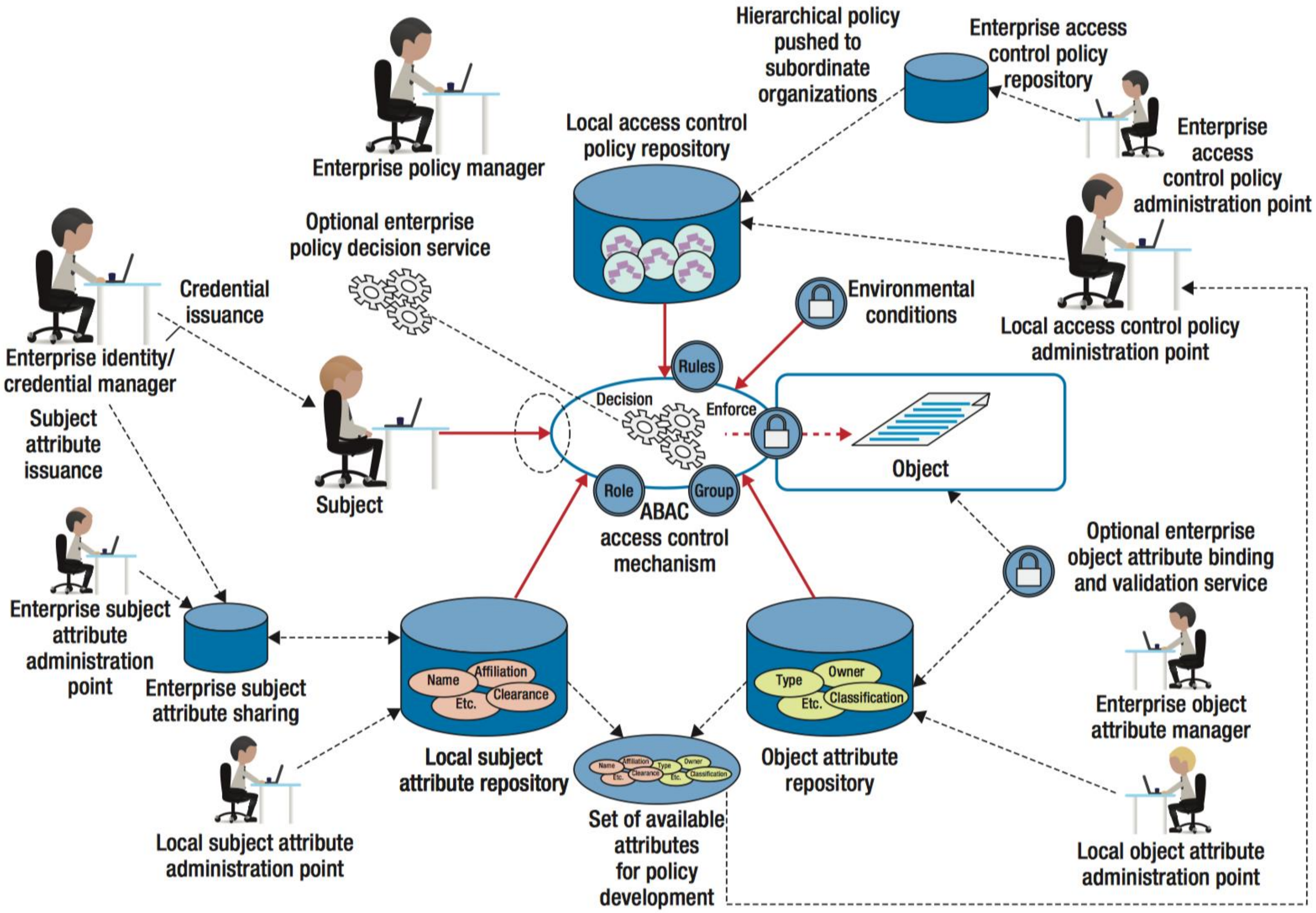

Authorization Services
Subject
Policy Enforcement Point (PEP)
Object
Policy Decision Point (PDP)
Policy Administration Point (PAP)
Policy Repository
Policy Information Point (PIP)
Environment Conditions
Attribute Repository

Note that

PEP, PDP, PAP & PIP may be on same machine or may be physically separated

Extended the architecture of RBAC

Conventional ABAC Framework Scenario

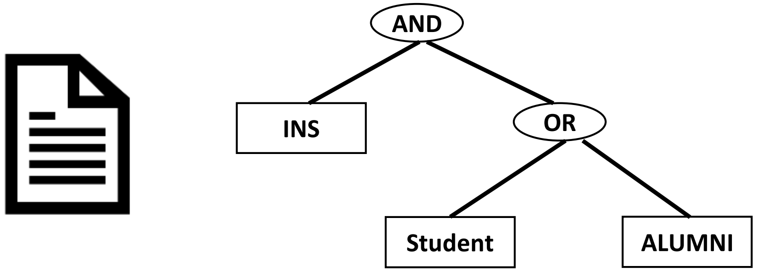

Hierarchical policy pushed to subordinate organizations
Enterprise access control policy repository
Enterprise access control policy administration point
Enterprise policy manager
Local access control policy repository
Optional enterprise policy decision service
Credential issuance
Enterprise identity/ credential manager
Subject attribute issuance
Environmental conditions
Local access control policy administration point
Rules
Decision
Enforce
Object
Subject
Role
Group
ABAC access control mechanism
Optional enterprise object attribute binding and validation service
Enterprise subject attribute administration point
Enterprise subject attribute sharing
Name
Affiliation
Clearance
Etc.
Type
Owner
Classification
Etc.
Enterprise object attribute manager
Local subject attribute repository
Object attribute repository
Set of available attributes for policy development
Local subject attribute administration point
Local object attribute administration point

V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, “Attribute-based access control,” Computer (Long. Beach. Calif)., vol. 48, no. 2, pp. 85–88, 2015.

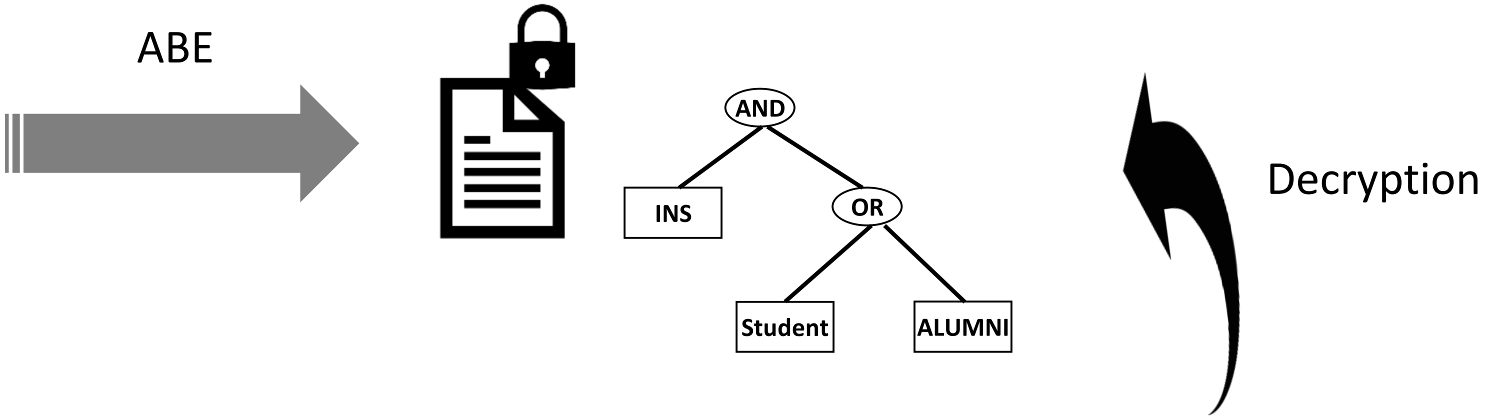
Crypto-based ABAC – Attribute-based Encryption

An intuitive example

Anyone who is student or alumni from INS department can access the file.



$\mathcal{P} = INS\ AND\ (Student\ OR\ Alumni)$



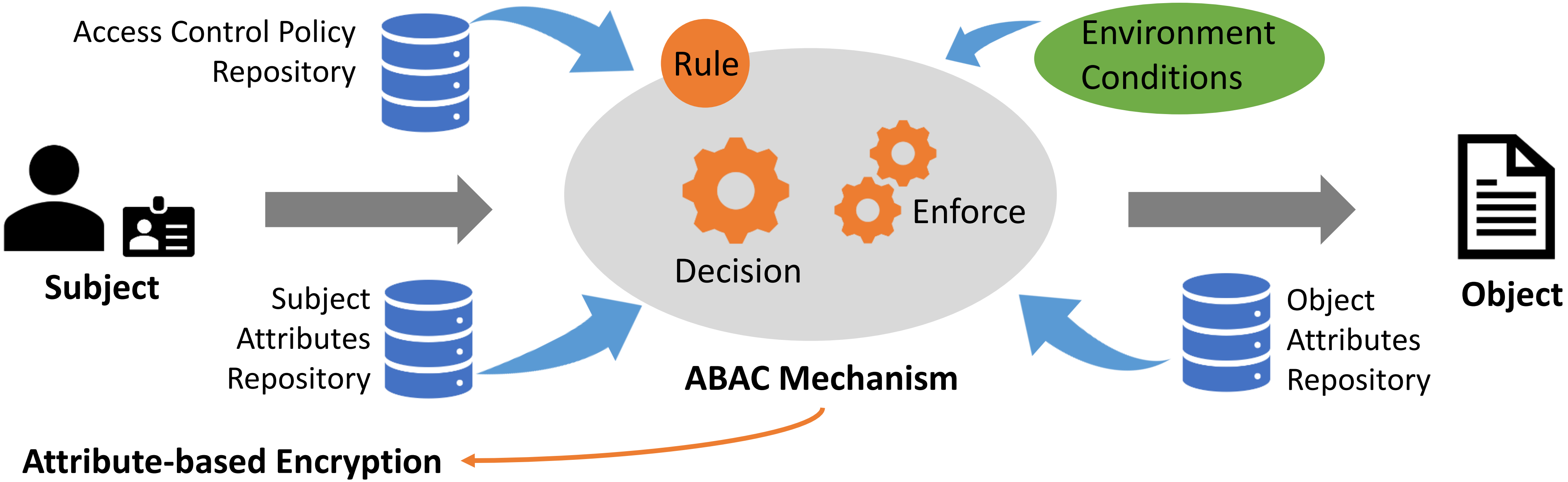
Attr: Student, DINS, Male, Age = 18

Attr: Student, CS, Male, Age = 20

Attr: Alumni, CS, Female, Age = 30

Combination of cryptography & access control

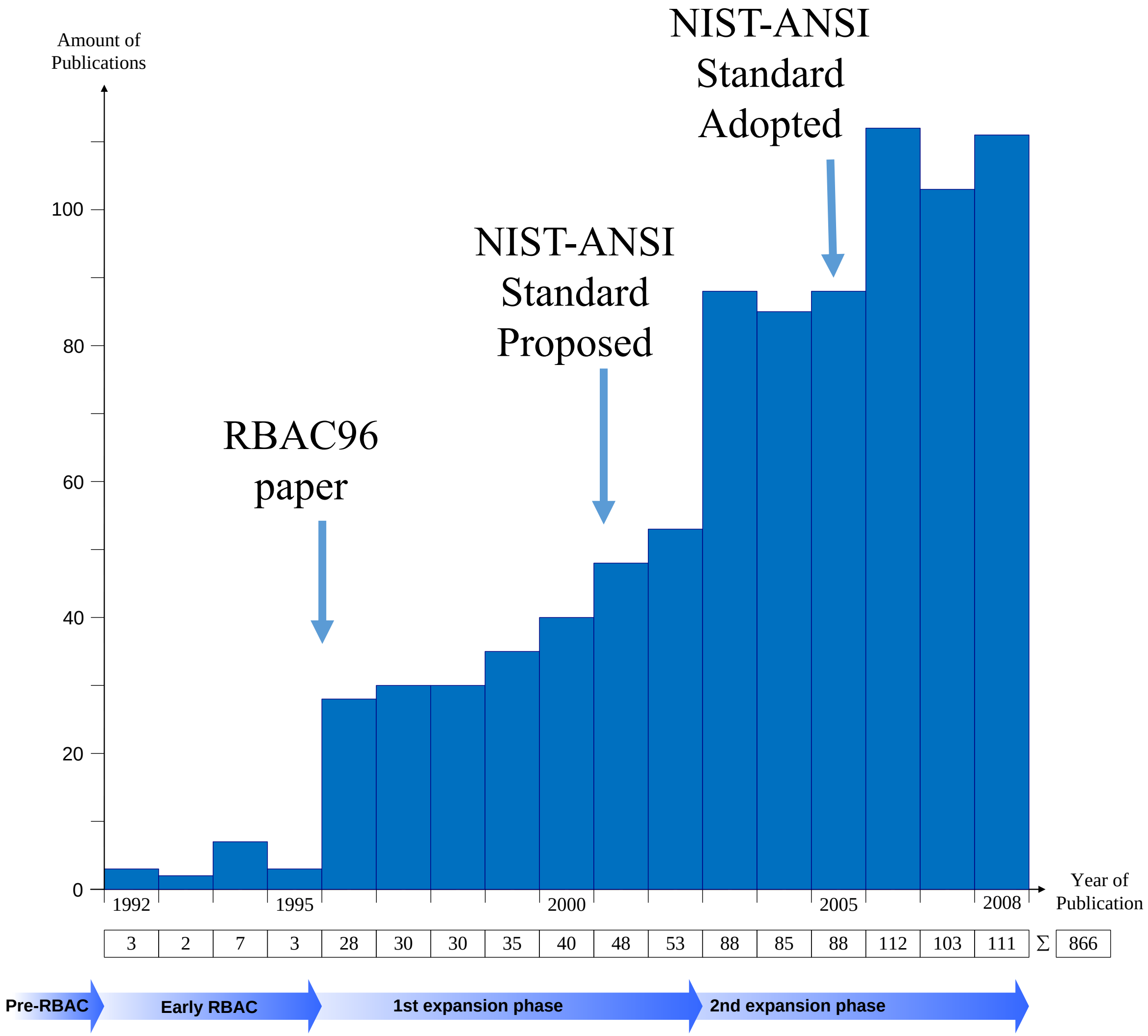
ABE – from the ABAC perspective



Access Control Policy Repository
Rule
Environment Conditions
Subject
Decision
Enforce
Object
Subject Attributes Repository
Object Attributes Repository
ABAC Mechanism
Attribute-based Encryption

- Decision/Enforce -- PIP/PAP → Third Party Authority, PDP/PEP → build-in automatically
- Access Policy -- owner defined access policy or access attribute set
- Subject’s Attributes -- CP-ABE, subject has attribute set
- Object’s Attributes -- KP-ABE, object is attached with attribute set
- Environment Conditions -- environment condition can be involved in access policy
- Additional Feature: Confidentiality

ABAC Prospect



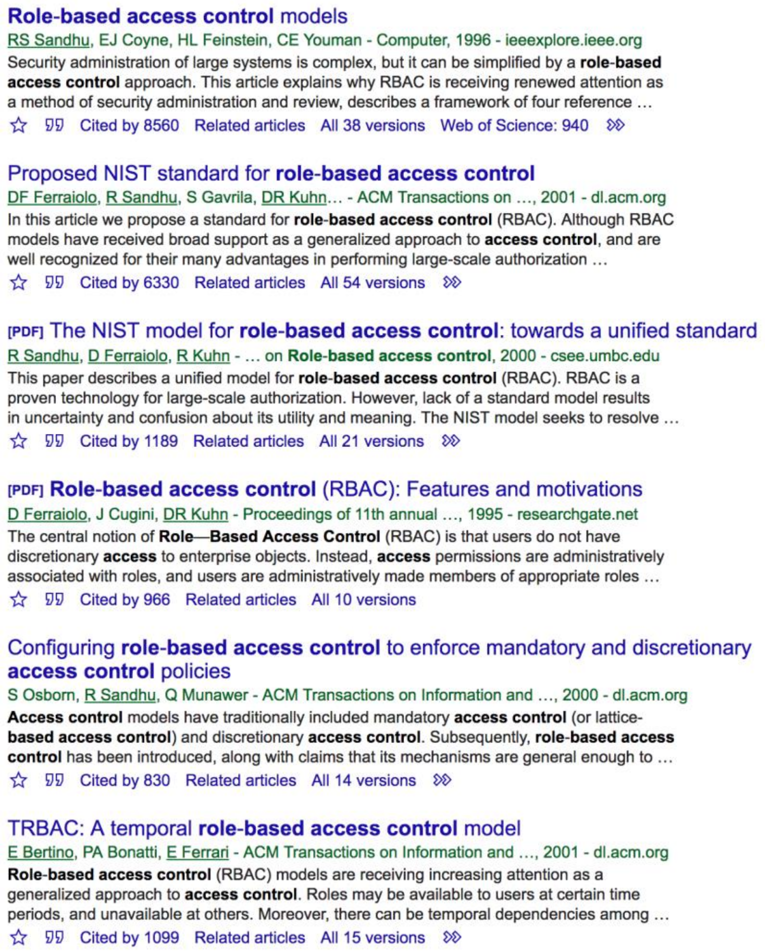
How about Attribute-based Access Control ?

