MediTrack Health Care

Paulo Bolinhas 110976
Rui Martins 110890
Rui Moniz 99323

Actors

Our project as several actors that must be known first

01 Patients

02 Doctors

03 Insurance Company

04 Server

05 Database

Machines

How we implemented system distribution

01 Machine 1 - Client

02 Machine 2 - Server (Port 12345)

03 Machine 3 - Database Server (Port 50000)

```
sudo /sbin/iptables -P INPUT DROP
sudo /sbin/iptables -P FORWARD DROP
sudo /sbin/iptables -P OUTPUT DROP
```

```
sudo /sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo /sbin/iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
sudo /sbin/iptables -A INPUT -i lo -j ACCEPT
sudo /sbin/iptables -A OUTPUT -o lo -j ACCEPT
```

```
# Allow incoming SSL connections from VM2 to VM1
sudo /sbin/iptables -A INPUT -p tcp -s 192.168.1.254 --dport 12345 -j ACCEPT

# Allow outgoing SSL connections from VM1 to VM2
sudo /sbin/iptables -A OUTPUT -p tcp -s 192.168.1.254 --dport 12345 -j ACCEPT
```

Machine 1 – Client Firewall

- Set each channel Drop everything
- Allow established and related connections
- Allow communication with the loopback Interface
- Allow incoming and outgoing SSL/TLS communications with machine 2

```
sudo /sbin/iptables -P INPUT DROP
sudo /sbin/iptables -P FORWARD DROP
sudo /sbin/iptables -P OUTPUT DROP
```

```
sudo /sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo /sbin/iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
sudo /sbin/iptables -A INPUT -i lo -j ACCEPT
sudo /sbin/iptables -A OUTPUT -o lo -j ACCEPT
```

```
sudo /sbin/iptables -A OUTPUT -p tcp -s 192.168.0.100 --dport 12345 -j ACCEPT

# From VM2 to VM3
sudo /sbin/iptables -A OUTPUT -p tcp -s 192.168.1.1 --dport 50000 -j ACCEPT

# From VM2 to the internet
sudo /sbin/iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
```

Machine 2
Server Firewall

- Set each channel Drop everything
- Allow established and related connections
- Allow communication with the loopback Interface
- Allow incoming and outgoing SSL/TLS communications with machine 1 and 3

```
sudo /sbin/iptables -P INPUT DROP
sudo /sbin/iptables -P FORWARD DROP
sudo /sbin/iptables -P OUTPUT DROP
```

```
sudo /sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo /sbin/iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
sudo /sbin/iptables -A INPUT -i lo -j ACCEPT
sudo /sbin/iptables -A OUTPUT -o lo -j ACCEPT
```

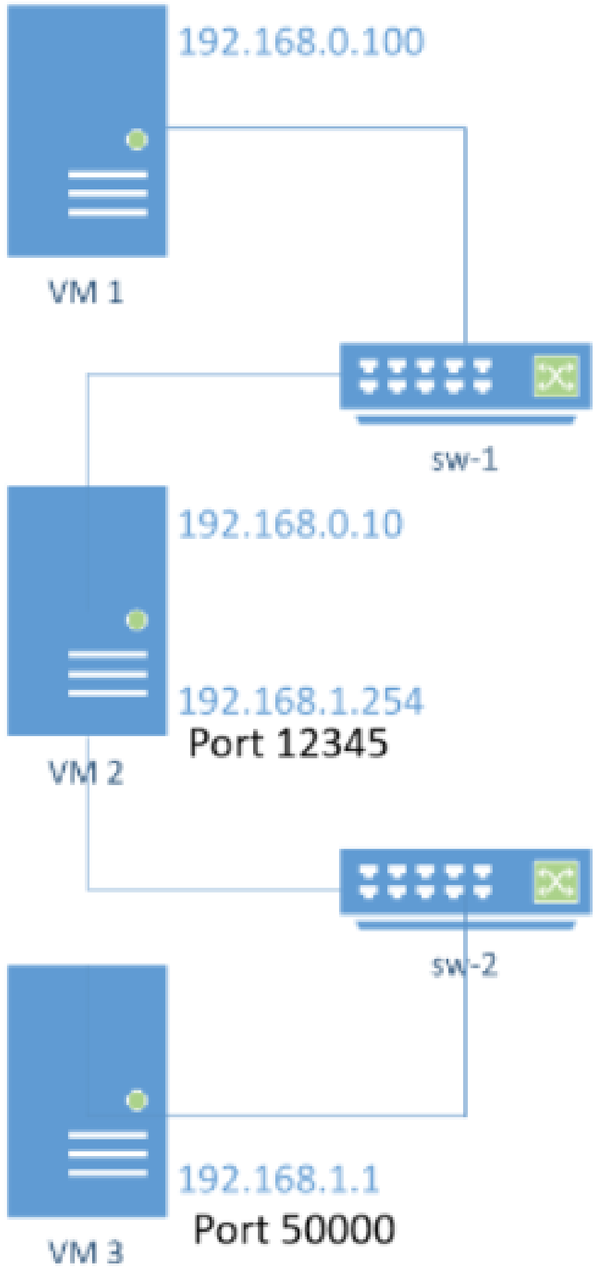
```
# Allow incoming SSL connections from VM2 to VM3
sudo /sbin/iptables -A INPUT -p tcp -s 192.168.1.254 --dport 50000 -j ACCEPT

# Allow outgoing SSL connections from VM3 to VM2
sudo /sbin/iptables -A OUTPUT -p tcp -s 192.168.1.254 --dport 50000 -j ACCEPT
```

