Secure Dissemination of EHR in Untrusted Cloud

Denis Ulybyshev¹, Bharat Bhargava¹, Leon Li², Jason Kobes², Donald Steiner², Harry Halpin⁴, ByungChan An¹, Miguel Villarreal¹, Rohit Ranchal³, Tim Vincent¹

¹Computer Science and CERIAS, Purdue University; ²NGC Research Consortium; ³IBM Watson Health Cloud; ⁴MIT

Tutorial

Table of Contents

| Initial Setup | |
|--|---|
| Secure Dissemination of EHR in Untrusted Cloud | 5 |

Initial Setup

Supported OS: Linux

- 1. Create a <Project_Folder>, go to that folder
 \$ cd Project_Folder
- 2. go to folder absoal6/console and install npm: \$ cd console \$ sudo npm install

node_modules folder must appear in the project directory. Then do the global update of "Express" framework :

\$ npm update -g express

3. Go to *Project_Folder/absoa16/scenarios/webcrypto* and run 'install' script. It will install npm for every service: doctor, insurance, researcher, hospital, authenticator.

\$./install

- 4. Install *mysql*: *\$ apt-get install mysql-server-5.6*
- 5. Set up MySQL database: \$ mysql -u root -p < db.sql
- 6. Install Java Runtime Environment. The project was tested under JRE version 8.
- 7. Run the project: go to *Project_Folder/absoa16/scenarios/webcrypto* and run 'start' script: *\$./start*

8. Open the browser, go to *http://localhost:3000/* (default port for prototype is 3000). Internet connection is required. You should see the page from Fig.1 below.

*To run prototype on a remote machine (not on localhost) modify 2 lines in the following source code files: *Project_Folder/absoa16/scenarios/webcrypto/hospital/public/index.html* and

Project_Folder/absoa16/scenarios/webcrypto/authenticator/public/index.html -replace localhost with real IP address where prototype (start script) will be running

Secure Dissemination of EHR in Untrusted Cloud

The server can be run either on a remote machine or on localhost. In our scenario server is running at waxedprune.com, port 3000. When you open the browser and type the following URL:

http://waxedprune.com:3000/
you will see the following page:



Fig.1. Secure Dissemination of EHR Main Page

| Ø | Secure Data Disseminat × 🕂 | | <i>.</i> | | 01 | Ŭ | | | | | | | |
|---------------|-----------------------------|-----------------------------|----------|-------------------------|----------|---|---|---|---|----|----------------|-------|-----|
| | ♦ ♦ (i) waxedprune.com:3000 | | | | C Search | | ☆ | Ô | ÷ | A | Ø 🍝 | = | = |
| • | Secure Dissemination of Ele | ectronic Healthcare Records | | | | | | | | | | | (1) |
| | НОМЕ | | | Request for Information | | | | | | | Flow | | L |
| | Scenarios | | | All | | | | | | | Jaliza | | L |
| | Hospital Service | | | User role | | | | | | | pane |) | |
| | | | | Doctor | | • | | | | | Clier | | |
| 1 | | | | Submit | | 2 | | | | | entic | | |
| | | | | | | | | | | | rogre | | |
| | | | \$ | | | | | | | | Polic | | L |
| Second | | | | | | | | | | | plica | | |
| | | | | | | | | | | | rogre | | |
| · P | | | | | | | | | | | etrie | | |
| | | | | | | | | | | | client | | |
| <u>الم</u> | | | | | | | | | | au | thori: data | | |
| | | | | | | | | | | | uala | | |
| | | | | | | | | | | | | | ų. |

Click "Hospital Service" button. Then you will see the following page:

Fig.2. Hospital Service Page

Select the role (Doctor, Insurance company or Researcher) and select information to request: 'All' or specific field, e.g. Contact Info of a Patient. Then click 'Submit' button. After that you will be redirected to authentication server (AS) web page, where you need to enter credentials. Since https protocol is used between client and authentication server, security exception needs to be added in the browser.



Fig.3. Adding security exception for https connection between client and AS



Fig.4. Security exception confirmation for https connection between client and AS



Fig.5. Password-based authentication of a Client at AS

If credentials entered by the Client are incorrect then data request is rejected. If credentials are correct then cryptographic capabilities of a browser are determined. If the level of cryptographic capabilities is high then Doctor will get data on behalf of 3 patients (see Fig.6), whereas if level of cryptographic capabilities is low then Doctor will get data on behalf of only 1 patient (see Fig.7). The idea behind this is that if level of cryptographic capabilities is high then Doctor can get data on behalf of patients assigned to other doctors, in addition to data of a patient (Monica Latte) assigned to the given Doctor.

