MediCryption

A Cryptographically-Secure Data-Sharing System for Electronic Health Records

EECS 598 PETs Final Project Presentation

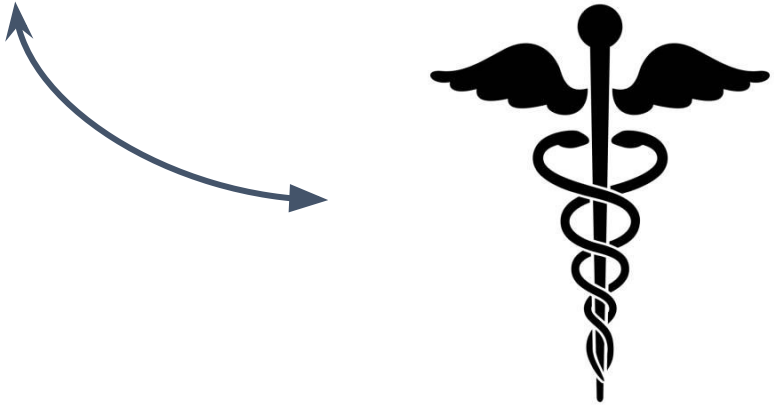
{lweijie, coopstev, namhokoh, cbzjr}@umich.edu

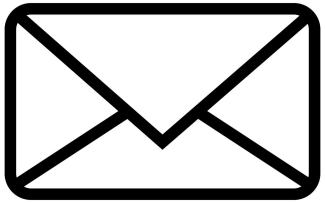
Presentation Outline

- Introduction
- Motivations
- *MediCrypt*
  - Threat Model
  - Assumptions
  - Our System
    - Attribute-Based Encryption
    - Expert Interview: Dr. David Hanauer
    - High Level System Overview
- Demonstration
- Future Work
- Conclusions

How Do You Share Your Medical Information?

Introduction





Introduction - Who's Driving Sharing

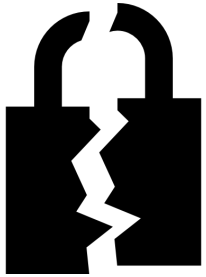
Net Health

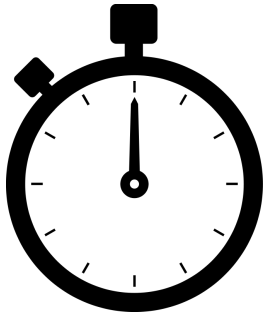
Cerner

Epic

Electronic Healthcare Record (EHR) Sharing is Incredibly Flawed

The System is Flawed…Here's Why





70%

of US Hospitals still rely on insecure methods of communication

89%

of respondents in a PEW Study expressed desire to access & share their records

Motivations

With the democratization of digital health records, patients need the ability to access, manage and share their data in an individual, cryptographically secure manner.

Motivations

Democratization of digital health records; patients need the ability to access, manage and ***share*** their data in an individual, cryptographically secure manner.

Motivations

- Sharing EHR data is largely abstracted away from patients
- Large corporations with large market shares make sharing difficult for anyone that doesn't use their product
- Current practices are largely insecure

MediCryption serves as a **remedy** to these issues, providing patients with the ability to **securely** share their health records with their practitioners

MediCryption: Threat Model

- Passive adversary
- Healthcare server cannot be fully trusted
- Doctors can turn rogue—revocability is important!

MediCryption: Assumptions

- Doctors obtain private keys in a secure way
- Machines used by doctor and patients are not compromised
- Server is not a bad actor / we have the ability to shut it off if it's been compromised

Attribute-Based Encryption (ABE)

- Allows for encryption based on attributes
  - E.g. patient **or** doctor, doctor **and** years > 5
- A tree-based flow for allowing access to information
- Offline
  - Encryption and decryption can happen locally

