Paweł Rajba
pawel@cs.uni.wroc.pl
http://itcourses.eu/

Application Security
Information Security

Agenda

- Introduction
- Concepts review
- Security requirements
- Security organizations

Security is as strong as the weakest link

…but in practice it is more complicated

Introduction

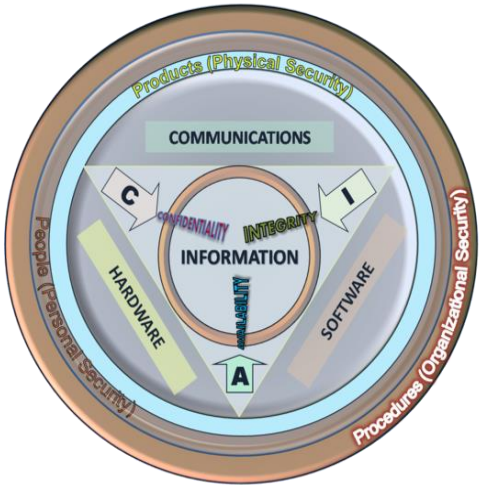
- Application Security
  - From Wikipedia
    Application security encompasses measures taken throughout the code's life-cycle to prevent gaps in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application.
  - Common problem:
    - usually considered in the end of dev when it is too late

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…)*

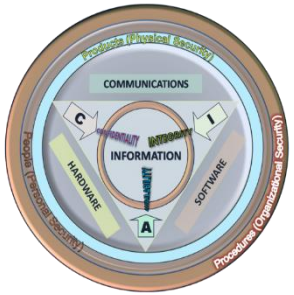
Basic concepts

- Information security basic concepts
  - Confidentiality
  - Integrity
  - Availability



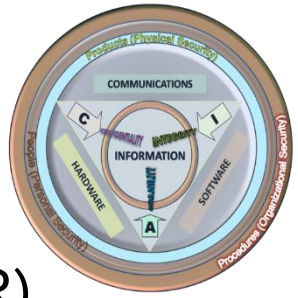
Basic concepts

- Information security basic concepts
  - Confidentiality
    - Preventing discloure information
      - It's about reading
    - Classification of information
      - Different ways, e.g.
        - Top secret, Secret, Official (in UK)
        - Confidential, Restricted, Internal use, Public (quite common)
      - *Clearance*: rules controlling the level of permission required to view information and how it must be stored, transmitted, and destroyed
      - Term ***need-to-know***
      - Time perspective („how long" and „it may change")
      - NDA agreements



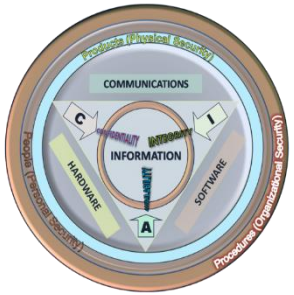
Basic concepts

- Information security basic concepts
  - Privacy (often confused with secrecy)
    - The General Data Protection Regulation (GDPR)
      - https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
    - Worth to watch
      - https://www.youtube.com/watch?v=NIf7YM71k5U (3 min)
        - Let's see this one
      - https://www.youtube.com/watch?v=pcSlowAhvUk (20 min)



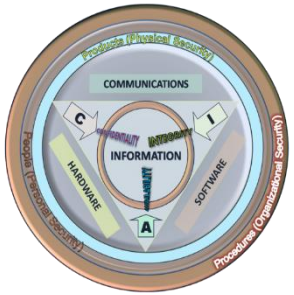
Basic concepts

- Information security basic concepts
  - Integrity
    - Consistency of data over its entire life-cycle
    - It's about writing
    - Often missed classification, but good to have as well
    - When confidentiality is low, but integrity high?



Basic concepts

- Information security basic concepts
  - Availability
    - Information must be available when needed
    - Usually regulated by SLA
      - Be carefull to what SLA is related to? Solution or component?
    - Connected with Service Continuity (Plans)
    - Number of 9 matters:
      - 99% = **3d** 15h 39m 29.5s
      - 99,9% = **8h** 45m 57.0s
      - 99,99% = **52m** 35.7s
      - 99,999% = **5m** 15.6s
        - Nice calculator: https://uptime.is/



Have we covered everything?

More concepts

- Information security basic concepts (more)
  - Authenticity
    - Ensure that the data, transactions or documents are genuine
  - Non-repudiation
    - Ensure involved party can't deny his or her participation in activity
  - Traceability
  - Anonymity

Have we covered everything now?

No, not really.
But we need a structured way
to capture the needs

Security requirements

- Security is usually considered as a part of non-functional requirements
- Most often we can consider 2 main sources
  - Customer's expectations
    - Authorizations, SSO, authentication method
  - Law and regulations (both internal and external)
    - PCI-DSS, HIPPA, GDPR, internal policies & directives
- Needs to be part of business requirements

Security requirements

- Clear, explicit and complete documentation
  - E.g. importance of shared understanding of authZ
- Prototypes (authZ matrix, flows)
- Part of definitione of done in product backlog
- How to test security requirements?
  - Part of test strategy
  - Concept of abuse bases:
    - Use case: The system allows bank managers to modify an account's interest rate
    - Abuse case: A user is able to spoof being a manager and thereby change the interest rate on an account

Security requirements

- All further consideration during these classes will be to satisfy some set of security requirements.
- For instance:
  - Confidentiality: Encryption, Access control
  - Integrity: Access Control
  - Availability: Backups
  - Authenticity: Authentication
  - Non-repudiation: Logs
    - Is the above list enough and complete?

Basic terms

- Asset
- Threat
- Vulnerability
- Exploit
- Attack
- Controls (or countermeasures)
- Risk management
- Defence of depth
- Access control
- Principle of Least Privilege

Security organizations

- Most important security organizations
  - OWASP: https://www.owasp.org/
    - OWASP Top 10
    - OpenSAMM
    - ASVS
  - WASC: http://www.webappsec.org/
    - Web Application Security Scanner Evaluation Criteria
    - Web Application Firewall Evaluation Criteria
    - Web Security Threat Classification
  - SANS Institute: http://www.sans.org/
    - GIAC certifications
    - Many trainings
    - A lot of articles
    - CWE/SANS Top 25 Most Dangerous Software Errors (joint with MITRE)

Security organizations

- Most important security organizations
  - ISACA: https://www.isaca.org/
    - CISA, CISM, CRISC, CGEIT certifications
    - COBIT framework
    - Trainings, a lot of events
  - ISC2: https://www.isc2.org/
    - CISSP and many other certifications
    - Trainings, a lot of events
  - NIST: http://csrc.nist.gov/
    - FIPS standards
      - e.g. FIPS 197 (AES), FIPS 140-2 (crypto modules)

References

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