Paweł Rajba
pawel@ii.uni.wroc.pl
http://kursy24.eu/

Application Security Introduction

Agenda

- Application Security
- Information Security
- Basic concepts
- Security organizations

Introduction

- Application Security
  - From Wikipedia

    Application security encompasses measures taken throughout the code's life-cycle to prevent gaps in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application.
  - Part of non-functional requirements
  - Important to be taken into account from begining
  - Common problem: usually security is underestimated

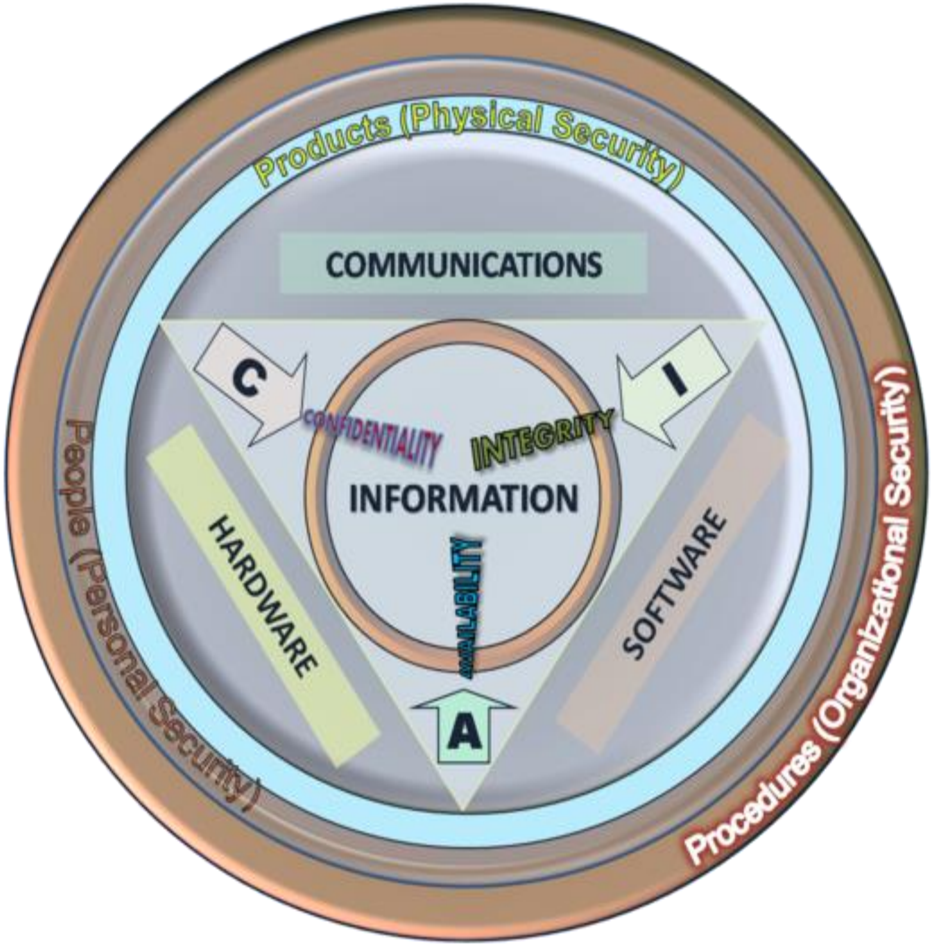
Introduction

- Information security
  - From Wikipedia:
    ***Information security**, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...)*

Introduction

- Information security basic concepts
  - Confidentiality
    - Preventing discloure information
  - Integrity
    - Consistency of data over its entire life-cycle
  - Availability
    - Information must be available when needed
  - Authenticity
    - Ensure that the data, transactions or documents are genuine
  - Non-repudiation
    - Ensure involved party can't deny his or her participation in activity

Introduction


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
HARDWARE
SOFTWARE
AVAILABILITY
A
People (Personal Security)
Procedures (Organizational Security)

Introduction

- Application security basic terms
  - Asset
  - Threat
  - Vulnerability
  - Attack
  - Countermeasure

Introduction

- Other concepts overview
  - Risk management
  - Controls (or countermeasures)
  - Defence of depth
  - Security classification for information
  - Access control
  - Business Continuity

Introduction

- Most important security organizations
  - OWASP
    - https://www.owasp.org/
  - WASC
    - http://www.webappsec.org/
  - SANS Institute
    - http://www.sans.org/
  - ISACA
    - https://www.isaca.org/
  - ISC2
    - https://www.isc2.org/
  - NIST
    - http://csrc.nist.gov/

References

- Application Security
  - http://en.wikipedia.org/wiki/Application_security
- Information Security
  - http://en.wikipedia.org/wiki/Information_security