| Secure | Data Dissemination with Active Bund | es - Mozilla Firefox | | 📼 en 🖂 🕴 🕇 🚛 🐠 🕽 | Ubuntu64BitCleanTalk 🔱 |
|--------|-------------------------------------|---|-----------------|------------------|---|
| Ø | Secure Data Disseminat × + | | | | |
| | Secure Dissemination of Elect | <u>.get?info=%26encryptedTicket%3Djwa76YilKTvKbDUO9evztYbVKoPLLJIWAe</u> nic Healthcare Records | ed4vYILZHyi7> C | ☆ 自 ♥ · | |
| | HOME Scenarios Result | Logged in as: Dr. J. Smith, MD Connected from: desktop Authentication method: token Authentication level: high | | | Flow visualization panel |
| | | Monica Latte, Female, Last Visit: 3 days ago John Adams, Male, Active Status L Smith, Female, Active Status | | | Client authentication in progress Policy application in progress |
| | | Actions: Send Medical Record to Patient's Insurance Comp Send Medical Record to University Research Part | | | Retrieved client's authorized data |

Fig.6. EHRs retrieved for Doctor with High Level of browser's crypto capabilities



Fig.7. EHR retrieved for Doctor with Low Level of browser's crypto capabilities

Each party (corresponding to the Role) interacts with an Active Bundle (AB), running on a cloud platform, to access only those data from AB for which the party is authorized.

If client (e.g. Doctor) clicks on a patient's record, then detailed information on behalf of that patient is displayed:

| Data Dissemination with Active Bund Secure Data Disseminat × + | iles - Mozilla Firefox | | n 🖂 | \$ 1 4 | €)) | 1 Ub | ountué | 4BitCl | eanTalk | с ф |
|---|---|--|---|---|---|---|--|---|--|--|
| (i 173.255.198.203:3001/proce | ss_get?info=%26encrypted | iTicket%3DYPJ7bLh%2BKvLbbCjJDYrCjtd%2Bpo%2BXnaBqqwy98! 🤇 🤇 Search | ☆ | Ê | | ŧ | 俞 | Q | | ≡ |
| Secure Dissemination of Electr | ronic Healthcare Reco | rds | | | | | | | | Ê |
| HOME | | Monica Latte, Female, Last Visit: 3 days ago | | | | | | Flo | w | |
| Scenarios | | Patient ID: | | | | | vis | | | n |
| Result | | 001122 | | | | | | | | |
| | | Contact info: Name: Monica Latte | | | | | aut | | | on |
| | N | Home Phone: 765 123 45 67 | | | | | in | prog | ress | |
| | 13 | Address: 4444 Coffee Ave Chocolate, California Office Phone: none | | | | | | Pol | icy | |
| | | Birth Date: 04/04/1950 | | | | | | | | |
| | | Gender: Female | | | | | in | prog | ress | |
| | | Marital Status: Divorced | | | | | F | | | |
| | | | | | | | a | | | |
| | | MedicalData | | | | | | da | ta | |
| | | Diagnosis: | | | | | | | | |
| | | DIABETES MELLITUS (ICD-250) | | | | | | | | |
| | Secure Data Disseminat × () 173.255.198.203:3001/proce Secure Dissemination of Electr HOME Scenarios | (c) 173.255.198.203:3001/process_get?info=%26encrypted Secure Dissemination of Electronic Healthcare Record HOME Scenarios | Secure Data Dissemination of Electronic Healthcare Records Secure Dissemination of Electronic Healthcare Records HOME Secure Dissemination of Electronic Healthcare Records Patient ID: 001122 Contact info: Name: Monica Latte Home Phone: 765 123 45 67 Address: 4444 Coffee Ave Chocolate, California Office Phone: none Birth Date: 04/04/1950 Status: Active Gender: Female MaricalData Diagnosis: | Secure Data Dissemination of Electronic Healthcare Records rome Scenarios Result Contact info: Name: Monica Latte Home Phone: 765 123 45 67 Address: 4444 Coffee Ave Chocolate, California Office Phone: none Birth Date: 04/04/1950 Status: Active Gender: Female Marital Status: Divorced SSN: 444 44-44444 Marital Status: Divorced SSN: 444 44-44444 Marital Status: Divorced SSN: 444 44-44444 | Secure Data Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Patient ID: 001122 Contact info: Name: Monica Latte Home Phone: 765 123 45 67 Address: 4444 Coffee Ave Chocolate, California Office Phone: none Birth Date: 04/04/1950 Status: Active Gender: Female Marital Status: Divorced SN: 444-44-4444 MedicalData Diagnosis: DIABETES MELLITUS (ICD-250) | Secure Data Dissemination Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Secure Dissemination of Electronic Healthcare Records Indef Ontice Latte, Female, Latt Visit 3 days ago Patient ID: Ontice Phone: none Birth Dat: Ontice Phone: None Marital Status: Divo | Secure Data Dissemination of Electronic Healthcare Records Image: Scenarios Patient ID: 001122 Contact info: Name: Monica Latte Home Phone: 765 123 45 67 Address: 4444 Coffee Ave Chocolate, California Office Phone: none Birth Date: 04/04/1950 Status: Active Gender: Female Marital Status: Divorced SSN: 444-44-4444 MedicalData Diagnosis: DIABETES MELLITUS (ICD-250) | Secure Data Dissemination of Electronic Healthcare Records Image: Contact info: Record Contact info: Name: Monica Latte Home Phone: 765 123 45 67 Address: 4444 Coffee Ave Chocolate, California Office Phone: none Birth Date: 04/04/1950 Status: Active Gender: Female Marical Status: Divorced SSN: 444-44-4444 MedicalData Diagnosis: DIABETES MELLITUS (ICD-250) | Secure Data Dissemination of Electronic Healthcare Records Incode: Beam Monica Latte, Female, Last Visit 3 days age Patient ID: 001122 Contact info: Name: Monica Latte Home: 765 123 45 67 Address: 44444 Coffee Ave Chocolate, California Office Phone: none Birth Data: 04/04/1950 Status: Active Gender: Female Marital Status: Divorced SSN: 444-444444 MedicalData Diagnosis: Diagnosis: Diagnosis: Diagnosis: | Secure Data Dissemination of Electronic Healthcare Records Incode: Beam Monical Latte, Female, Last Visit: 3 days spe Patient ID: 001122 Contact info: Name: Monical Latte Home: 765 123 45 67 Address: 44444 Coffee Ave Chocolate, California Office Phone: none Birth Date: 04/04/1950 Status: Active Gender: Female Marital Status: Divorced SSN: 444-44 4444 Diagnosis: Diagnosis: Diagnosis: Diagnosis: Diagnosis: Diagnosis: |