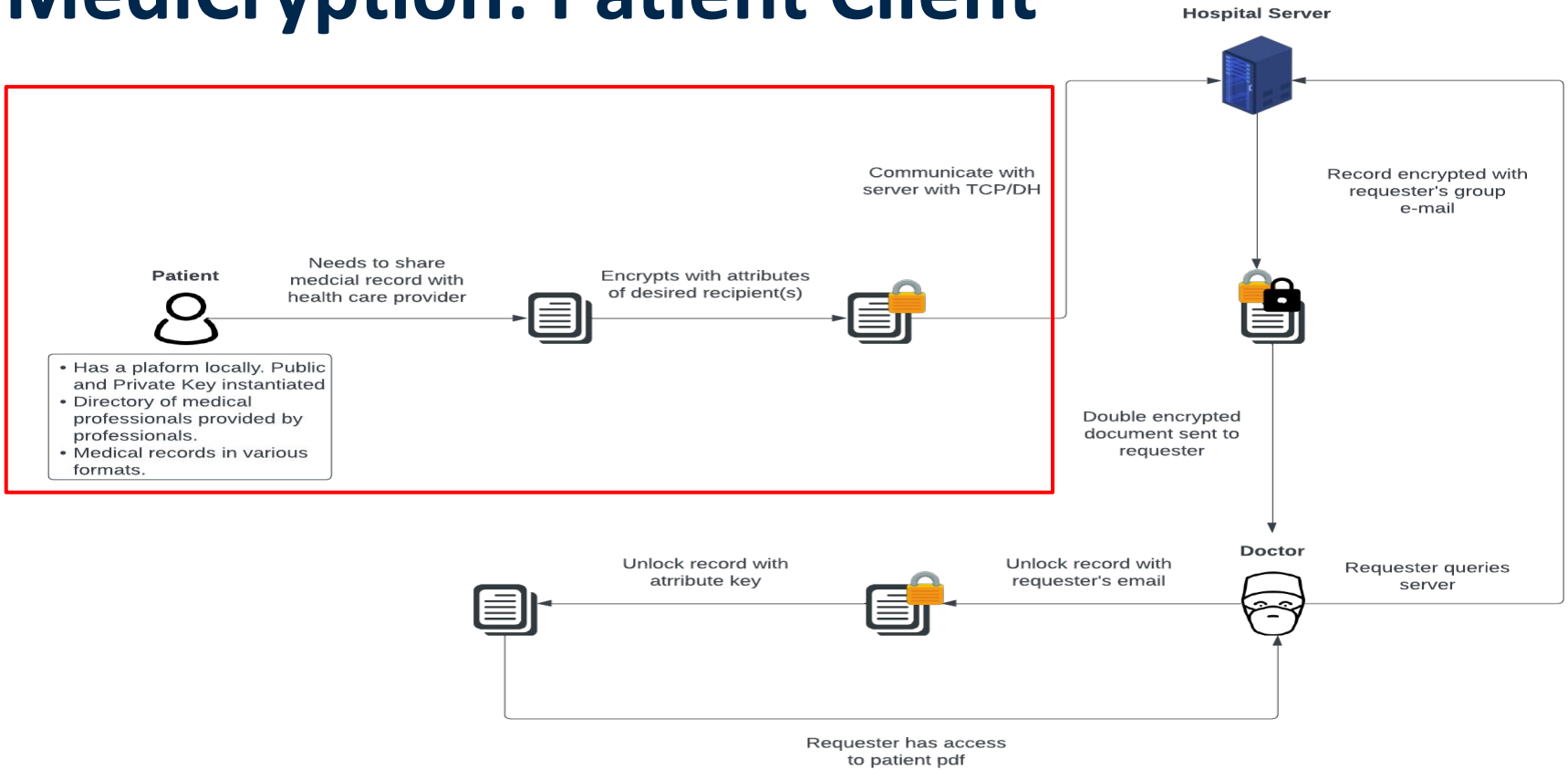
Attribute-Based Encryption (ABE)

- Initialized with global and private keys
  - Represents the state of the scheme. ABEs initialized with the same global and private keys and encrypt and decrypt interchangeably
- Global key
  - Enables encryption
  - Enables decryption if the private key is given
- Private key
  - Enables generation of private keys based on **any** attribute
  - The “secrets” of ABE

