The need for security

- Mission-critical applications use sensitive information that need protection
- Sensitive information is exchanged over public networks
- Security design is usually not considered from the beginning of software development
- Availability of hacking tools
- Security requirements
  - Authentication
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
  - Reliability
Healthcare security

• DITIS system
• Security infrastructure covering People – Systems – Procedures
  – Hardening security of components by configuring security features
  – PKI infrastructure
  – VPN connections for remote administration
  – Access control though role-separation
  – Security policies (i.e. password creation, updates, system usage, backups, fails safe plan etc)
  – Security education and training program
  – Legal documents supporting the Data Protection Law
    • Developers
    • Medical and paramedical personnel
    • Patients
WSN Security

• The need for security is even more critical in WSNs

• WSNs are used in many sensitive areas i.e. healthcare, military, environmental-related etc

• Limitations drive the security implementation in WSNs
  – Limited resources (energy, computation power, storage)
  – Hostile environment
  – Random topology
  – Dynamically changing topology
  – Insecure wireless medium
  – Attacks
WSN Key Research Security Areas

• Secure routing
  – Secures the routing process

• Key management
  – Procedures related to the generation, exchange, update and revocation of encryption keys

• Trust management
  – Builds and manages trust relationships between nodes

• Intrusion detection
  – Monitors the behavior of nodes and detects malicious activities

• Secure localization
  – Sensors securely determine their location

• Secure data aggregation
  – Secures the communication between nodes and aggregators
WSN Security Framework

• Integration of the key security areas under a common framework to support a spherical security approach
• A cross-layer approach to promote the efficient and effective cooperation of the security areas
• Support of adaptable security features based on operational conditions, security and application requirements
Routing in WSNs

- Mission-critical applications require a reliable operation
- Availability, reliability, resilience through multipath routing
- Confidentiality, integrity, authentication through secure routing
Secure multipath routing in WSNs

- Activities
  - *Threat model specification*, identifying adversary’s objectives and strategies against secure multipath routing protocols
  - *Design and evaluation framework development*, promoting the design of new protocols, their security assessment and comparison with similar protocols
  - *New protocol development*
    - addressing limitations of existing protocols
    - considering the security aspects of multipath routing instead using it only as a delivery technique
    - interoperating with other security areas to establish a secure, reliable and resilient multipath routing operation
  - *Attack patterns identification*, supporting intrusion detection features