Maybe still in pre-/early phase

* Ludwig Fuchs, Gunther Pernul and Ravi Sandhu, Roles in Information Security-A Survey and Classification of the Research Area, Computers & Security, Volume 30, Number 8, Nov. 2011, pages 748-76

Crypto-based ABAC Prospect

A perspective of research citations (Check at Sept. 17 2018)



Role-based access control models
RS Sandhu, EJ Coyne, HL Feinstein, CE Youman - Computer, 1996 - ieeexplore.ieee.org
Security administration of large systems is complex, but it can be simplified by a **role-based access control** approach. This article explains why RBAC is receiving renewed attention as a method of security administration and review, describes a framework of four reference …
☆ ❞ Cited by 8560 Related articles All 38 versions Web of Science: 940 »

Proposed NIST standard for **role-based access control**
DF Ferraiolo, R Sandhu, S Gavrila, DR Kuhn… - ACM Transactions on …, 2001 - dl.acm.org
In this article we propose a standard for **role-based access control** (RBAC). Although RBAC models have received broad support as a generalized approach to **access control**, and are well recognized for their many advantages in performing large-scale authorization …
☆ ❞ Cited by 6330 Related articles All 54 versions »

[PDF] The NIST model for **role-based access control**: towards a unified standard
R Sandhu, D Ferraiolo, R Kuhn - … on **Role-based access control**, 2000 - csee.umbc.edu
This paper describes a unified model for **role-based access control** (RBAC). RBAC is a proven technology for large-scale authorization. However, lack of a standard model results in uncertainty and confusion about its utility and meaning. The NIST model seeks to resolve …
☆ ❞ Cited by 1189 Related articles All 21 versions »

[PDF] **Role-based access control** (RBAC): Features and motivations
D Ferraiolo, J Cugini, DR Kuhn - Proceedings of 11th annual …, 1995 - researchgate.net
The central notion of **Role—Based Access Control** (RBAC) is that users do not have discretionary **access** to enterprise objects. Instead, **access** permissions are administratively associated with roles, and users are administratively made members of appropriate roles …
☆ ❞ Cited by 966 Related articles All 10 versions

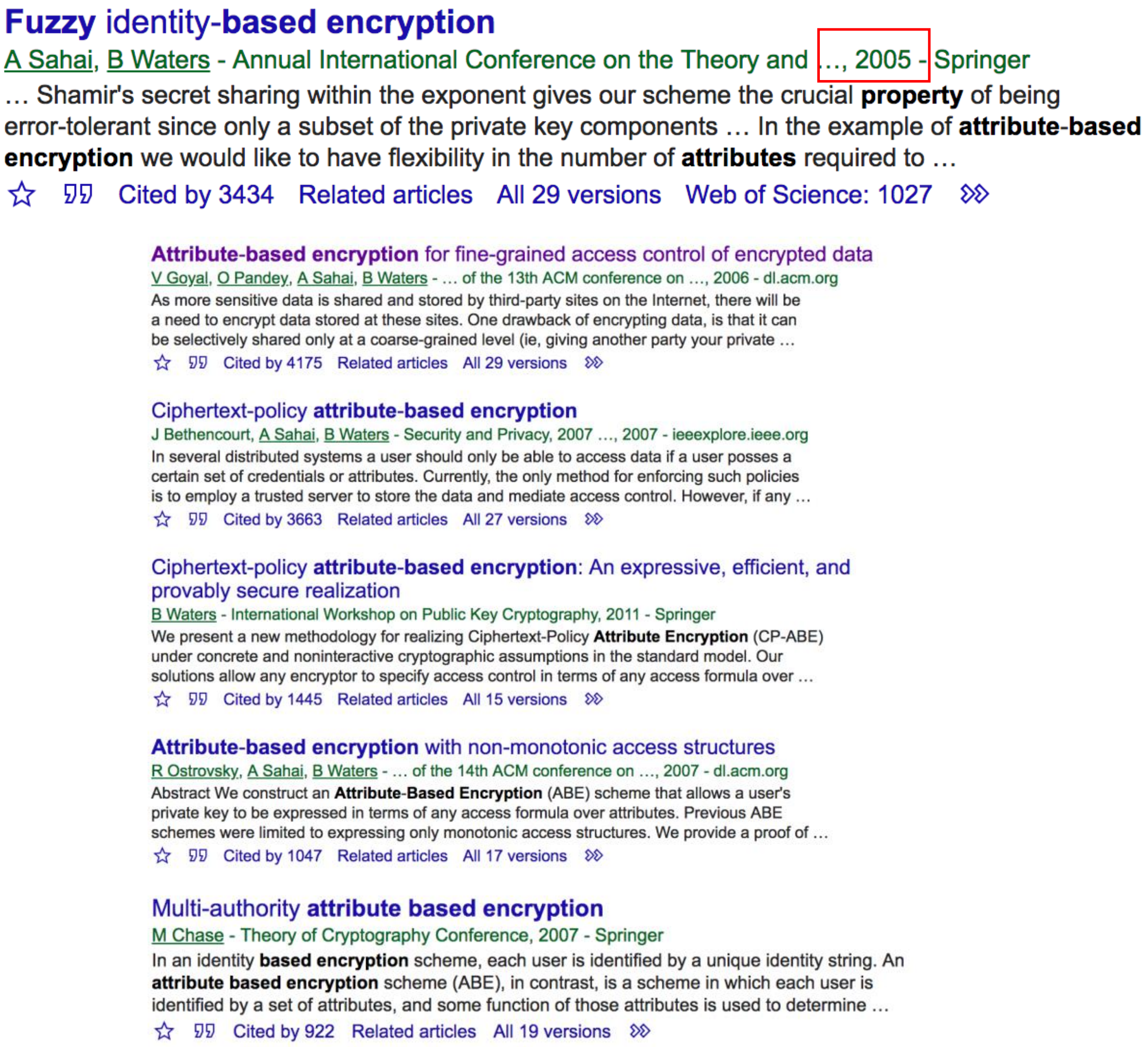
Configuring **role-based access control** to enforce mandatory and discretionary **access control** policies
S Osborn, R Sandhu, Q Munawer - ACM Transactions on Information and …, 2000 - dl.acm.org
Access control models have traditionally included mandatory **access control** (or lattice-based **access control**) and discretionary **access control**. Subsequently, **role-based access control** has been introduced, along with claims that its mechanisms are general enough to …
☆ ❞ Cited by 830 Related articles All 14 versions »

TRBAC: A temporal **role-based access control** model
E Bertino, PA Bonatti, E Ferrari - ACM Transactions on Information and …, 2001 - dl.acm.org
Role-based access control (RBAC) models are receiving increasing attention as a generalized approach to **access control**. Roles may be available to users at certain time periods, and unavailable at others. Moreover, there can be temporal dependencies among …
☆ ❞ Cited by 1099 Related articles All 15 versions »

18974

VS.

11389



Fuzzy identity-**based encryption**
A Sahai, B Waters - Annual International Conference on the Theory and …, 2005 - Springer
… Shamir's secret sharing within the exponent gives our scheme the crucial **property** of being error-tolerant since only a subset of the private key components … In the example of **attribute-based encryption** we would like to have flexibility in the number of **attributes** required to …
☆ ❞ Cited by 3434 Related articles All 29 versions Web of Science: 1027 »

Attribute-based encryption for fine-grained access control of encrypted data
V Goyal, O Pandey, A Sahai, B Waters - … of the 13th ACM conference on …, 2006 - dl.acm.org
As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (ie, giving another party your private …
☆ ❞ Cited by 4175 Related articles All 29 versions »

Ciphertext-policy **attribute-based encryption**
J Bethencourt, A Sahai, B Waters - Security and Privacy, 2007 …, 2007 - ieeexplore.ieee.org
In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any …
☆ ❞ Cited by 3663 Related articles All 27 versions »

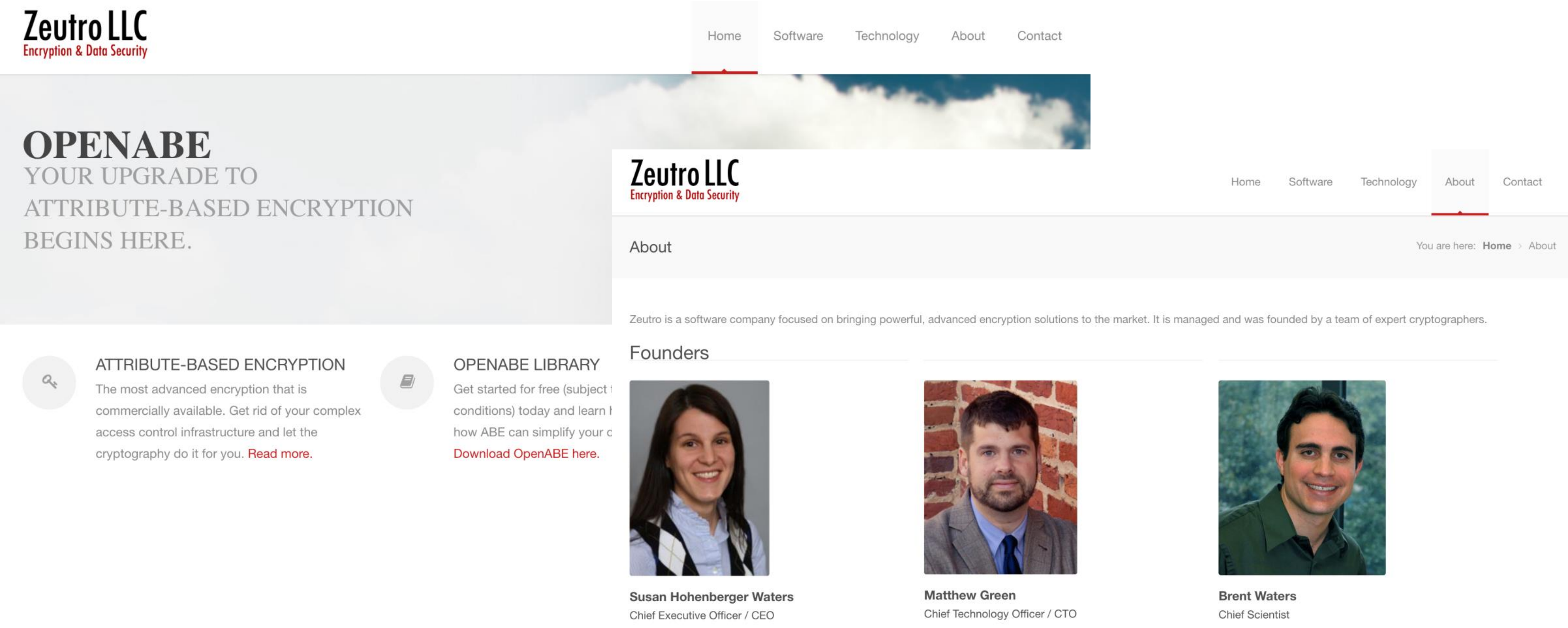
Ciphertext-policy **attribute-based encryption**: An expressive, efficient, and provably secure realization
B Waters - International Workshop on Public Key Cryptography, 2011 - Springer
We present a new methodology for realizing Ciphertext-Policy **Attribute Encryption** (CP-ABE) under concrete and noninteractive cryptographic assumptions in the standard model. Our solutions allow any encryptor to specify access control in terms of any access formula over …
☆ ❞ Cited by 1445 Related articles All 15 versions »

Attribute-based encryption with non-monotonic access structures
R Ostrovsky, A Sahai, B Waters - … of the 14th ACM conference on …, 2007 - dl.acm.org
Abstract We construct an **Attribute-Based Encryption** (ABE) scheme that allows a user's private key to be expressed in terms of any access formula over attributes. Previous ABE schemes were limited to expressing only monotonic access structures. We provide a proof of …
☆ ❞ Cited by 1047 Related articles All 17 versions »

Multi-authority **attribute based encryption**
M Chase - Theory of Cryptography Conference, 2007 - Springer
In an identity **based encryption** scheme, each user is identified by a unique identity string. An **attribute based encryption** scheme (ABE), in contrast, is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine …
☆ ❞ Cited by 922 Related articles All 19 versions »

Crypto-based ABAC Prospect

An startup focuses on advanced encryption solutions, e.g., ABE



Zeutro LLC
Encryption & Data Security

OPENABE
YOUR UPGRADE TO
ATTRIBUTE-BASED ENCRYPTION
BEGINS HERE.

ATTRIBUTE-BASED ENCRYPTION

The most advanced encryption that is commercially available. Get rid of your complex access control infrastructure and let the cryptography do it for you. Read more.

OPENABE LIBRARY

Get started for free (subject t
conditions) today and learn h
how ABE can simplify your d
Download OpenABE here.

Zeutro LLC
Encryption & Data Security

About

You are here: **Home** › About

Zeutro is a software company focused on bringing powerful, advanced encryption solutions to the market. It is managed and was founded by a team of expert cryptographers.