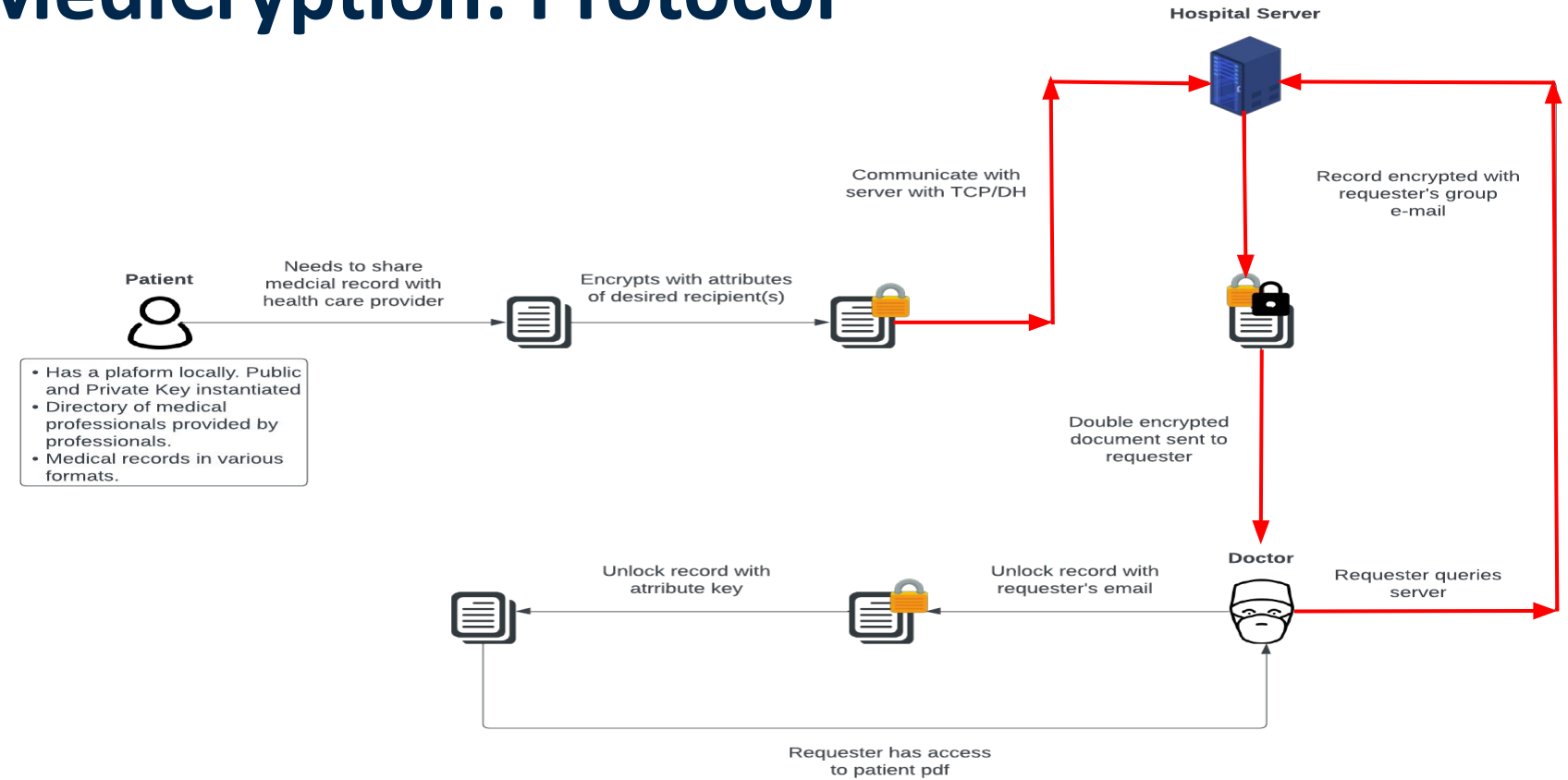
Takeaways: Expert Interview

- There is no reproducible way to send documents from one provider to another within a health system
- No standardized directory for the Michigan Medicine
  - We cannot automatically obtain all members of a given attribute group
- Everyone is treated as a potential bad actor
  - There is a need for revocability of access
- It is not feasible to share with one care provider and not another
  - The receiving doctor is legally obligated to make a note in the chart when making any decision
  - The associated document will be shared with everyone that has general access permissions

