

# Video surveillance networks

A person is seated at a desk in a control room, monitoring a large array of video surveillance cameras. The room is dimly lit, and the monitors display various outdoor scenes, including streets and buildings. The person is wearing a light-colored shirt and is looking towards the screens. The overall atmosphere is one of focused surveillance.

Aleksandra Karimaa

---

# Surveillance systems

- Real-time content distribution
  - Storage solution
  - Management system
  - User interface
-

---

# Video surveillance systems

- IP-based
  - Real-time video
  - Compression
  - Data and audio - addition to video content
  - Recording of video with associated system data
  - User interface with video displaying
  - Event management
-

---

# Challenges for networks

- Real-time streams - bandwidth, delay
  - Movement of stored data
  - System distribution
  - Open architecture
  - Reliability - networking infrastructure, redundant paths and nodes
  - Scalability – modularity, grouping
-

---






# Risk factors

- Data movement
  - Multicast
  - Availability of resources
  - System components:
    - untrusted storage
    - independent security domains
    - client communication
-

---

# Security services..

## .. and mechanisms

- Confidentiality       Authentication mechanisms, encryption, digital signature
  - Data integrity       Error detection algorithms, error recovery mechanisms
  - Access control       Client communication, user rights
  - Data availability       Mirroring, RAID, backups
  - Resilience       Redundancy mechanisms
-

---

# Closed networks security

- Characteristics:
    - ❑ Often analog
    - ❑ Physical access
    - ❑ Expensive
    - ❑ Local
    - ❑ No public services
  - Security:
    - ❑ Access control on physical level
    - ❑ Resilience – physical redundancy
-

---

# Open networks

- Characteristics:
    - Connected to public domain to use internet services
    - Automated
    - User- friendly
    - Low cost (maintenance)
-



---

# Open networks security

- Access control and confidentiality the most important
    - Monitoring
    - Authentication for Client interface and resources access based on identity not physical location
    - