# SECURITY COMPUTER PROJECT

SECURE MEDICAL SYSTEM

Alessandro Spinosi
Guillaume Kerckhofs
Samain Clément
Randi Dochot
Alix Declerck

Abstract. The goal of this project is to implement a secure client / server system handling patient's medical records, such as the ones available in hospitals.

## Contents

## 1. Project description

## 2. Check-list

### 2.1. Confidentiality

Do I properly ensure confidentiality?

- Are sensitive data transmitted and stored securely?
- Are sensitive requests sent to the server transmitted securely?
- Do I achieve end-to-end encryption (if relevant)?
- Does a system administrator have access to the sensible data of some arbitrary user?

### 2.2. Integrity

Do I properly ensure integrity of stored data?

### 2.3. Non repudiation

Do I properly ensure non-repudiation?

- Do I use signature, certificates, a proper authority?

### 2.4. Strong authentification scheme

Do I use a proper and strong authentication scheme?

- Do I follow OWASP guidelines?
- Is my authentication broken (cf. OWASP 10) [1]

### 2.5. Relying secrecy

Do my security features rely on secrecy, beyond credentials?

### 2.6. Injection vulnerability

Am I vulnerable to injection?

- URL, SQL, Javascript and dedicated parser injections

### 2.7. Remanence attack vulnerability

Am I vulnerable to data remanence attacks?

### 2.8. Replay attack vulnerability

Am I vulnerable to replay attacks?

### 2.9. Fraudulent request forgery vulnerability

Am I vulnerable to fraudulent request forgery?

### 2.10. Monitoring

Am I monitoring enough user activity so that I can immediately detect maliciousor analyse an attack a posteriori?

- Do I simply reject invalid entries, or do I analyse them?
- Can logs be falsified?

## 2.11. Component security knowledge

Am I using components with know vulnerabilities?

## 2.12. System

Is my system updated?

## 2.13. Access control

Is my access control broken (cf. OWASP 10) [1]? Do I use indirect references to resource or functions?

## 2.14. General security features

Are my general security features misconfigured (cf. OWASP 10) [1]? Also, note that you will unlinkely graduate should you fail to

- use a (at least self-signed) certificate for your server,
- use a framework (at least for the server's side),
- achieve end-to-end encryption (if relevant).

## References

[1] "Owasp guidelines." [Online]. Available: https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

UMONS, Belgium
*Email address:* alessandro.spinosi@student.umons.ac.be

UMONS, Belgium
*Email address:* guillaume.kerckhofs@student.umons.ac.be

UMONS, Belgium
*Email address:* samain.clement@student.umons.ac.be

UMONS, Belgium
*Email address:* randi.dochot@student.umons.ac.be
*URL:* www.dochot.be

UMONS, Belgium
*Email address:* alix.Declerck@student.umons.ac.be