Exercises 1

Risks, Attacks and Security Goals

Group 3

Marcel Bernhardt, Ruben Ehritt, Eric Fiebig, Sabine Lenze,
Stefan Wasmer, Valentin Schwabe

04/23/2024

Contents

1 The individual Security Requirements

given: description of security requirements for a hospital information system
task: list the individual security requirements, the risks arising if they are not fulfilled and how to implement these requirements using the security mechanisms of today's standard operating systems

1.1 individual security requirements

- non-repudiability (integrity & authenticity) of life-critical data
- *CIA* of patient data / patient records / medical data bases / medical documents
- anonymity of patients and their records for research purposes
- integrity / availabilty of technical systems
- secure communication between different medical institutions

CIA **C**onfidentiality, **I**ntegrity, **A**vailability

1.2 risks

- incorrect treatment of patients and because of that possible harm to patients
  - wrong dosage of medication
  - no medication at all
- unauthorized access to patient data
  - exfiltration of data for ransom, blackmailing and selling
  - manipulation of data
    - getting access to medication like pain killers / opioids
  - usage of data in order to harm patients
    for example:
    - knowledge of a patient's allergies
    - changing a patient's blood type
- serious consequences for medical practice and patients
- admission of patients to the hospital is not possible when the systems / service are not available

1.3 implementation

- electronic authentication and encryption tools
  - having users with different roles and permissions
  - two-factor authentication
  - digital signatures
  - AQUA Protocol
- only be able to access data when you are inside the network
  - VPN
  - network segregation with different subnetworks
- role-based access control & time limitation of permissions
- proper anonymisation of patient data
  - k-anonymity in databases
- having backup procedures
  - 3-2-1 backup: 3 total backups, 2 different mediums, 1 backup offsite
- regular security audits and penetration tests
- regular updates of software and hardware
- security for standard attacks
  - firewalls
  - intrusion detection systems
  - antivirus software
  - buffer overflow protection
  - SQL injection protection