Founders

Susan Hohenberger Waters
Chief Executive Officer / CEO

Matthew Green
Chief Technology Officer / CTO

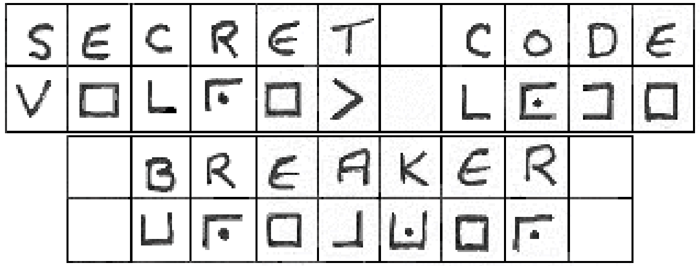
Brent Waters
Chief Scientist

Attribute-based Encryption

An Introduction to Crypto and ABE

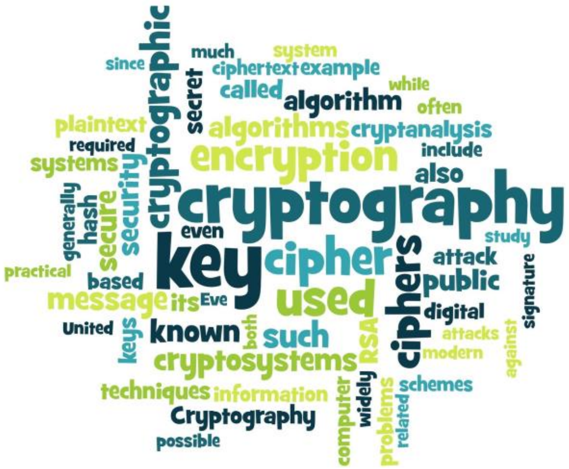
Cryptography

What’s in your mind?



strange symbols?

(cipher pig pen font)



some keywords?

of the private key for T is identical to that in the original scheme.

Challenge The adversary $\mathcal{A}$, will submit two challenge messages m_0 and m_1 to the simulator. The simulator flips a fair binary coin ν, and returns an encryption of m_ν. The ciphertext is output as:

$$E = (\gamma, E' = m_\nu Z, \{E_i = C^{r_i}\}_{i \in \gamma})$$

If $\mu = 0$ then $Z = e(g,g)^{abc}$. If we let $s = c$, then we have $Y^s = (e(g,g)^{ab})^c = e(g,g)^{abc}$, and $E_i = (g^{r_i})^c = C^{r_i}$. Therefore, the ciphertext is a valid random encryption of message m_ν.

Otherwise, if $\mu = 1$, then $Z = e(g,g)^z$. We then have $E' = m_\nu e(g,g)^z$. Since z is random, E' will be a random element of $\mathbb{G}_2$ from the adversaries view and the message contains no information about m_ν.

Phase 2 The simulator acts exactly as it did in Phase 1.

Guess $\mathcal{A}$ will submit a guess ν' of ν. If $\nu' = \nu$ the simulator will output $\mu' = 0$ to indicate that it was given a valid BDH-tuple otherwise it will output $\mu' = 1$ to indicate it was given a random 4-tuple.

As shown in the construction the simulator's generation of public parameters and private keys is identical to that of the actual scheme.

In the case where $\mu = 1$ the adversary gains no information about ν. Therefore, we have $\Pr[\nu \neq \nu' | \mu = 1] = \frac{1}{2}$. Since the simulator guesses $\mu' = 1$ when $\nu \neq \nu'$, we have $\Pr[\mu' = \mu | \mu = 1] = \frac{1}{2}$.

If $\mu = 0$ then the adversary sees an encryption of m_ν. The adversary's advantage in this situation is ϵ by definition. Therefore, we have $\Pr[\nu = \nu' | \mu = 0] = \frac{1}{2} + \epsilon$. Since the simulator guesses $\mu' = 0$ when $\nu = \nu'$, we have $\Pr[\mu' = \mu | \mu = 0] = \frac{1}{2} + \epsilon$.

The overall advantage of the simulator in the Decisional BDH game is $\frac{1}{2}\Pr[\mu' = \mu | \mu = 0] + \frac{1}{2}\Pr[\mu' = \mu | \mu = 1] - \frac{1}{2} = \frac{1}{2}(\frac{1}{2} + \epsilon) + \frac{1}{2}\frac{1}{2} - \frac{1}{2} = \frac{1}{2}\epsilon$.

Chosen-Ciphertext Security. Our security definitions and proofs have been in the chosen-plaintext model. Similar to [32], we notice that our construction can be extended to the chosen-ciphertext model by applying the technique of using simulation-sound NIZK proofs to achieve chosen-ciphertext security [31]. However, in Section 9 we describe how our delegation mechanism can be used with the techniques of Cannetti, Halevi, and Katz [16] to achieve a much more efficient CCA-2 system.

5. LARGE UNIVERSE CONSTRUCTION

In our previous constructions, the size of public parameters grows linearly with the number of possible attributes in the universe. Combining the tricks presented in section 4 with those in the large universe construction of Sahai and Waters [32], we construct another scheme which uses all elements in $\mathbb{Z}_p^*$ as the universe. Yet the size of public parameters only grow linearly in a parameter n. The parameter n is the maximum size of the set γ we can encrypt under. [3]

As noted in [32], having large universe allows us to apply a collision resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p^*$ and use arbitrary strings, that were not necessarily considered during public key setup, as attributes. For example we can add any verifiable attribute, such as "Lives in Beverly Hills", to a user's private key.

5.1 Description

Let $\mathbb{G}_1$ be a bilinear group of prime order p, and let g be a generator of $\mathbb{G}_1$. Additionally, let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ denote the bilinear map. A security parameter, κ, will determine the size of the groups. Also define the Lagrange coefficient $\Delta_{i,S}$ for $i \in \mathbb{Z}_p$ and a set, S, of elements in $\mathbb{Z}_p$, exactly as before. The data will be encrypted under a set γ of n elements[4] of $\mathbb{Z}_p^*$. Our construction follows.

Setup (n) Choose a random value $y \in \mathbb{Z}_p$ and let $g_1 = g^y$. Now choose a random element g_2 of $\mathbb{G}_1$.

Next, choose $t_1, \ldots, t_{n+1}$ uniformly at random from $\mathbb{G}_1$. Let N be the set $\{1, 2, \ldots, n+1\}$. Define a function T, as:

$$T(X) = g_2^{X^n} \prod_{i=1}^{n+1} t_i^{\Delta_{i,N}(X)}.$$

Function T can be viewed as the function $g_2^{X^n} g^{h(X)}$ for some n degree polynomial h. The public parameters PK are: $g_1, g_2, t_1, \ldots, t_{n+1}$ and the master key MK is: y.

Encryption (m, γ, PK) To encrypt a message $m \in \mathbb{G}_2$ under a set of attributes γ, choose a random value $s \in \mathbb{Z}_p$ and publish the ciphertext as:

$$E = (\gamma, E' = me(g_1, g_2)^s, E'' = g^s, \{E_i = T(i)^s\}_{i \in \gamma}).$$

Key Generation $(\mathcal{T}, \mathrm{MK}, \mathrm{PK})$ The algorithm outputs a key which enables the user to decrypt a message encrypted under a set of attributes γ, if and only if $\mathcal{T}(\gamma) = 1$. The algorithm proceeds as follows. First choose a polynomial q_x for each non-leaf node x in the tree $\mathcal{T}$. These polynomials are chosen in the following way in a top down manner, starting from the root node r.

For each node x in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$. Now for the root node r, set $q_r(0) = y$ and d_r other points of the polynomial q_r randomly to define it completely. For any other node x, set $q_x(0) = q_{\mathrm{parent}(x)}(\mathrm{index}(x))$ and choose d_x other points randomly to completely define q_x.

Once the polynomials have been decided, for each leaf node x, we give the following secret values to the user:

$$\begin{aligned} D_x &= g_2^{q_x(0)} \cdot T(i)^{r_x} \quad \text{where } i = \mathrm{att}(x) \\ R_x &= g^{r_x} \end{aligned}$$

where r_x is chosen uniformly at random from $\mathbb{Z}_p$ for each node x. The set of above secret pairs is the decryption key D.

[3] If we are willing to accept random oracles [4], it is possible to overcome the size-limitation on γ by replacing the function $T(X)$ in our construction (see Setup) by a hash function (see [30] for details). This also improves the efficiency of the system.

[4] With some minor modifications, which we omit for simplicity, we can encrypt to all sets of size $\leq n$.

94

theoretical papers ?

Cryptography Base

What is Cryptography?

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries……

-- from Wikipedia

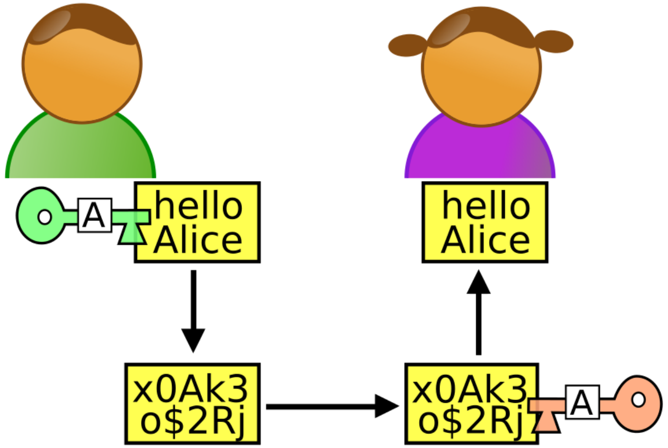
Unofficial but Interesting (Weird) Introduction to Basic Cryptography

BTW, here are official ways to learn cryptography.
Some courses from School of Computing and Information

- ❖ INFSCI 2170/TELCOM 2820: Cryptography
- ❖ INFSCI 2150/TELCOM 2810: Information Security and Privacy
- ❖ CS 1653: Applied Cryptography and Network Security

Cryptography Base

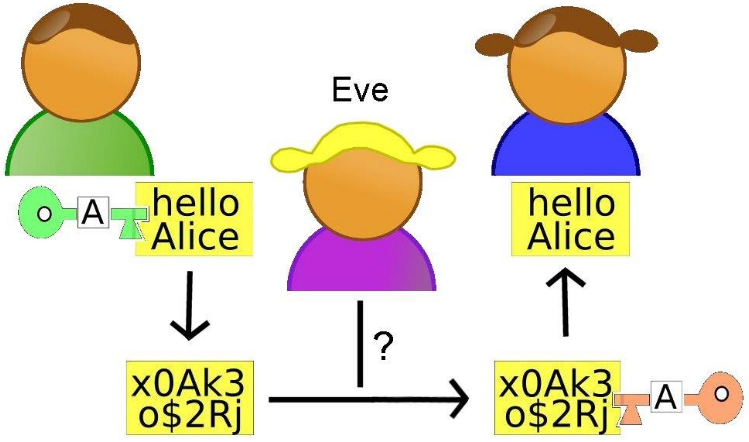
Famous Persons



Their only hobby is talking about secrets

OH ALICE... YOU'RE THE ONE FOR ME
BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE?
ψ+ or ψ- ?

The World’s Most Famous Cryptographic Couple



Sometime, Eve likes to eavesdrop on their secret

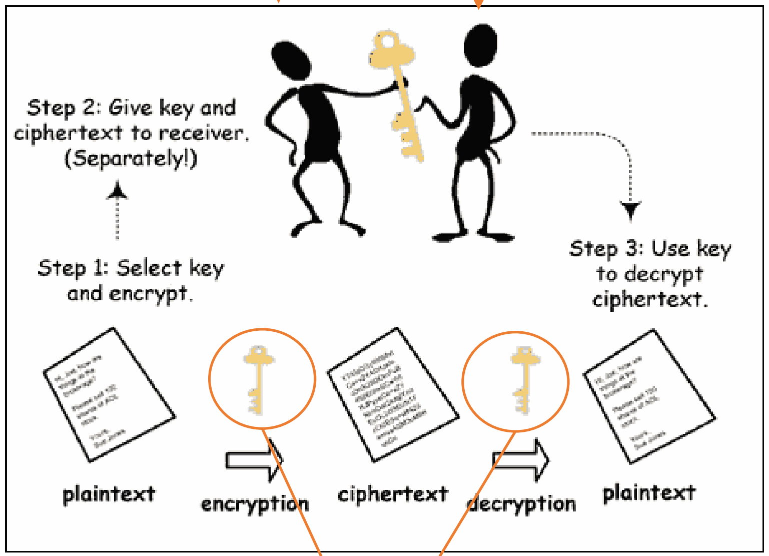
The synopsis could be found here. http://cryptocouple.com/

Cryptography Base

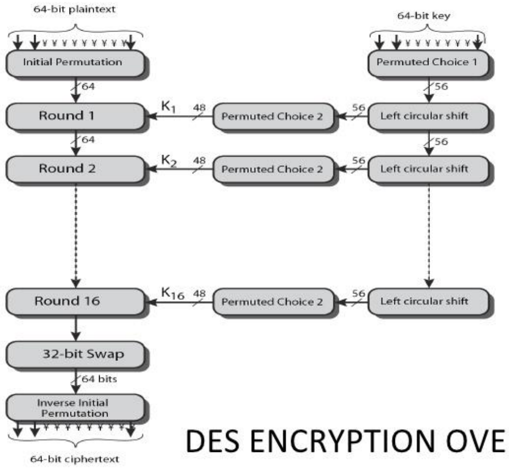
- Symmetric-key Encryption
  - *AES, DES, RC4…*
- How it works

Alice

Bob

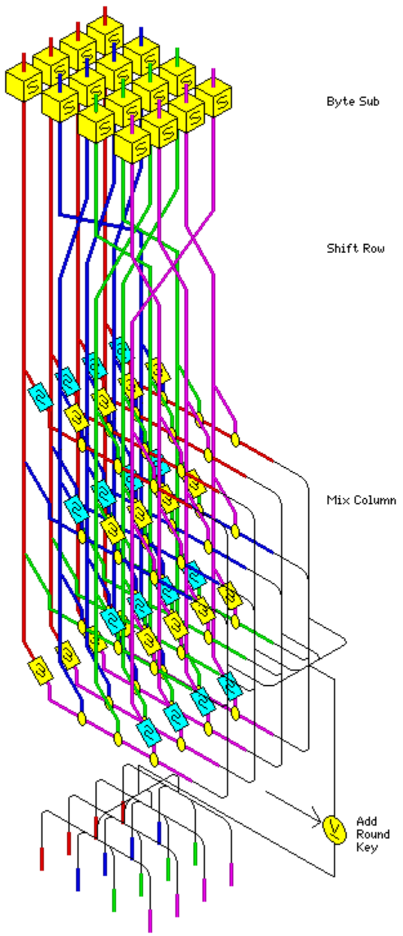

Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

Same key (symmetric key)



DES ENCRYPTION OVERVIEW

https://en.wikipedia.org/wiki/Data_Encryption_Standard

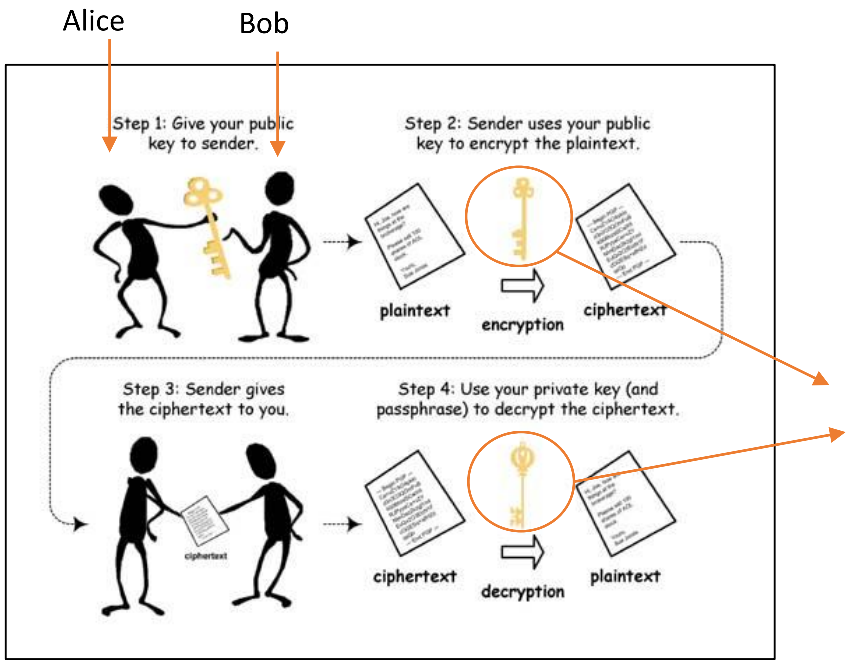


Advanced Encryption Standard (AES)

Here is a simple example to illustrate the principle
http://www.quadibloc.com/crypto/co040401.htm

Cryptography Base

- Public-key Encryption
    - *RSA, DH-key exchange, IBE, ABE…*
- How it works



Step 1: Give your public key to sender.