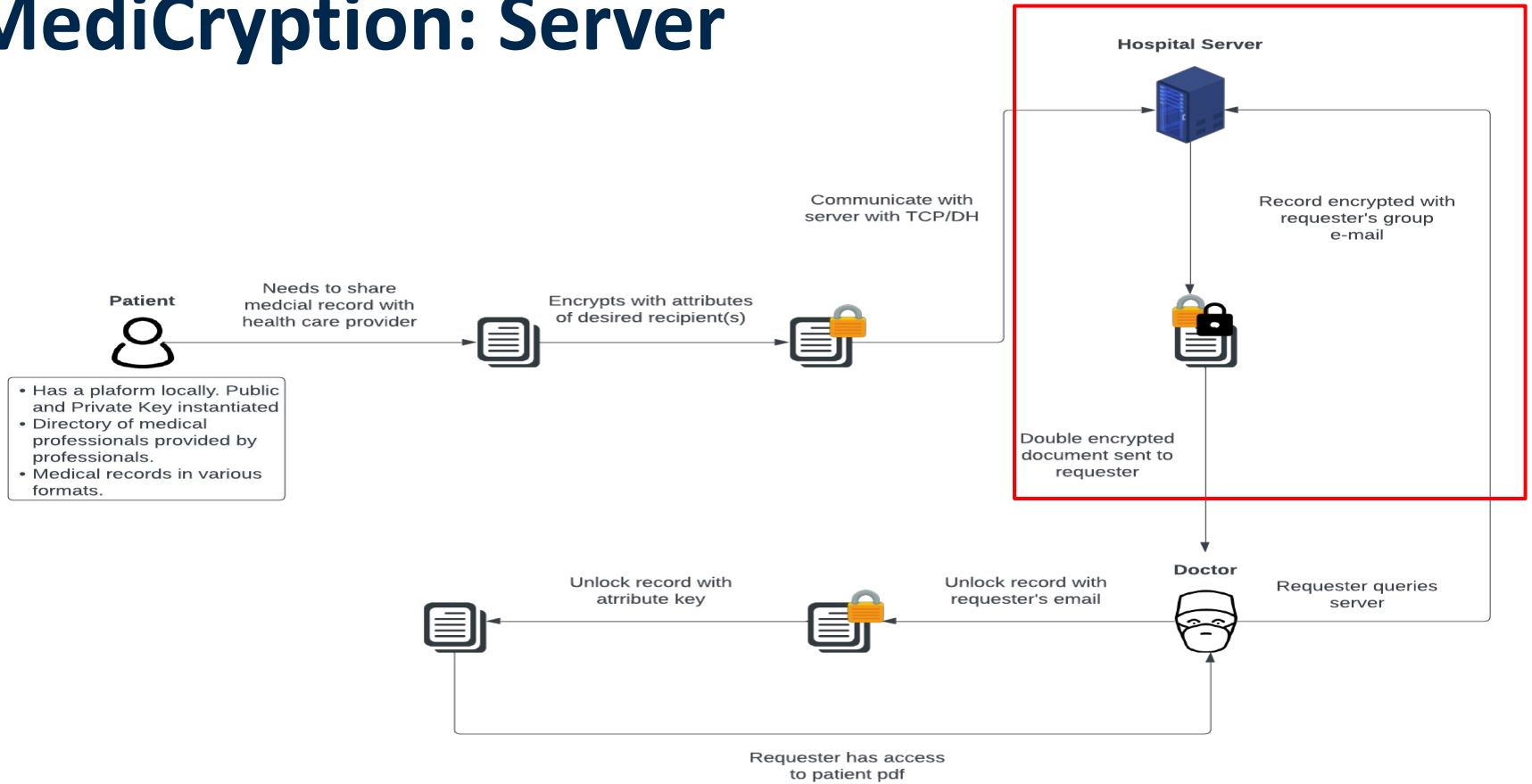
MediCryption: Patient Client



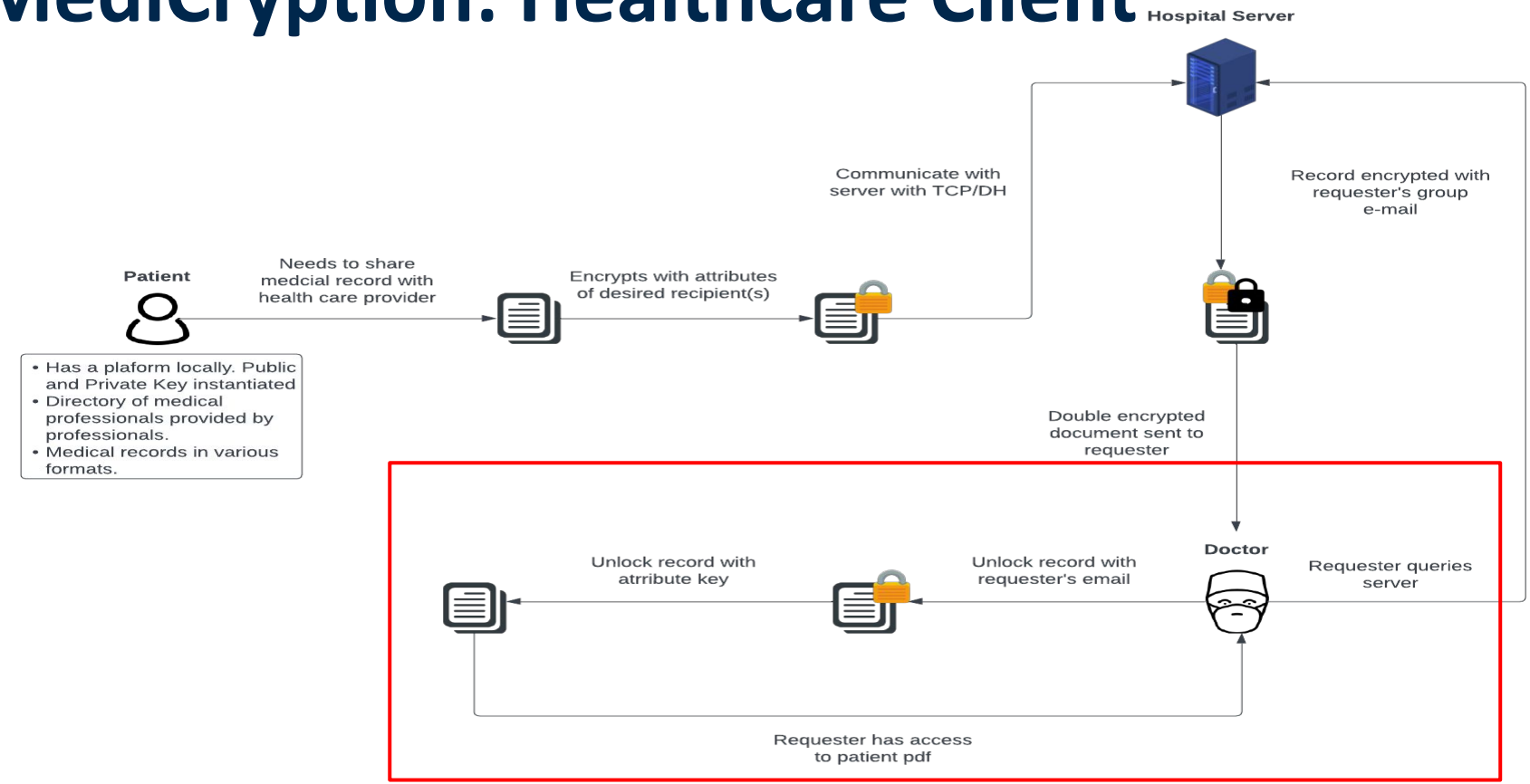
MediCryption: Protocol



MediCryption: Server



