NUSMED

A NHC Parody

Final Demo

IFS4205 Team 02
AY19/20

Agenda

1. System Summary

2. System Demo

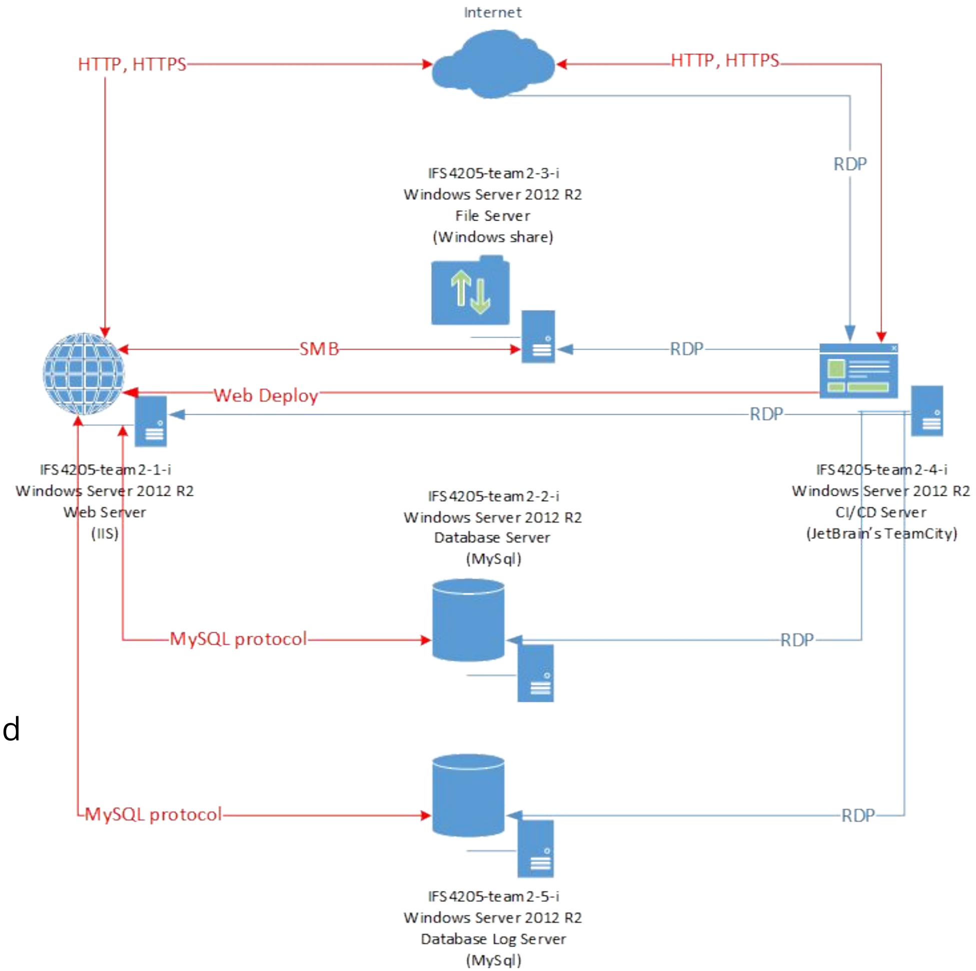
3. Security Claims and Security Mechanisms

4. Questions and Answers

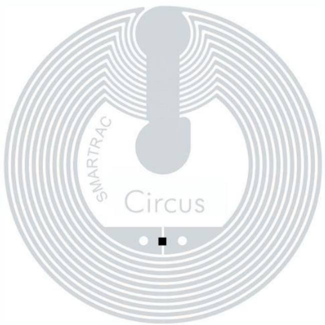
-System Summary-

System Architecture

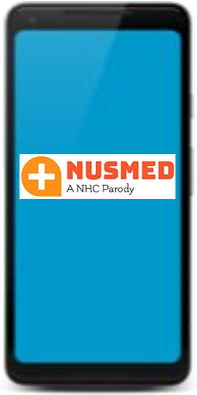
- 1x Web Server
  - IIS configured for TLS1.3
  - ModSecurity (WAF)
- 2x Database Server
  - Accessible from Web Server only (TLS1.2)
- 1x File Server
  - Authentication via AD (SMB 3.1.1)
  - File Server Resource Manager (FSRM) is enabled



Components for Users



NFC Tag



Mobile App

Web App

Authentication

- Web Application
  - Use of **Form Authentication** to hold authenticated sessions.
  - **ASP.NET Membership** is used to authorize roles to specific directories.