Machine 3 Database Firewall

- Set each channel Drop everything
- Allow established and related connections
- Allow communication with the loopback Interface
- Allow incoming and outgoing SSL/TLS communications with machine 2

Network Structure



But how do these machines securily communicate?

MACHINE 1 – CLIENTS

- Client
  - Server Certificate
  - Other Entities
- Doctor
  - Server Certificate
  - Other Entities
- Insurance Company
  - Server Certificate
  - Other Entities

MACHINE 2 – SERVER

- KeyStore
  - Private Key
  - Certificate w/ Public Key
- TrustStore
  - Client Certificates
  - Database Certificate

MACHINE 3 – DATABASE

- KeyStore
  - Private Key
  - Certificate w/ Public Key
- TrustStore
  - Server Certificate

Views


```
{
 "patient": {
  "userId": "000000001",
  "name": "Bob",
  "sex": "Male",
  "dateOfBirth": "2004-05-15",
  "C.C.": "73606210 Z AR9",
  "NIF": "526890125",
  "insuranceCompany": "Freedom Insurance",
  "address": "Example Street, nº14",
  "phoneNumber": "935940912",
  "e-mail": "bob@email.com",
  "emergencyPhoneNumber": "921542859",
  "bloodType": "A+",
  "knownAllergies": ["Penicillin"],
  "knownIllnesses": ["Anemia"],
  "consultationRecords": [
   {
    "date": "2022-05-15",
    "medicalSpeciality": "Orthopedic",
    "doctorName": "Dr. Smith",
    "practice": "OrthoCare Clinic",
    "treatmentSummary": "Fractured left tibia;",
    "treatmentCost": "15.00",
    "paymentDestination": "00000001200201"
   }
  ]
```


Patient View

All fields get encrypted with patient's public key, so that only him can access it, as well as access it whole

Views


```
{
 "patient": {
  "userId": "000000001"
  "name": "Bob",
  "sex": "Male",
  "dateOfBirth": "2004-05-15",
  "C.C.": "73606210 Z AR9",
  "NIF": "526890125",
  "insuranceCompany": "Freedom Insurance",
  "address": "Example Street, nº14",
  "phoneNumber": "935940912",
  "e-mail": "bob@email.com",
  "emergencyPhoneNumber": "921542859",
  "bloodType": "A+",
  "knownAllergies": ["Penicillin"],
  "knownIllnesses": ["Anemia"],
  "consultationRecords": [
   {
    "date": "2022-05-15",
    "medicalSpeciality": "Orthopedic",
    "doctorName": "Dr. Smith",
    "practice": "OrthoCare Clinic",
    "treatmentSummary": "Fractured left tibia;",
    "treatmentCost": "15.00",
    "paymentDestination": "00000001200201"
   }
  ]
```


Unencrypted information, as it is simply identifying the record

Personal information, is encrypted with patient's public key, as it should never be made available to other users

Urgent information, is encrypted with patient's public key, as it is not to be shared.