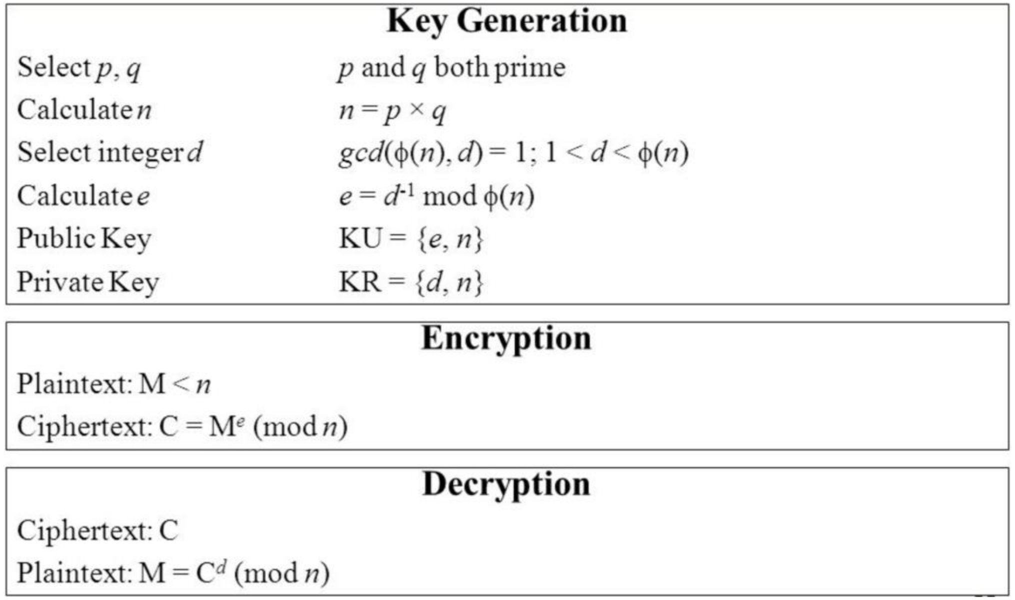
Step 2: Sender uses your public key to encrypt the plaintext.

Step 3: Sender gives the ciphertext to you.

Step 4: Use your private key (and passphrase) to decrypt the ciphertext.

a key pair
- public key
- private key

RSA Algorithm



Key Generation

Select p, q	p and q both prime
Calculate n	$n = p \times q$
Select integer d	$gcd(\phi(n), d) = 1;\ 1 < d < \phi(n)$
Calculate e	$e = d^{-1} \bmod \phi(n)$
Public Key	$KU = \{e, n\}$
Private Key	$KR = \{d, n\}$

Encryption

Plaintext: $M < n$

Ciphertext: $C = M^e \pmod{n}$

Decryption

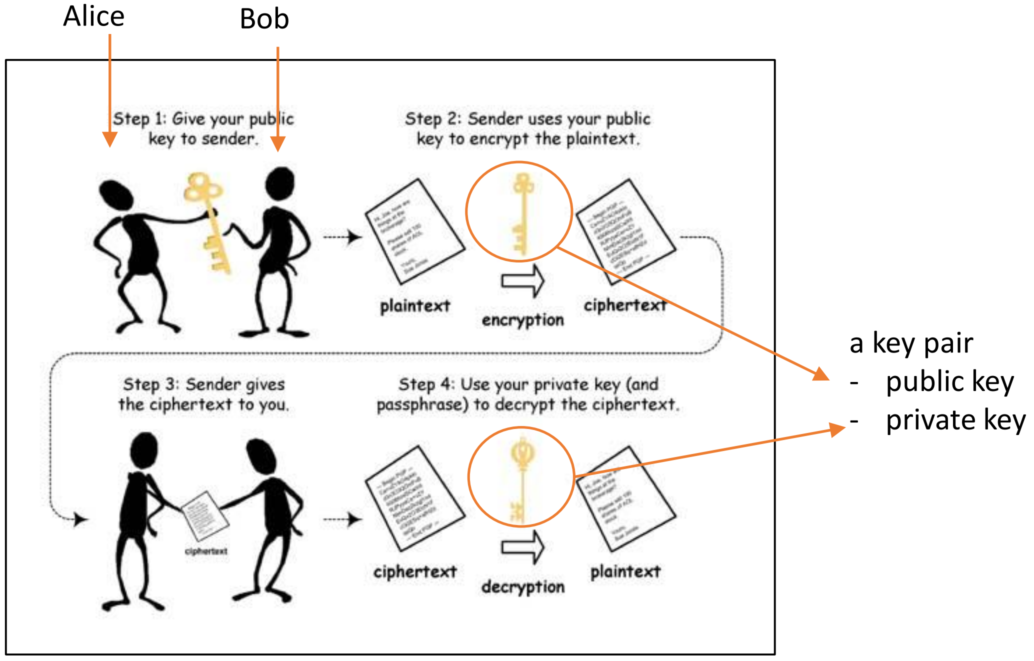
Ciphertext: C

Plaintext: $M = C^d \pmod{n}$

http://doctrina.org/How-RSA-Works-With-Examples.html

Cryptography Base

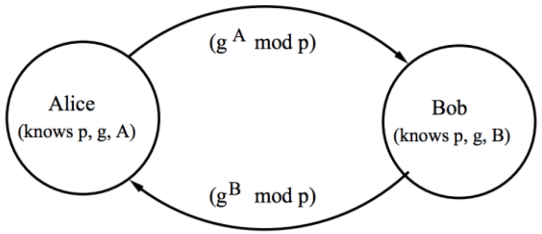
- Public-key Encryption
  - *RSA, DH-key exchange, IBE, ABE…*
- How it works



Alice
Bob
Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
ciphertext
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
decryption
plaintext

a key pair
- public key
- private key

Diffie-Hellman key exchange



Steps in the algorithm:

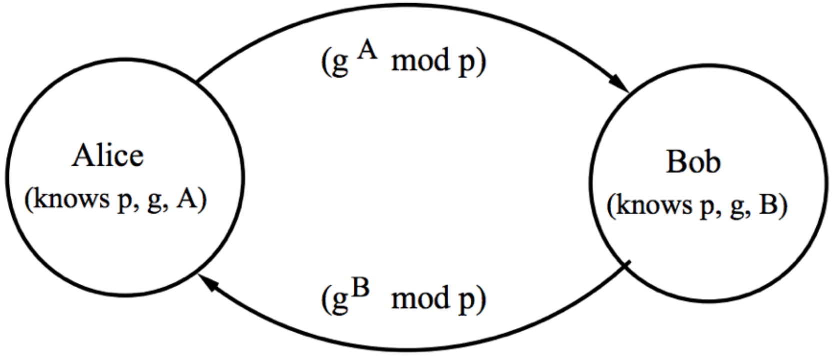
1. Alice and Bob agree on a prime number p and a base g.
2. Alice chooses a secret number a, and sends Bob ($g^a \mod p$).
3. Bob chooses a secret number b, and sends Alice ($g^b \mod p$).
4. Alice computes $((g^b \mod p)^a \mod p)$.
5. Bob computes $((g^a \mod p)^b \mod p)$.

Both Alice and Bob can use this number as their key. Notice that p and g need not be protected.

Cryptography Base

- Design Principle
  - *Mathematical construction*
    - exponentiation, pairing-based operation (bilinear map, multilinear map), ……
  - *Computational hardness assumption*
    - Computational hardness problem
      - No polynomial time algorithm can solve the problem
  - *Take DH-key exchange as an example*

g^r g^{-r} -> $g^r g^{-r} = g^{r-r} = g^0 = 1$



Given g, g^A and g^B, it is hard to compute g^{AB}

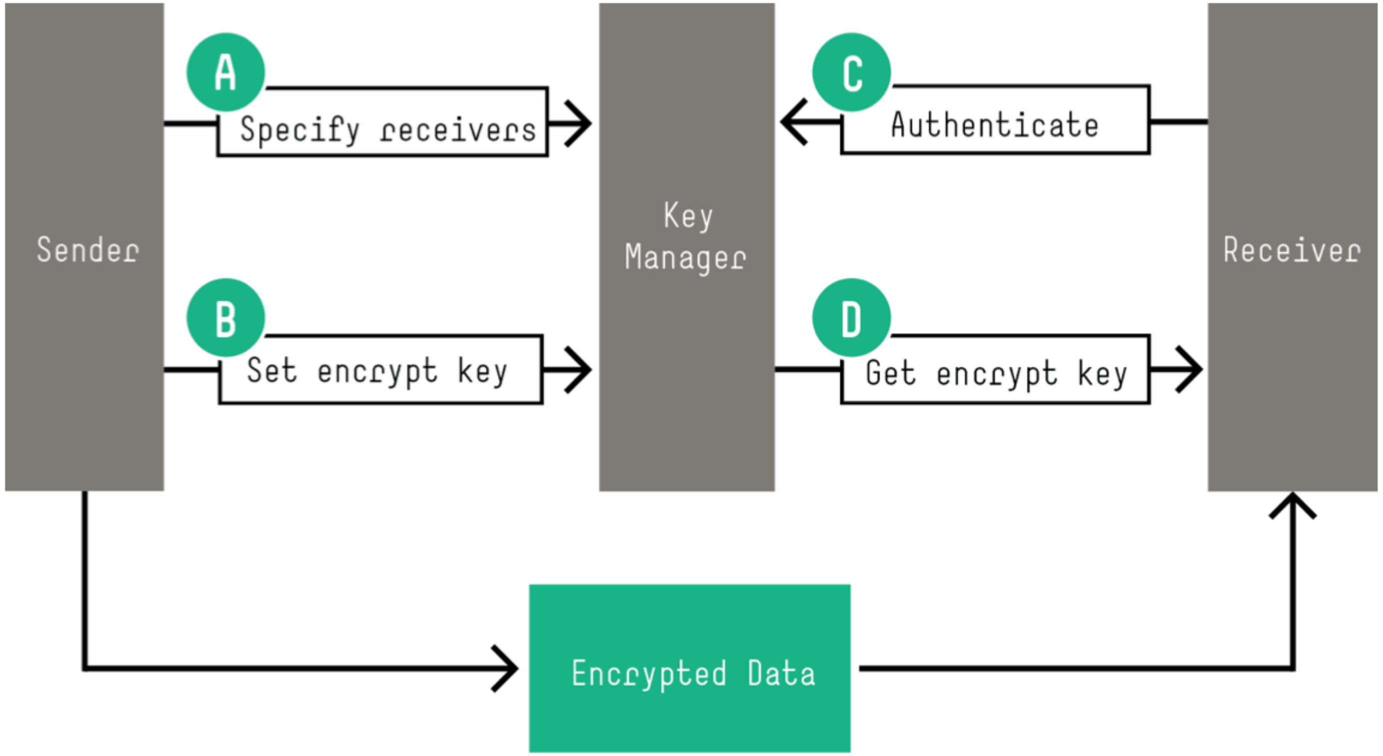
Given g^A and g, it is hard to compute A
Given g and A, it is easy to compute g^A

Identity based Encryption (IBE)

Let’s review some issues in traditional cryptography approaches

Key Management Issue

High Storage Costs
High Availability Needs



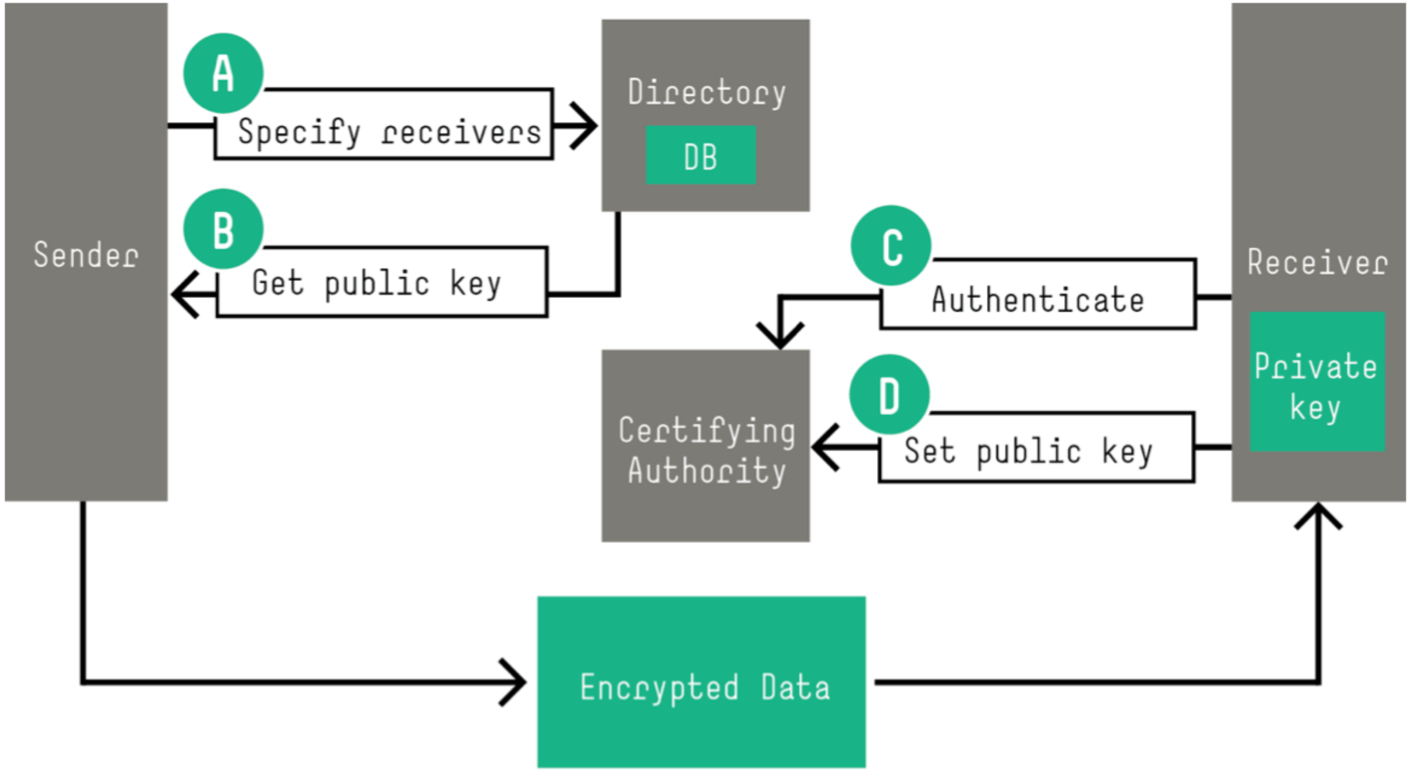
Symmetric Key Management

Identity based Encryption (IBE)

Let’s review some issues in traditional cryptography approaches

Key Management Issue

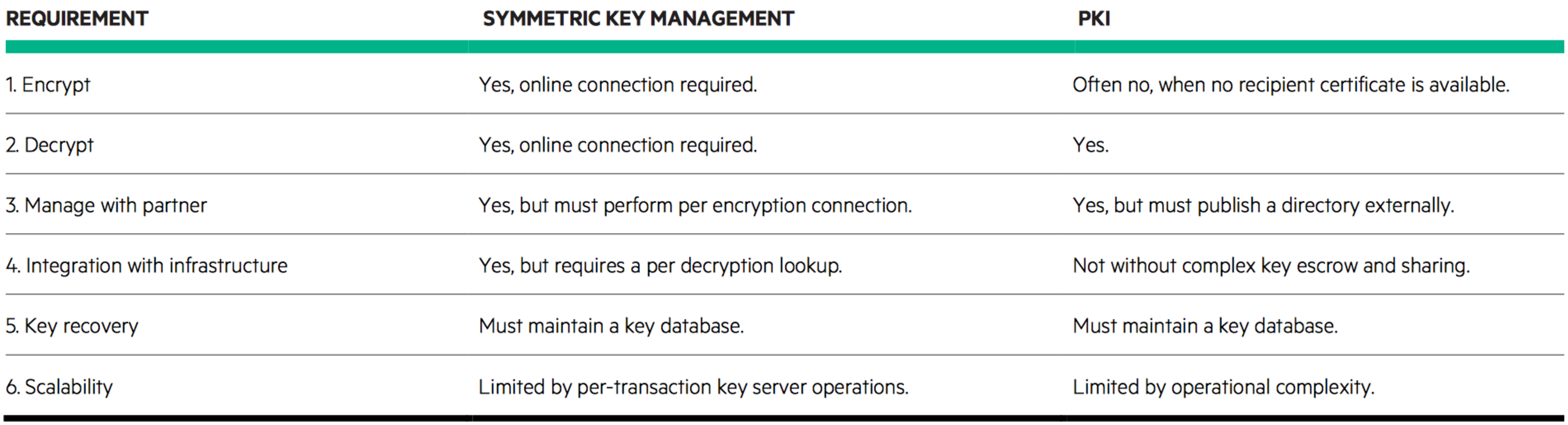
Do not contact with key server each time
Impractical to use and make key recovery difficulty



Certificated-based Key Management

Identity based Encryption (IBE)

Let’s review some issues in traditional cryptography approaches



REQUIREMENT	SYMMETRIC KEY MANAGEMENT	PKI
1. Encrypt	Yes, online connection required.	Often no, when no recipient certificate is available.
2. Decrypt	Yes, online connection required.	Yes.
3. Manage with partner	Yes, but must perform per encryption connection.	Yes, but must publish a directory externally.
4. Integration with infrastructure	Yes, but requires a per decryption lookup.	Not without complex key escrow and sharing.
5. Key recovery	Must maintain a key database.	Must maintain a key database.
6. Scalability	Limited by per-transaction key server operations.	Limited by operational complexity.

Both symmetric key management and PKI fall short of meeting all six of the requirements of an effective enterprise key management system

Identity based Encryption (IBE)

- Motivation
  - Sender must have recipient’s certificate
  - Complexity of certificate management/key management

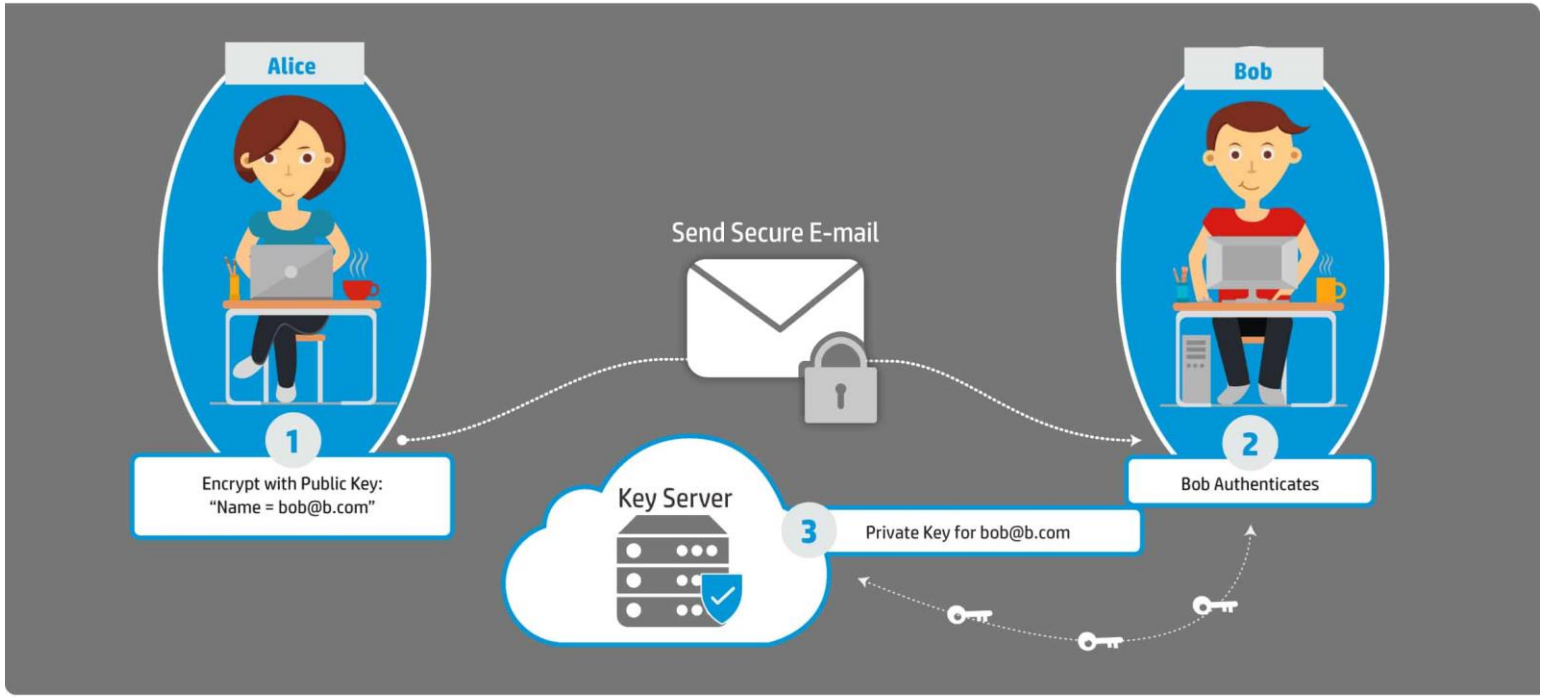
- IBE: Public key encryption scheme where public key is an arbitrary string (id).
  - Examples: user’s e-mail address, current-date, …

- IBE system is made up of 4 algorithms:
  - Setup: generate params and master-key, MK
  - Keygen: given pub-key ID and master-key output priv-key, d_{ID}
  - Encrypt: using pub-key ID (and params)
  - Decrypt: using priv-key

Identity based Encryption (IBE)

An example illustrates how Alice would send a secure email to Bob using IBE

- ❖Alice encrypts the email using Bob’s e-mail address, **“bob@b.com”, as the public key**.
- ❖When Bob receives the message, he contacts the key server. The key server contacts a directory or other external **authentication** source to authenticate Bob’s identity and establish any other policy elements.
- ❖After authenticating Bob, the key server then returns his **private key**, with which Bob can decrypt the message. This private key can be used to **decrypt** all future messages received by Bob.

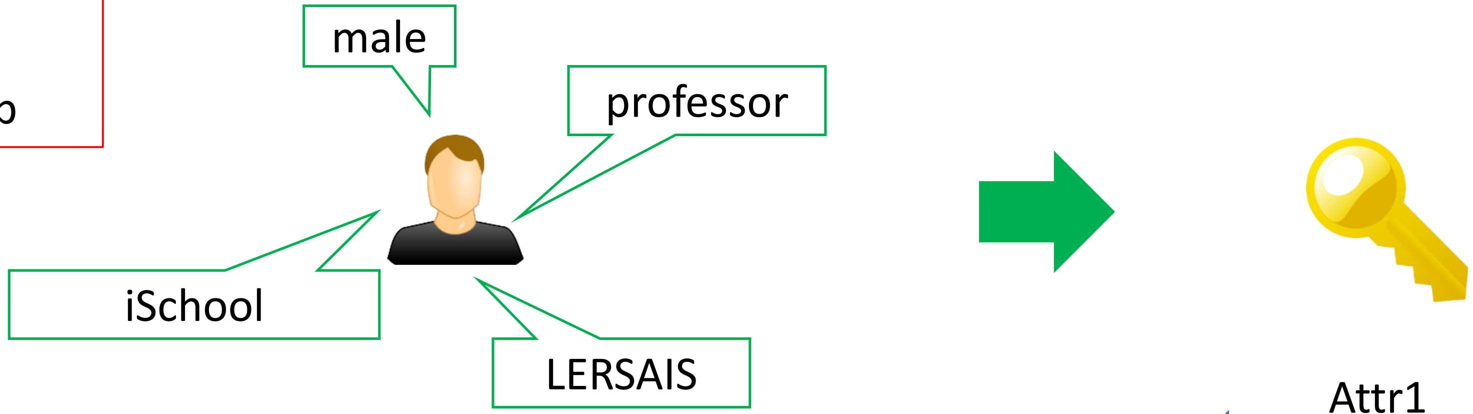

Alice
Bob
Send Secure E-mail
1
Encrypt with Public Key: “Name = bob@b.com”
2
Bob Authenticates
Key Server
3
Private Key for bob@b.com

Attribute based Encryption (ABE)

- Attribute Based Encryption
  - *An extend scheme of Identity based Encryption*
  - *Utilization of attribute information for Encryption/Decryption*

Only ID?
Attributes → "ID"
Decryption: one → group

Access Control



Access Policy

Attr1
Attr1, Attr2, … (*OR*)
Attr1 *AND* Attr2

Combination of encryption and access control

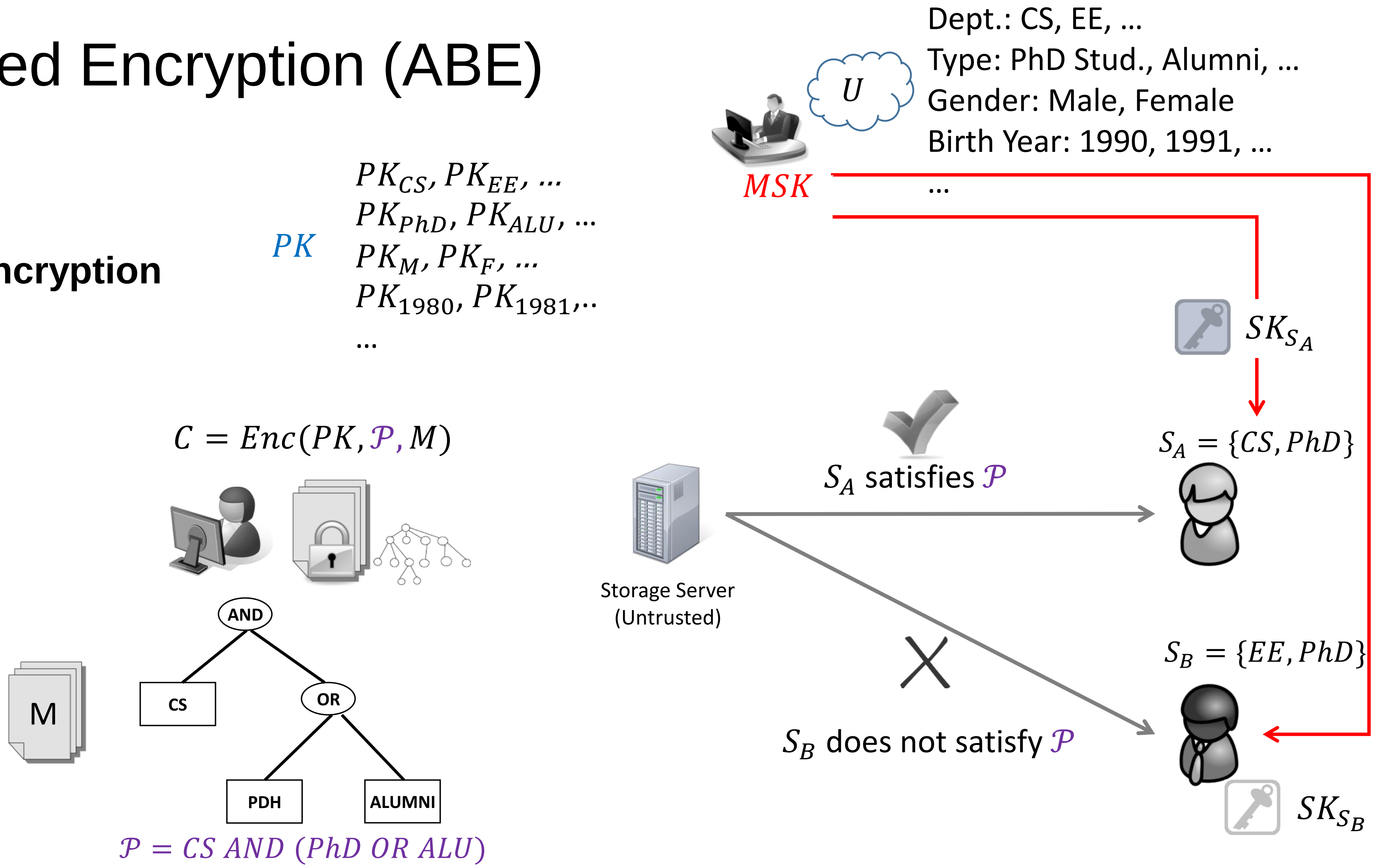
Attribute based Encryption (ABE)

Overview of

Ciphertext-Policy

Attribute based Encryption

- ❖ Setup
- ❖ Encrypt
- ❖ Key Generation
- ❖ Decrypt



U

Dept.: CS, EE, …

Type: PhD Stud., Alumni, …

Gender: Male, Female

Birth Year: 1990, 1991, …

…

MSK

PK

$PK_{CS}, PK_{EE}, \ldots$

$PK_{PhD}, PK_{ALU}, \ldots$

$PK_{M}, PK_{F}, \ldots$

$PK_{1980}, PK_{1981}, ..$

…

$C = Enc(PK, \mathcal{P}, M)$

SK_{S_A}

$S_A = \{CS, PhD\}$

S_A satisfies $\mathcal{P}$

Storage Server (Untrusted)

$S_B = \{EE, PhD\}$

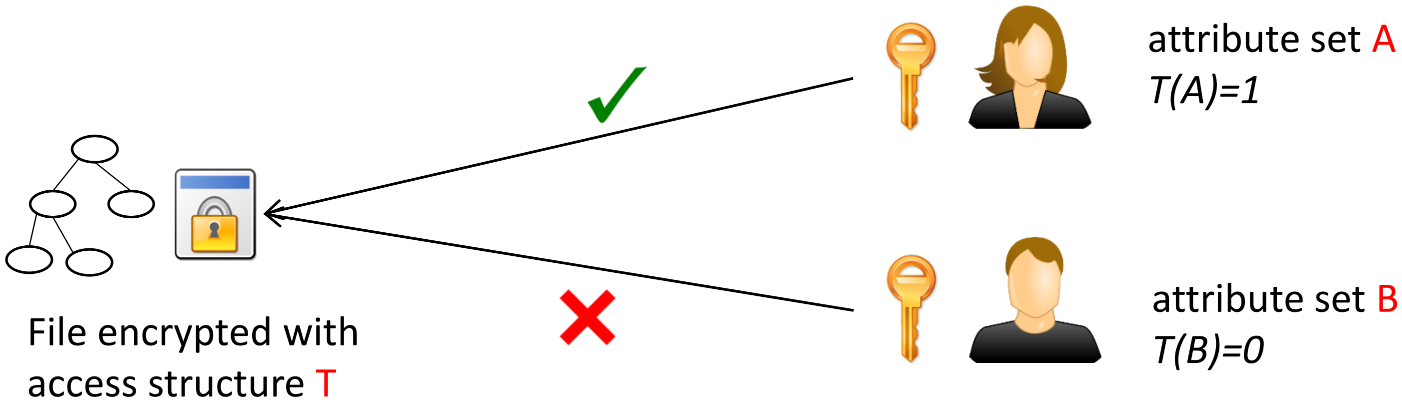
S_B does not satisfy $\mathcal{P}$

SK_{S_B}

$\mathcal{P} = CS\ AND\ (PhD\ OR\ ALU)$

Attribute based Encryption (ABE)

Ciphertext Policy Attribute based Encryption



File encrypted with access structure T

✓

✗

attribute set A

T(A)=1

attribute set B

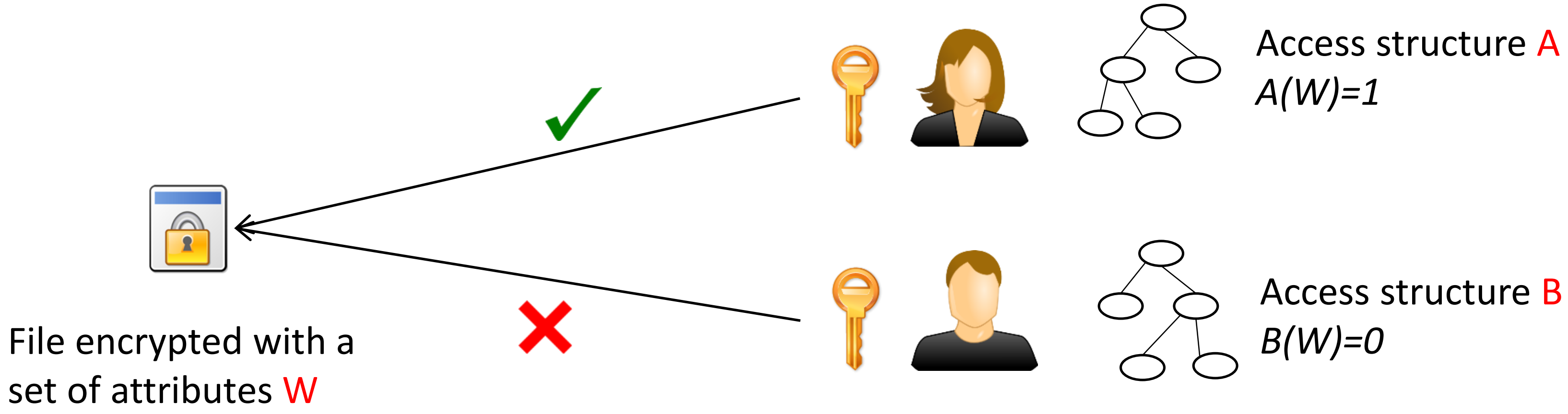
T(B)=0

Role-based Access Control ←→ CP-ABE

Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." *2007 IEEE symposium on security and privacy (S&P'07)*. IEEE, 2007.

Attribute based Encryption (ABE)

Key Policy Attribute based Encryption



Access structure A
A(W)=1

Access structure B
B(W)=0

File encrypted with a set of attributes W

Content-based Access Control ←→ KP-ABE

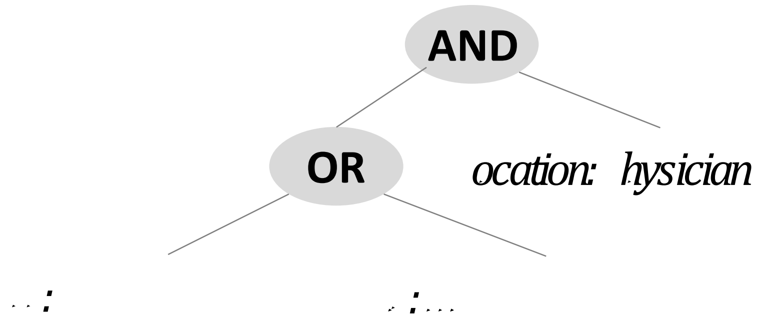
Goyal, Vipul, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89-98. Acm, 2006.

Attribute based Encryption (ABE)

Application: Attribute-based Access Control

- *Access Structures of ABE schemes*
  - And-gate olicy ffiliation: niversity ospital ∧ ocation: hysician
  - Tree-based olicy . . : ∨ . : . .) ∧ ocation: hysician
  - LSSS Matrix olicy . . : ∧ . : . .) ∨ ocation: hysician

ffiliation: niversity ospital . .
ocation: hysician



$$\left[\begin{array}{ccc}0 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & -1\end{array}\right]\begin{array}{l}\rightarrow \text{. . :}\\ \rightarrow \text{. : . . .}\\ \rightarrow \text{ocation: hysician}\end{array}$$

most efficient AS for encryption

Application in Health Informatics

Securing Electronic Medical Records Using Attribute-based Encryption on Mobile Devices

Electronic Medical Records

“The systematized collection of patient and population electronically-stored health information in a digital format.”

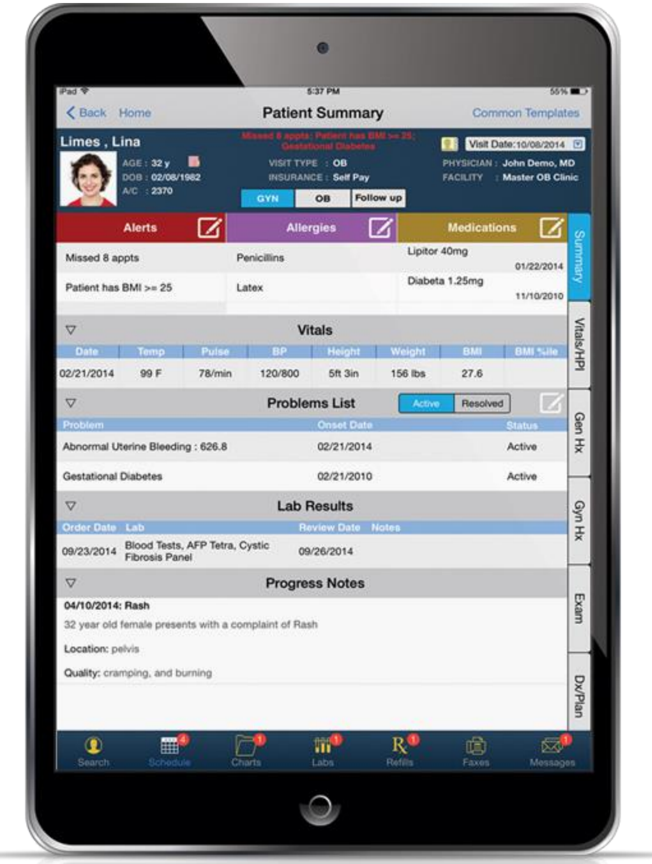
Patients and insurers can avoid repeating studies

Lab tests,
Images,
Diagnoses,
Prescriptions,
Medical histories,
etc.

e.g., avoid to expose patient to additional radiation.

EMR on Mobile Devices

More patients and physicians are shifting towards accessing EMRs via their mobile devices for quicker record access.



iPad 5:37 PM 55%

< Back Home **Patient Summary** Common Templates

Limes , Lina

Missed 8 appts; Patient has BMI >= 25; Gestational Diabetes

Visit Date:10/08/2014

AGE : 32 y
DOB : 02/08/1982
A/C : 2370

VISIT TYPE : OB
INSURANCE : Self Pay

PHYSICIAN : John Demo, MD
FACILITY : Master OB Clinic

GYN | OB | Follow up

Alerts	Allergies	Medications
Missed 8 appts	Penicillins	Lipitor 40mg 01/22/2014
Patient has BMI >= 25	Latex	Diabeta 1.25mg 11/10/2010

Vitals

Date	Temp	Pulse	BP	Height	Weight	BMI	BMI %ile
02/21/2014	99 F	78/min	120/800	5ft 3in	156 lbs	27.6	

Problems List Active | Resolved

Problem	Onset Date	Status
Abnormal Uterine Bleeding : 626.8	02/21/2014	Active
Gestational Diabetes	02/21/2010	Active

Lab Results

Order Date	Lab	Review Date	Notes
09/23/2014	Blood Tests, AFP Tetra, Cystic Fibrosis Panel	09/26/2014	

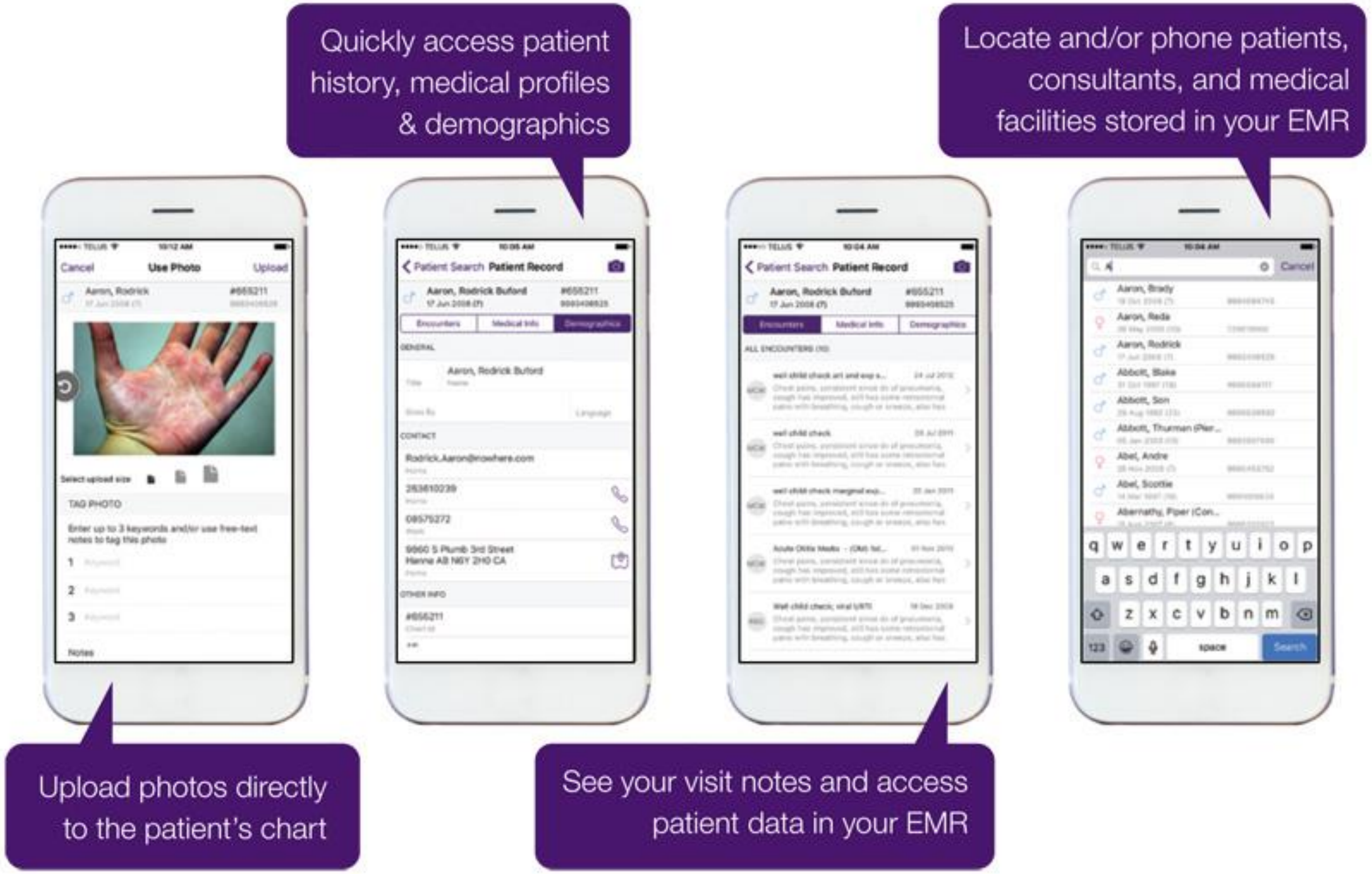
Progress Notes

04/10/2014: Rash

32 year old female presents with a complaint of Rash

Location: pelvis

Quality: cramping, and burning



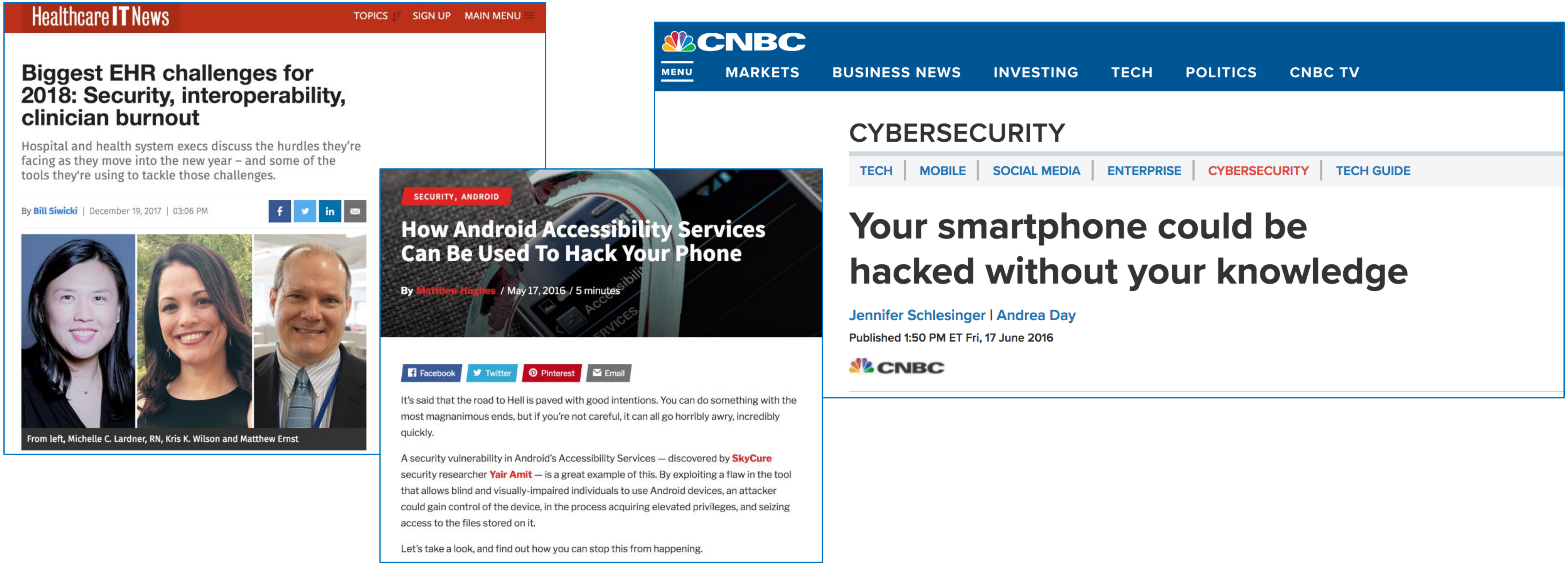
Quickly access patient history, medical profiles & demographics

Locate and/or phone patients, consultants, and medical facilities stored in your EMR

Upload photos directly to the patient's chart

See your visit notes and access patient data in your EMR

EMR on Mobile Devices -- Concerns



Biggest EHR challenges for 2018: Security, interoperability, clinician burnout

Hospital and health system execs discuss the hurdles they're facing as they move into the new year – and some of the tools they're using to tackle those challenges.

By Bill Siwicki | December 19, 2017 | 03:06 PM

From left, Michelle C. Lardner, RN, Kris K. Wilson and Matthew Ernst

How Android Accessibility Services Can Be Used To Hack Your Phone

By Matthew Hughes / May 17, 2016 / 5 minutes

It's said that the road to Hell is paved with good intentions. You can do something with the most magnanimous ends, but if you're not careful, it can all go horribly awry, incredibly quickly.

A security vulnerability in Android's Accessibility Services — discovered by SkyCure security researcher Yair Amit — is a great example of this. By exploiting a flaw in the tool that allows blind and visually-impaired individuals to use Android devices, an attacker could gain control of the device, in the process acquiring elevated privileges, and seizing access to the files stored on it.

Let's take a look, and find out how you can stop this from happening.

CYBERSECURITY

Your smartphone could be hacked without your knowledge

Jennifer Schlesinger | Andrea Day

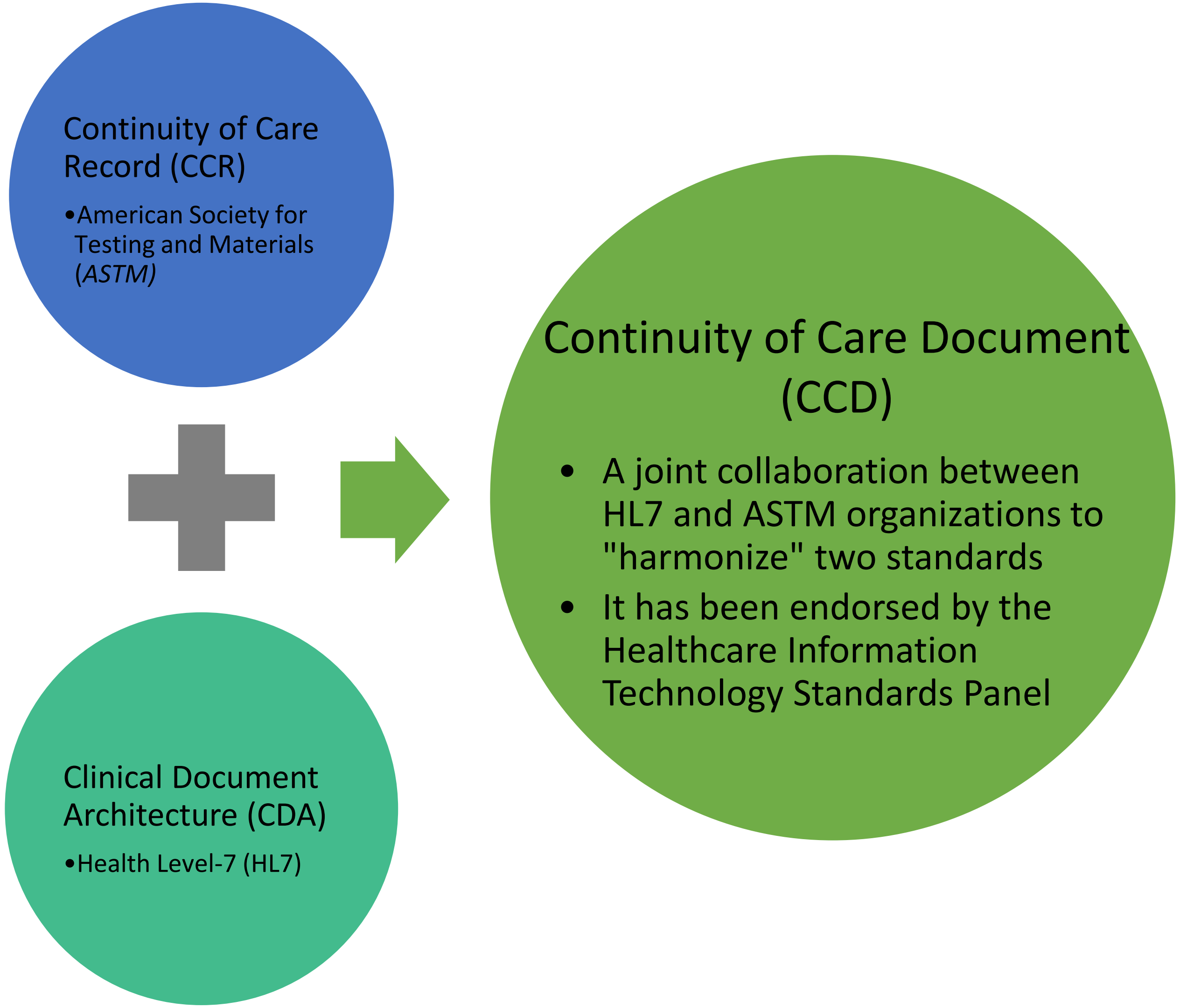
Published 1:50 PM ET Fri, 17 June 2016

It is possible to exploited vulnerability to bypass application permissions and access users' data

Status Quo and Challenge

- EMR systems’ reliance on transport security.
    - *Recipients of EMRs obtain the cleartext records and are usually cached unprotected on the end device.*
- Access control is online only.
- Provider-centric environment.
- Records are not well protected today.
    - *Huge clinical employees can access EMRs*
    - *The server or database is unavailable, access control decisions cannot be made, or records cannot be reached.*
- Complexity of access policies.

Requirement of Emerging Standards



Continuity of Care Record (CCR)

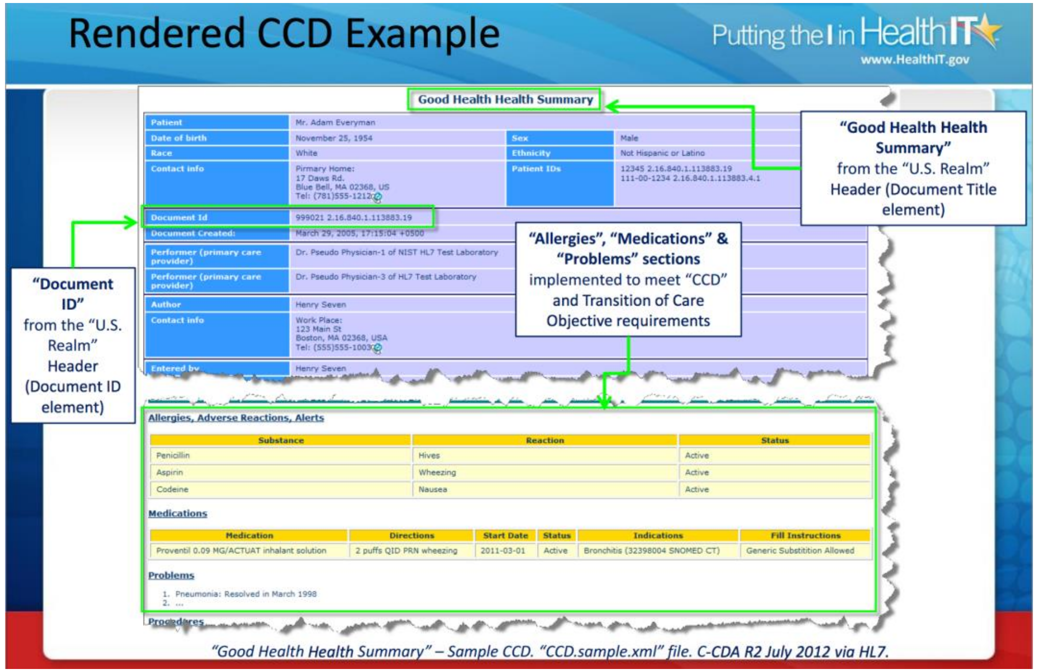
- American Society for Testing and Materials (*ASTM)*

Clinical Document Architecture (CDA)

- Health Level-7 (HL7)

Continuity of Care Document (CCD)

- A joint collaboration between HL7 and ASTM organizations to "harmonize" two standards
- It has been endorsed by the Healthcare Information Technology Standards Panel



Rendered CCD Example

Good Health Health Summary

Patient	Mr. Adam Everyman		
Date of birth	November 25, 1954	Sex	Male
Race	White	Ethnicity	Not Hispanic or Latino
Contact info	Pirmary Home: 17 Daws Rd. Blue Bell, MA 02368, US Tel: (781)555-1212	Patient IDs	12345 2.16.840.1.113883.19 111-00-1234 2.16.840.1.113883.4.1
Document Id	999021 2.16.840.1.113883.19		
Document Created:	March 29, 2005, 17:15:04 +0500		
Performer (primary care provider)	Dr. Pseudo Physician-1 of NIST HL7 Test Laboratory		
Performer (primary care provider)	Dr. Pseudo Physician-3 of HL7 Test Laboratory		
Author	Henry Seven		
Contact info	Work Place: 123 Main St Boston, MA 02368, USA Tel: (555)555-1003		
Entered by	Henry Seven		

"Good Health Health Summary" from the "U.S. Realm" Header (Document Title element)

"Document ID" from the "U.S. Realm" Header (Document ID element)

"Allergies", "Medications" & "Problems" sections implemented to meet "CCD" and Transition of Care Objective requirements

Allergies, Adverse Reactions, Alerts

Substance	Reaction	Status
Penicillin	Hives	Active
Aspirin	Wheezing	Active
Codeine	Nausea	Active

Medications

Medication	Directions	Start Date	Status	Indications	Fill Instructions
Proventil 0.09 MG/ACTUAT inhalant solution	2 puffs QID PRN wheezing	2011-03-01	Active	Bronchitis (32398004 SNOMED CT)	Generic Substitition Allowed

Problems

1. Pneumonia: Resolved in March 1998
2. ...

Procedures

"Good Health Health Summary" – Sample CCD. "CCD.sample.xml" file. C-CDA R2 July 2012 via HL7.

> *" The CCR document instance must be self-protecting when possible, and carry sufficient data embedded in the document instance to permit access decisions to be made based upon confidentiality constraints or limitations specific to that instance. "*

ABE Application Scenario

A patient-centric health application

-- that allows a patient/user to store and manage all his Electronic Health Records (EHRs) by storing them in Cloud Storage

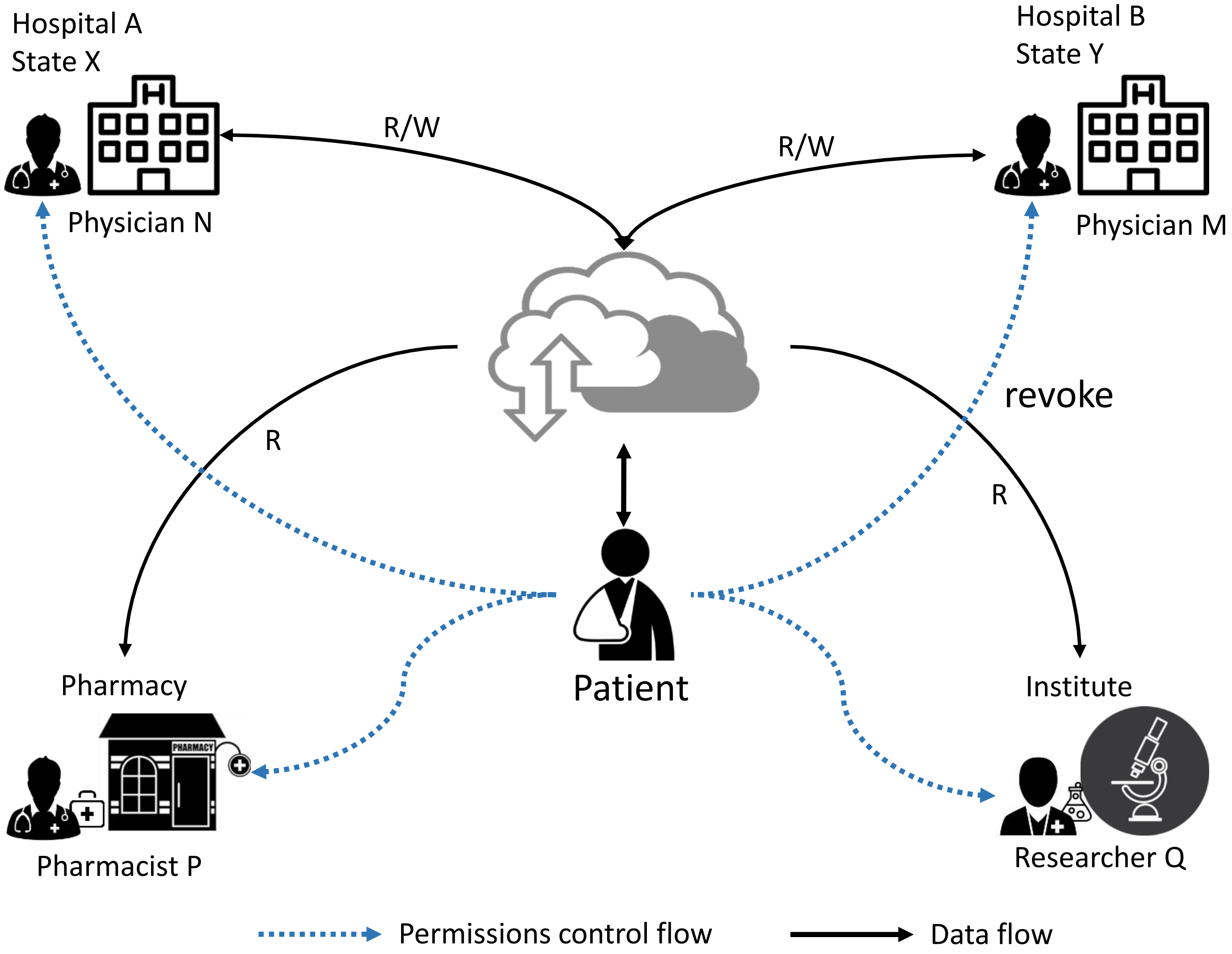
Similar scenarios:

User-centric applications

Organization-centric applications

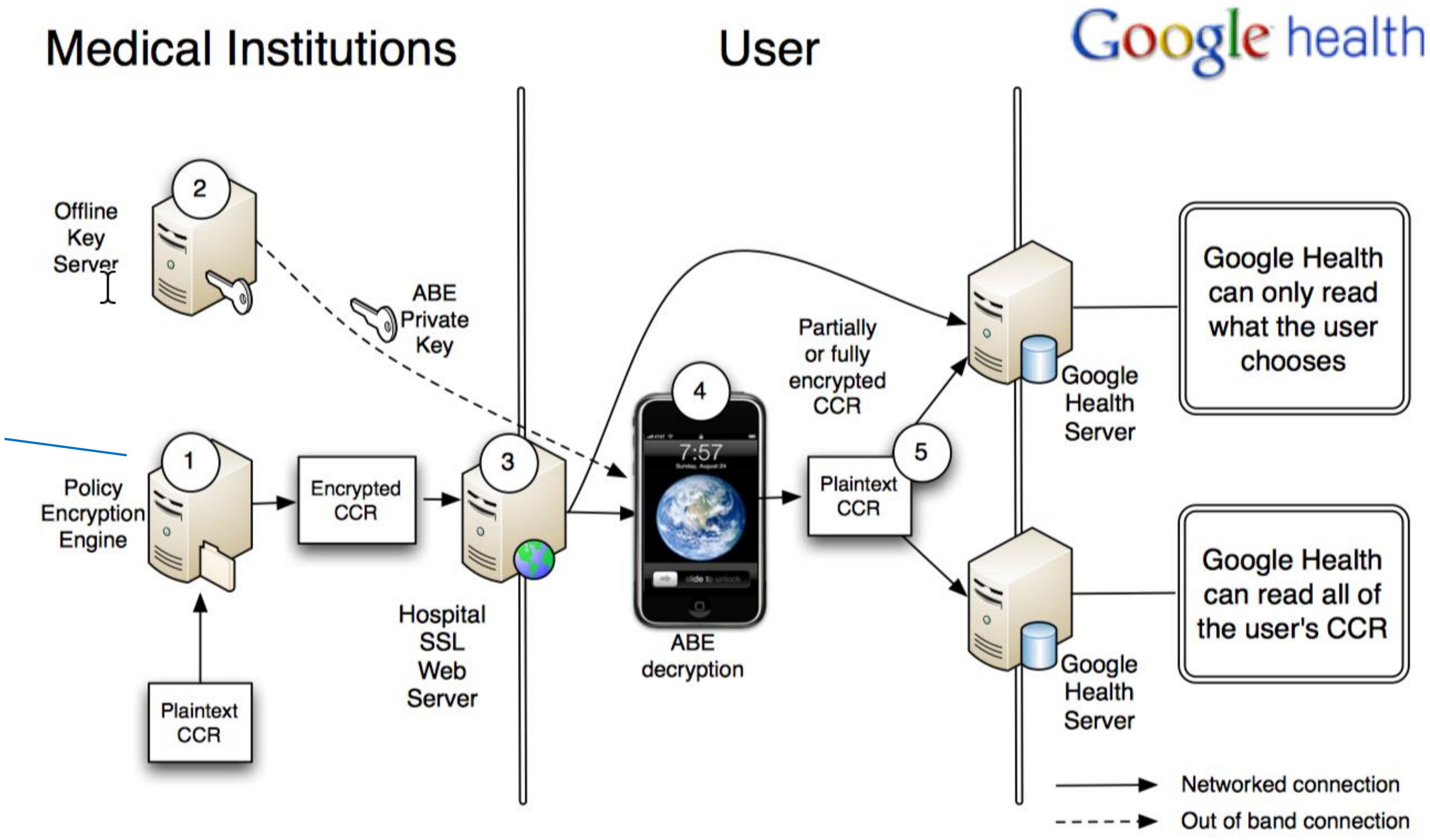
Hospital-centric applications

Build-in Access Control of Data

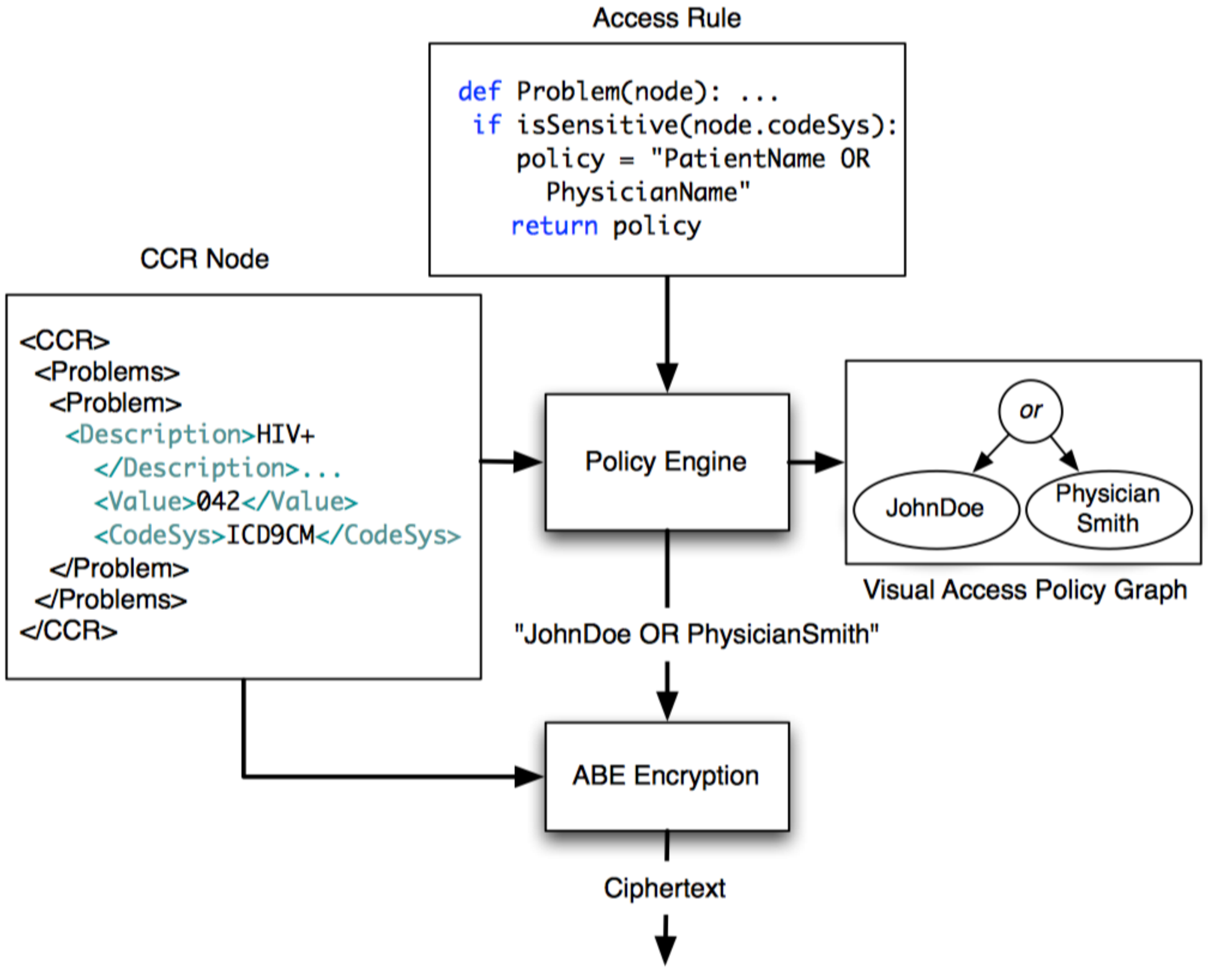


Framework Prototype

Parses each node in the CCR to calculate an appropriate access policy



Policy Engine



```
def Problem(node): ...
 if isSensitive(node.codeSys):
    policy = "PatientName OR
      PhysicianName"
   return policy
```

```
<CCR>
 <Problems>
  <Problem>
   <Description>HIV+
     </Description>...
     <Value>042</Value>
     <CodeSys>ICD9CM</CodeSys>
  </Problem>
 </Problems>
</CCR>
```

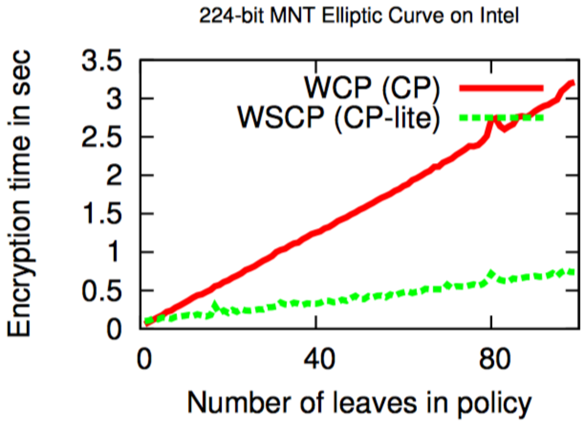
A policy engine prototype that evaluates EMRs based on CCR-compliant metadata.

The policy engine then determines the appropriate access policy from a set of rules created by the provider.

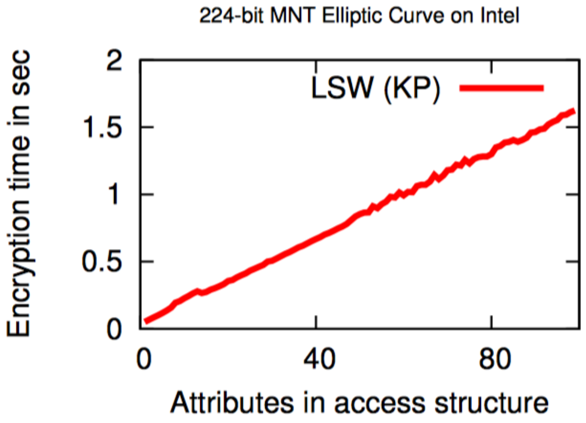
Key Management

- Offline Key Server (PKG)
  - *Initialization*
    - physically present at a trusted PKG facility
      - such as a hospital, clinic or Regional Health Information Organization (RHIO)
    - to have their iPhones provisioned with the appropriate ABE decryption keys
      - e.g., via a USB connection / Bluetooth connection
  - *Key Update*
    - Generates the patient's ABE private keys, a public-key certificate, a RSA public and private key-pair
    - to be used for secure remote key updates.
  - *Revocation*
    - "Lazy" revocation – add a certain time period in generated private key
    - Full revocation – employ online mediator / re-encrypt
    - Tradeoffs

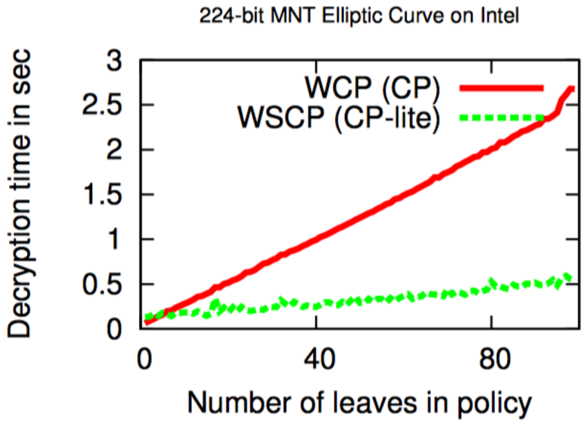
Computation Performance



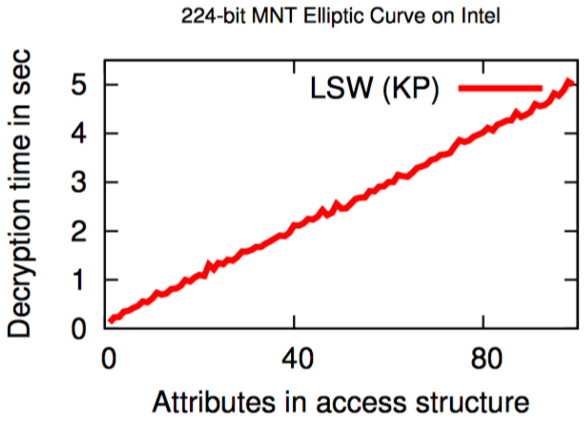
(a) Encryption time (Intel)



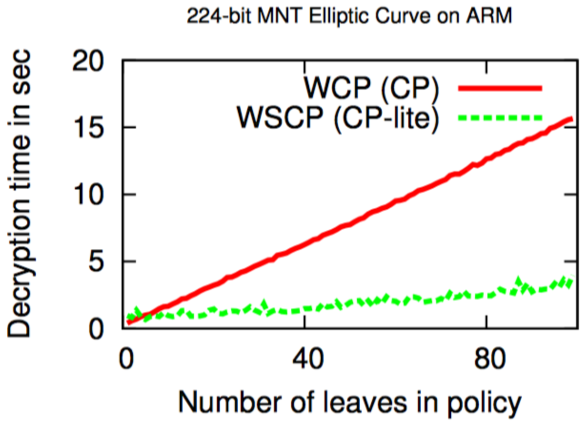
(b) Encryption time (Intel)



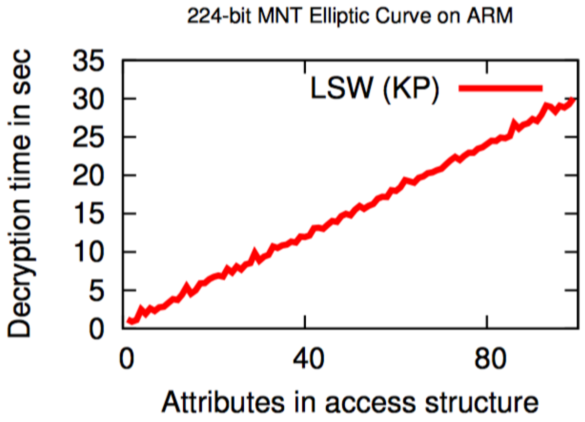
(c) Decryption time (Intel)



(a) Decryption time (Intel)



(b) Decryption (ARM)



(c) Decryption (ARM)

Thanks.