- Android Application
  - Use of NRIC + password + mobile device + NFC tag to authenticate
  - JSON Web Token (**JWT**)

Account Roles

Account Roles

- Patient
- Therapist
- Researcher
- Administrator (Clerk, Nurse, etc)

Accounts are able to possess multiple roles at the same time, but user can only log in as one role each time.

Permission System

Controls Patient Information and Records.

- Record Types
  - Therapists requests for and Patients approves. (whitelisting)
- Fine-Grain Record Permissions
  - To blacklist specific therapists from certain records. (blacklisting)
- Global Record Permissions
  - To “delete” records.

Patient information can be viewed by only approved therapists.

K-Anonymisation

- Datafly algorithm
- Quasi-identifiers: Age, Sex, Gender, Marital Status, Postal Code
- K: 3
- Suppression threshold: 10%

-System Demo-

-Security Claims-

Server and Infrastructure Security Claims (Items 1 - 2)

- S1-TLS
  - It is not possible to perform sniffing and man-in-the-middle attacks on the following connections due to TLS implementations.
    - Between NUS SOC reverse proxy and end users using the Web App and or Mobile App
    - Between web server (server 1) and main database (server 2); and logging database (server 5)
    - Between web server (server 1) and file server (server 4)

- S2-ACCESS
  - It is not possible to access any systems or services that are not intended to be accessible.
  - Mechanisms: Server configuration on all servers that whitelists access

Server and Infrastructure Security Claims (Items 3)

- S3-MOBILESTORAGE
  - It is not possible to retrieve the device ID or JWT from the shared preferences of NUSMed's mobile app via another application installed on the mobile device.
  - Mechanisms: Encrypted shared preferences (via the androidx.security.crypto library)

Web Application Security Claims (Items 1 - 3)

- W1-SQLINJECT: It is not possible to perform SQL injection attacks throughout the entire system.
  - Mechanisms: ModSecurity WAF, ASP.NET page validation, Parameterization

- W2-XSS: It is not possible to perform cross site scripting attacks throughout the entire system.
  - Mechanisms: ModSecurity WAF, ASP.NET page validation, HttpOnly Cookie

- W3-CSRF: It is not possible to perform cross site request forgery attacks throughout the entire system.
  - Mechanisms: Anti CSRF tokens

Web Application Security Claims (Items 4)

- W4-SESSION: It is not possible for any single user to initiate 2 concurrent sessions at any time; in that an account is able to be logged in more than once to achieve 2 concurrent sessions.
    - Mechanism: Server-side caching

Functional Claims, Access Control (Items 1 - 3)

- F1-JWT
  - It is not possible for attackers to craft or modify a JWT that enables him/her to authenticate and login.
  - Mechanisms: JWT Digital Signature

- F2-FORMAUTH: It is not possible for attackers to craft their own Form Authentication Cookie that enables him/her to authenticate and login into the web application.
  - Mechanisms: Cookie encryption, Server-side GUID caching

- F3-MFA: It is not possible for an attacker to perform unauthorized access without all three secrets: password, Device ID, Token ID.

Functional Claims, Access Control (Items 4 - 6)

- F4-KANON: It is not possible to identify a patient from the quasi-identifiers.
  - Mechanisms: Quasi-identifiers are generalised till number of records to be suppressed falls below the threshold

- F5-ACCESSCONTROL: It is not possible for therapist, patients or admins to perform any action outside of their given roles and permissions as according to functional specifications.

