Course title: Information security and privacy

Course code: 63521

ECTS: 6

Professor: Denis Trček

Master's program

Short course decription:

- Introduction.
- Key standards and organizations (ISO, ITU-T, IETF, W3C, OASIS, OMA).
- Risk management.
- Security mechanisms (symmetric and asymmetric algorithms, strong one way hash functions, homomorphic cryptography), security services (principles and practical implementations of authentication, confidentiality, integrity, non-repudiation, access control, logging and alarming), public key infrastructure (time base, name space management, operational protocols), post-quantum computing (quantum key exchange, Lamport crypto scheme), side channels problems and countemeassures.
- Engineering issues related to securiity mechanisms.
- Authentication, authorization and accounting infrastructure (principles, examples of standardized solutions like RADIUS and Diameter).
- Security of physical and data layers (example protocols are WEP, WPA, WPA2 and WPA3).
- Security of network, transport and application layers, including internet of things and clouds (example protocols and applications included are IPSec, TLS, S/MIME, XMLSec, SAML, XACML, WS-*, Bitcoin and blockchains, Passkey).
- Formal methods (taxonomy of formal methods with examples like R. Rueppl's method and SPIN / Promela).
- Privacy (privacy by design) with trust management and reputation management in services oriented architectures.
- New security paradigms – Interenet of Things and cloud computing.
- Secure programming practices and verification (model checking).
- Risk management in information systems, organizational views and human factor views (security policies, human factor modelling and simulations).
- Accreditation and auditing of IS related to security (ISO 2700X, CISSP), standards for technical implementations of hardware and software components (Common Criteria), and standards for security management of artificial intellignece solutions.
- Basic legislation in the area of IS security and privacy (EU directives, national implementations).
- Conclusions.
- Addendum: Mini practical tasks covering the latest selected technological issues.