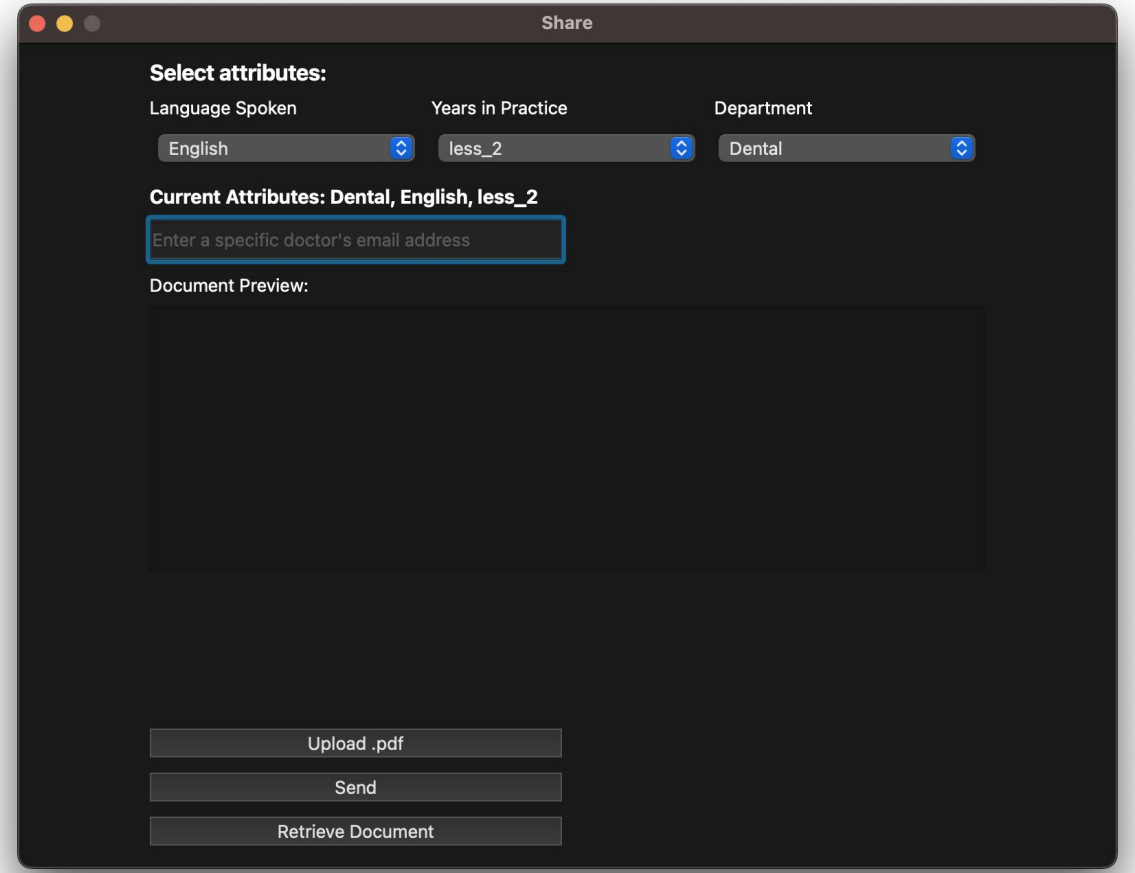
MediCryption: Healthcare Client



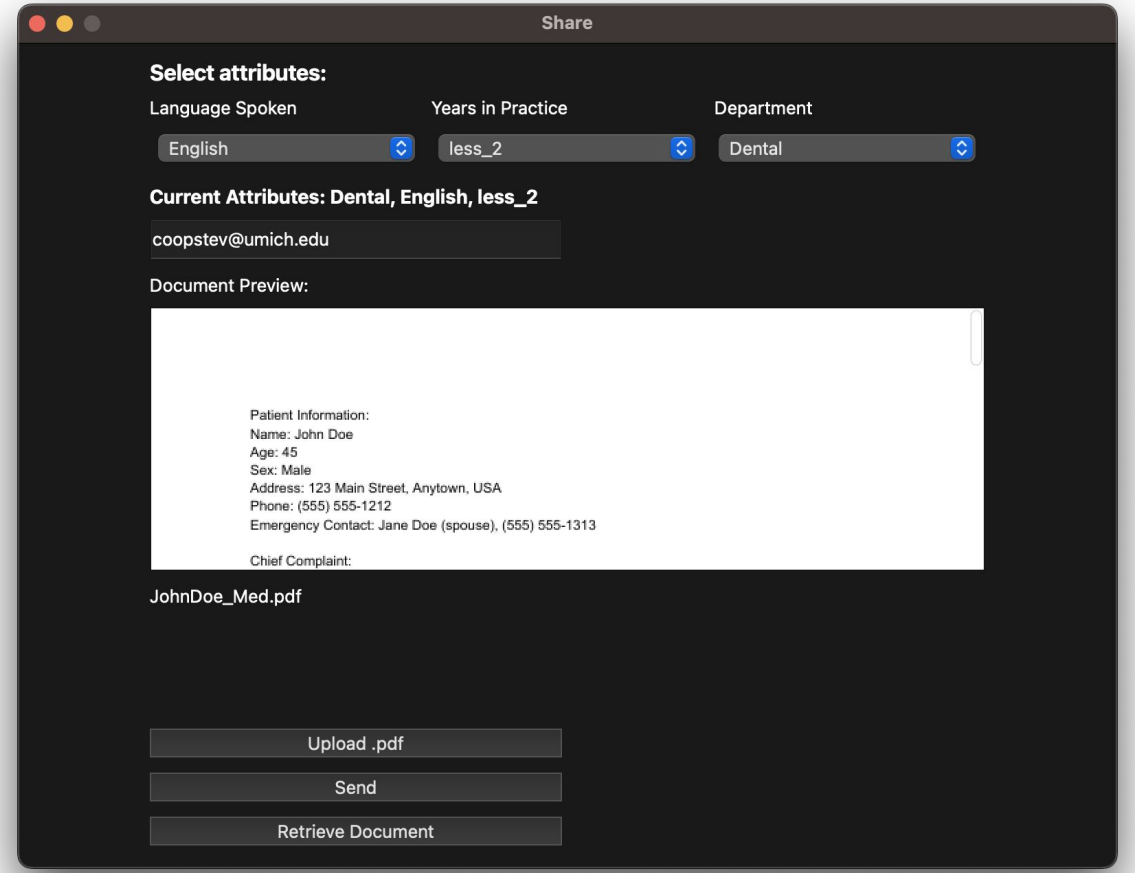
MediCryption Demonstration