- F6-PASS: It is not possible to obtain any user account password via cracking, guessing or other means.
  - Mechanisms: Account lockout

Functional Claims, Access Control (Items 7 - 8)

- F7-RECORD: It is not possible to modify any record that had been previously uploaded; be it owned by him/herself and or others.

- F8-FILE: It is not possible for an attacker to upload file types or file sizes that is not specified to be allowed by the system.
    - This extends to exploiting the file upload to perform remote code execution, remote file inclusion and other related attacks.
    - Mechanisms: ModSecurity WAF, File Resource Server Management (FRSM)

-Resources for Pen-Testing-

Source Code and Documentation

- Web Application & Documents Repo:
  https://github.com/seanieyap/IFS4205-AY1920-S1-Team02-NUSMed-WebApp

- Mobile Application Repo:
  https://github.com/seanieyap/IFS4205-AY1920-S1-Team02-NUSMed-AndroidApp

Items to be Provided for Testing

- Team 01 will receive...
  2 x Patient Account, 1 x Therapist/Researcher Account (1 token each, 3 tokens total)
- CS3235 team (Wei Lin and Ahn Tae Gyu) will receive...
  1 x Patient Account, 1 x Therapist/Researcher Account (1 token each, 2 tokens total)
- Each user will require an Android phone (NFC capable) to install the Mobile Application.
- Subset of K-anon database

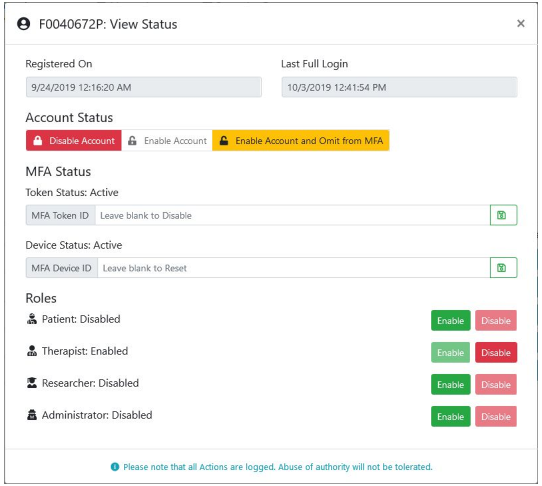
-End-

Thank you for everyone’s time and attention !

-Questions & Answers-

Registration

Admin assigns token



F0040672P: View Status ×

Registered On: 9/24/2019 12:16:20 AM

Last Full Login: 10/3/2019 12:41:54 PM

Account Status

MFA Status

Token Status: Active

MFA Token ID: Leave blank to Disable

Device Status: Active

MFA Device ID: Leave blank to Reset

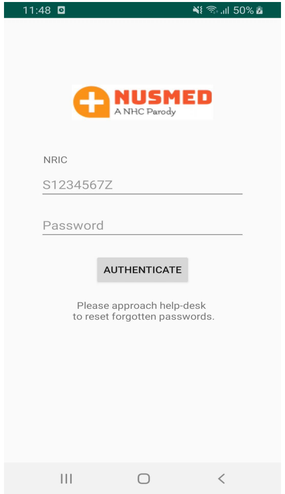
Roles

Patient: Disabled	Enable	Disable
Therapist: Enabled	Enable	Disable
Researcher: Disabled	Enable	Disable
Administrator: Disabled	Enable	Disable

Please note that all Actions are logged. Abuse of authority will not be tolerated.

- Token ID is a 128-bit UUID generated by java.util.UUID library
- Admin manually assigns a token to a user via admin console

User authenticates with registered credentials and issued token



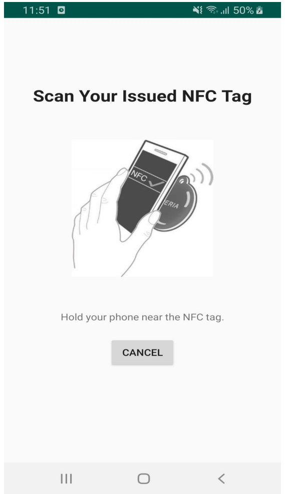
11:48 50%

NUSMED
A NHC Parody

NRIC: S1234567Z

Password

Please approach help-desk
to reset forgotten passwords.



