Lecture 1

maandag 6 februari 2023 14:45

first lectures will also be part of exam

this course emphasizes IoT networks, instead of IT networks
↓
which introduce several constraints

IEEE 802.15.4 Zigbee
IEEE 802.11 wifi

a security service is a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers

fundamental security services, i.e. objectives

- **authentication**: assures claimed ID is correct; either peer or data can be authenticated
  - → source/dest are intended ones (not content!)
  - → in connection-oriented transfer, provides confidence that one is communicating with claimed ID
- **access control**: having rights to perform a given action
- **confidentiality**: guarantees data are received only by intended receiver — helps to prevent passive attacks
- **integrity**: assures data has not been maliciously modified — helps to prevent active attacks
- **non-repudiation**: ensures sender/receiver cannot deny having sent/received a particular message
- (+1) **availability**: system always being available & ready to serve requesting entities

trust + privacy are not fundamental:
- they do not necessarily imply communication
- their definition is not strictly security-related

a security algorithm is a mathematical procedure applied to secure data

a security protocol is a sequence of operations providing one or more security services to the data or communication, through one or more security algorithms

many different types:
- authentication protocols
- authenticated encryption protocols
- key management protocols

a security framework is a series of documented processes that define policies and procedures around the implementation and ongoing management of information security controls

≃ set of objectives
generally in non-specific way

algorithms: ECDH
- not asymmetric cryptography; they are classes of algorithms
- hashing is a class of algorithms
- X.509 but not exactly; more like a format (of certificates)

protocols: TLS
WPA

key agreement is a class of both algorithms and protocols