Start page upon launching MediCryption

User may log in or sign up for the application

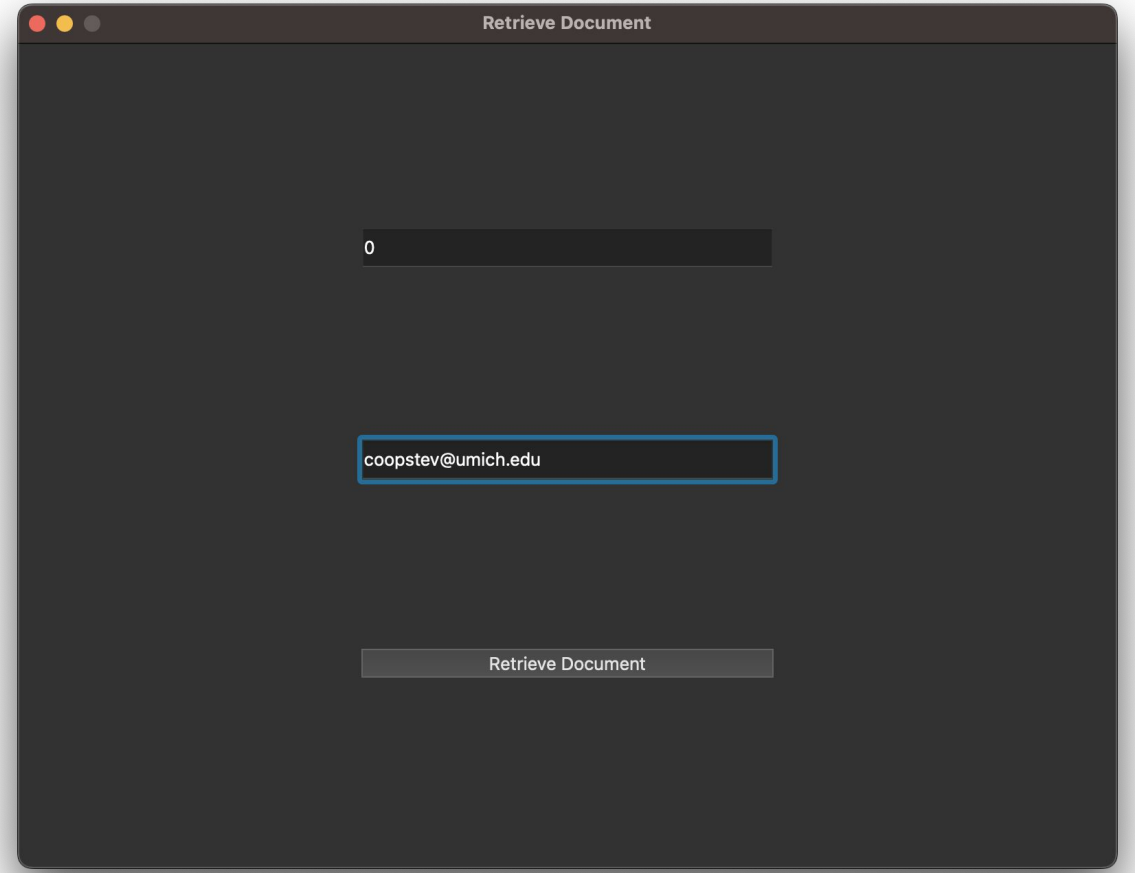


User may select a set of