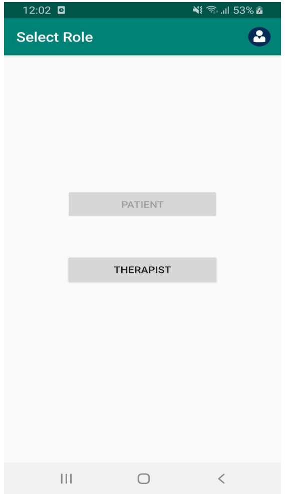
11:51 50%

Scan Your Issued NFC Tag

Hold your phone near the NFC tag.

- User downloads app which automatically generates a 128-bit device ID via the java.util.UUID library upon launch
- The device ID would be tagged to the user thus scanning the token from another phone would not work

User selects role



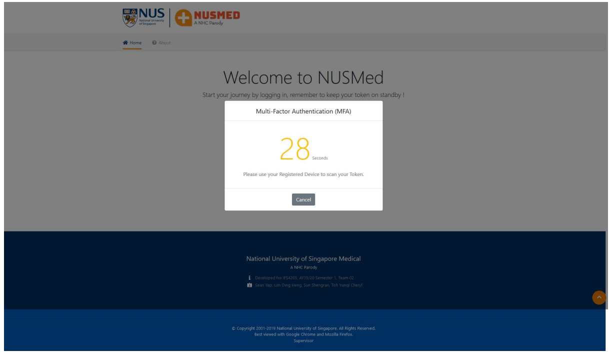
12:02 53%

Select Role

- User is able to select only the roles he has
- App is assigned a JWT which expires after 15 mins of inactivity

Web Login

User logs in on web app



Welcome to NUSMed

Start your journey by logging in, remember to keep your token on standby !

Multi-Factor Authentication (MFA)

28 Seconds

Please use your Registered Device to scan your Token.

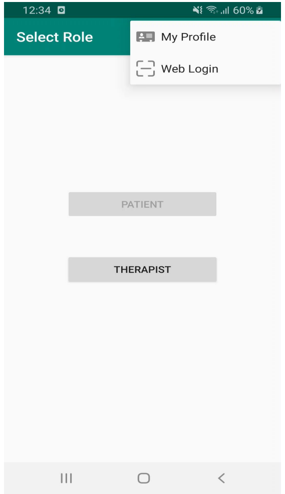
National University of Singapore Medical
A NHC Parody

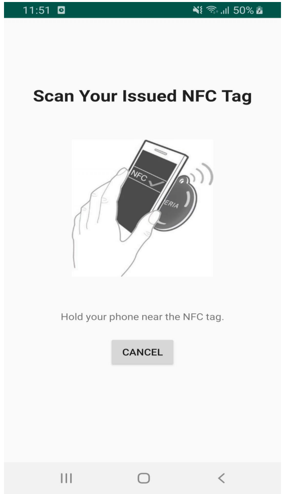
Developed for IFS4205, AY19/20 Semester 1, Team 02
Sean Yap, Lim Ding Heng, Sun Shengran, Toh Yunqi Cheryl

© Copyright 2001-2019 National University of Singapore. All Rights Reserved.
Best viewed with Google Chrome and Mozilla Firefox.
Supervisor

- User has 30 seconds to scan his issued NFC token via the mobile application

User selects web login on the mobile application





Scan Your Issued NFC Tag

Hold your phone near the NFC tag.