Fig.8. Detailed EHR of a patient retrieved for Doctor

Doctor can also select among 2 actions "Send Medical Record to Patient's Insurance Company" or "Send Medical Record to University Research Partner". Then Active Bundle, containing EHR on behalf of a patient, will be sent to another cloud, i.e. to corresponding service running in another cloud.

| Secure I | Data Dissemination with Active Bundles - Mozilla | Firefox | 📼 en 🖾 🕴 🕇 🚛 🐠 🕽 | 🗜 Ubuntu64BitCleanTalk 🖞 |
|-----------|--|--|------------------|--------------------------|
| 0 | Secure Data Disseminat × 🕂 | | | |
| | (173.255.198.203:3001/process_get?info=5 | 626encryptedTicket%3Djwa76YilKTvKbDUO9evztYbVKoPLLJIWAed4vYILZHyi7> 🛛 🕻 🛛 🔍 Search | ☆ 自 ♥ · | ↓ ☆ ♡ ▲ ▼ ≡ |
| | Secure Dissemination of Electronic Health | care Records | | |
| | HOME | Logged in as: Dr. J. Smith, MD | | Flow |
| E | Scenarios | Connected from: desktop Authentication method: token | | visualization |
| | Result | Authentication level: high | | panel |
| P | | | | Client |
| 120 | | Medical Record is sent to Insurance Company! | | authentication |
| | | Monica Latte, Fem | | in progress |
| | | John Adams, Male | | |
| | | | | Policy |
| | | L Smith, Female, Active Status | | application |
| ** | | | | in progress |
| 84 | | Actions: | | Retrieved |
| | | Send Medical Record to Patient's Insurance Company | | client's |
| · >_ | | Send Medical Record to University Research Partner | | authorized |
| | | | | data |
| <u>ڪ</u> | | | | |
| | | | | |
| | ar | | | |

Fig.9. EHR sent to service running in another cloud

According to specified Role-Based Access Control Policies, Doctor can get access to Contact, Medical and Billing Information of a Patient; Insurance company can get access to Contact and Billing information (see Fig. 10 below); Researcher can get access to Medical and Billing Information (see Fig.11 below).



Fig.10. Patient's data accessible by Insurance Company



Fig.11. Patient's data accessible by University Researcher

It should be said, that Active Bundle is tamper-resistant: if malicious user tries to modify policies

or AB code or bypass policy check then tamper attack will be detected and data access will be denied. Context-based and trust-based data dissemination is also supported by Active Bundles.

On the right side of web pages (see Fig.12) you can see flow visualization panel: it shows the phase of a data access process. Initially, client authentication phase is in progress. Then, after client enters correct credentials, data request is transferred to the Active Bundle and 'Policy application' phase starts. Then role-based access control policies specified in Active Bundle are applied abd finally, data for which the party (according to the Role) is authorized are retrieved and sent to the Client.



Fig.12. Flow visualization panel