attributes using the drop down menu ui



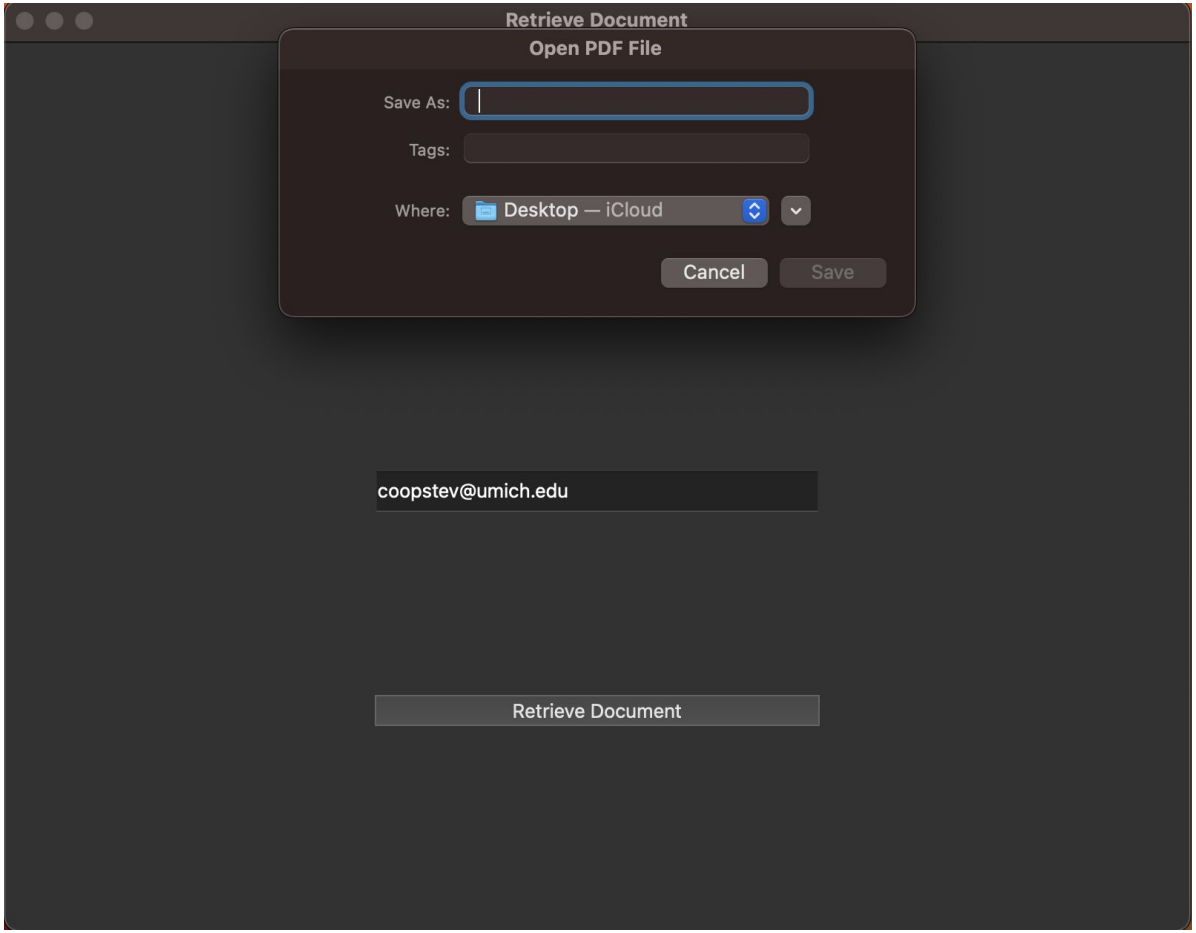
The user may upload the document and enter the recipient email address