Consult medical information, is encrypted with the respective speciality secret key

Financial information, is encrypted with insurance company's public key, to only be accessed by it

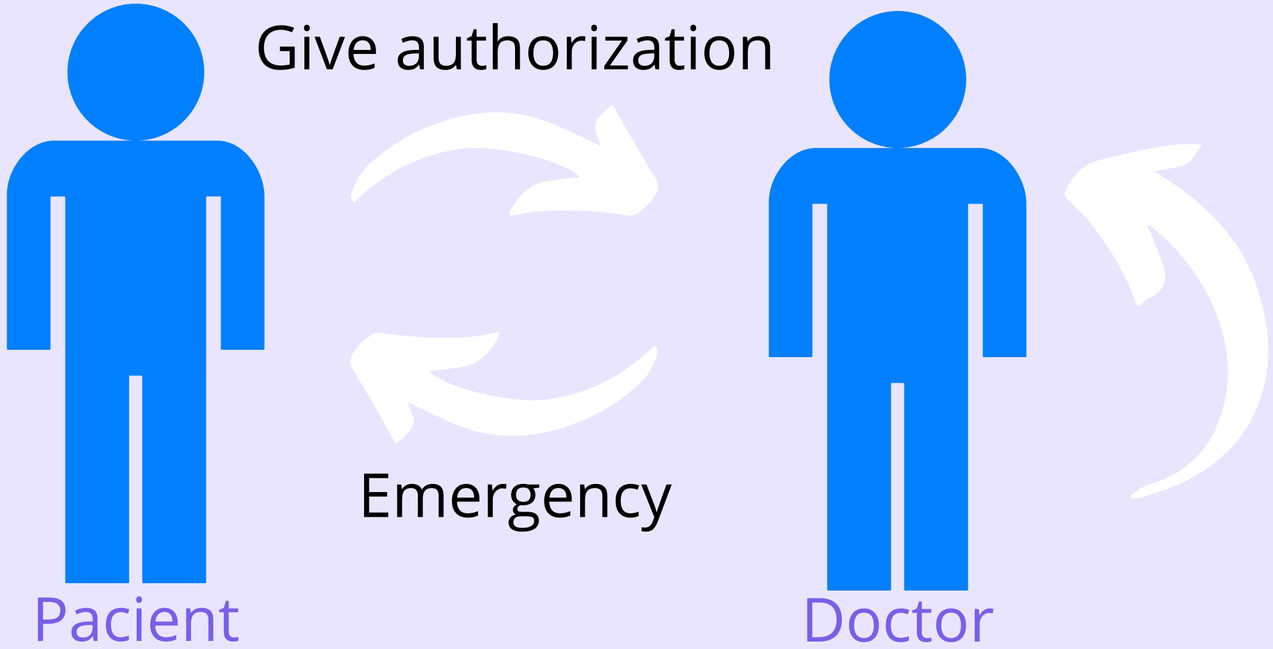
Views


```
{
 "patient": {
  "userId": "000000001",
  "name": "Bob",
  "sex": "Male",
  "dateOfBirth": "2004-05-15",
  "C.C.": "73606210 Z AR9",
  "NIF": "526890125",
  "insuranceCompany": "Freedom Insurance",
  "address": "Example Street, nº14",
  "phoneNumber": "935940912",
  "e-mail": "bob@email.com",
  "emergencyPhoneNumber": "921542859",
  "bloodType": "A+",
  "knownAllergies": ["Penicillin"],
  "knownIllnesses": ["Anemia"],
  "consultationRecords": [
   {
    "date": "2022-05-15",
    "medicalSpeciality": "Orthopedic",
    "doctorName": "Dr. Smith",
    "practice": "OrthoCare Clinic",
    "treatmentSummary": "Fractured left tibia;",
    "treatmentCost": "15.00",
    "paymentDestination": "00000001200201"
   }
  ]
```


Emergency View

All fields get encrypted with emergency speciality key, to work as a workaround to the normally sealed record by the patient public key

Security Challenge



Conclusion