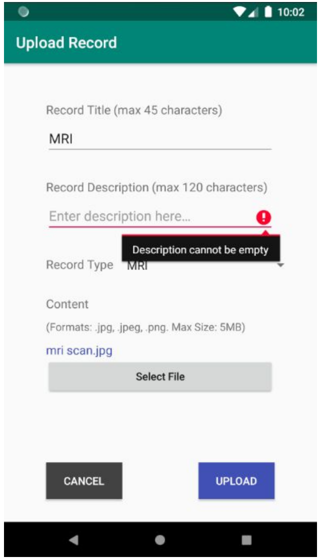
- App would send the device ID, token ID and the JWT to the server to be validated

Record Upload from Device

- ➢ Two security checks from mobile application side
  - ○ One check happens whenever user keys in a value / selects a file from local storage
  - ○ The other overall check happens when user clicks “Upload” button

- ➢ One security check from web server side
  - ○ Device ID + JWT
  - ○ User inputs (i.e. medical type, record content)

Patient Upload



Upload Record

Record Title (max 45 characters)

MRI

Record Description (max 120 characters)

Enter description here...

Description cannot be empty

Record Type MRI

Content

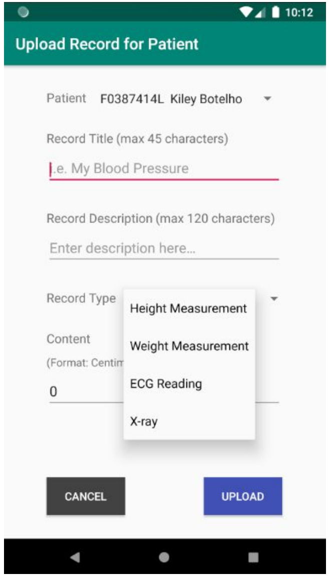
(Formats: .jpg, .jpeg, .png. Max Size: 5MB)

mri scan.jpg

NUSMED
A NHC Parody

Record Upload from Device

Therapist Upload



10:12

Upload Record for Patient

Patient F0387414L Kiley Botelho

Record Title (max 45 characters)

i.e. My Blood Pressure

Record Description (max 120 characters)

Enter description here...

Record Type

- Height Measurement
- Weight Measurement
- ECG Reading
- X-ray

Content

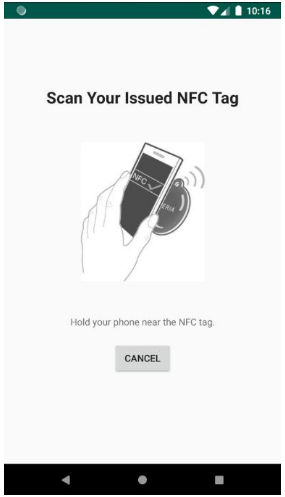
(Format: Centim

0

CANCEL UPLOAD

Only the medical types permitted by the patient are shown in the selection field.

Therapist Upload (for emergency patient)

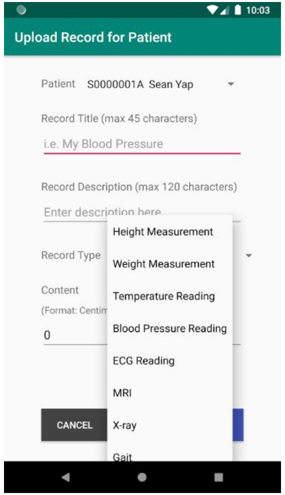


10:16

Scan Your Issued NFC Tag

Hold your phone near the NFC tag.

CANCEL



10:03

Upload Record for Patient

Patient S0000001A Sean Yap

Record Title (max 45 characters)

i.e. My Blood Pressure

Record Description (max 120 characters)

Enter description here

Record Type

- Height Measurement
- Weight Measurement
- Temperature Reading
- Blood Pressure Reading
- ECG Reading
- MRI
- X-ray
- Gait

Content

(Format: Centim

0

CANCEL

- Therapist assigned to the emergency patient can scan patient’s NFC to authenticated himself and to confirm the association.
- Therapist can upload any type of records for the emergency patient afterwards.
- After the patient becomes conscious again, he can reset the therapist's permission, and deny the ownership of records uploaded by the therapist when he was unconscious.