This is protected with a shared secret computed using Diffie-Hellman

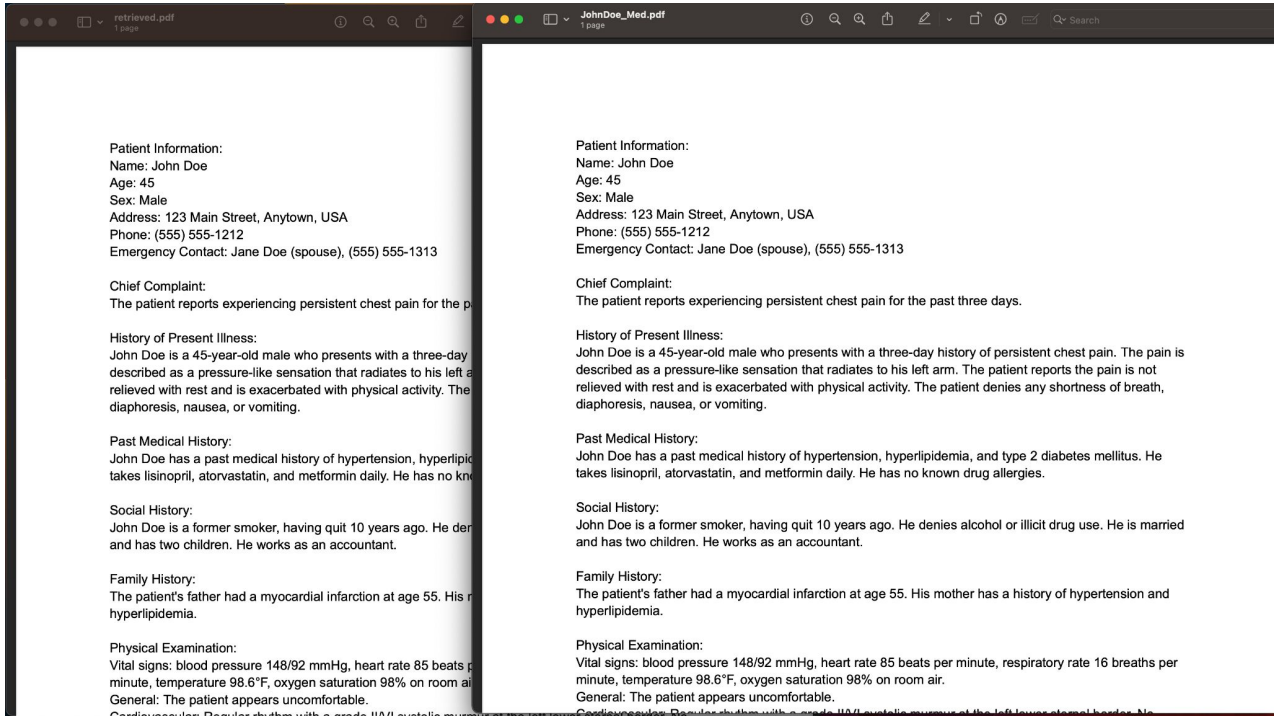


The recipient receives an email detailing a record that is available to them

The recipient may enter the DocID to retrieve the document



Once the document is retrieved, the recipient is able to store it locally



When retrieval is successful, the application will decrypt the ciphertext and show the document

Retrieved document

Sent document

Future Work

- Move away from Diffie-Hellman Key Exchange
- More user-friendly UI
- Security Hardening
  - Duo 2FA, Trusted Execution Enclaves
- Implement more robust revocation techniques
- Support additional forms of medical information
  - In particular, FHIR Records
- Provide means for practitioners to share updated records with patient
- Compress the ciphertexts

Conclusions

- A step towards practical, transparent systems
- ABE is promising but requires additional testing
  - Powerful tool to create a near zero-trust system
- ABE installation is complex!

Thank You!

Q&A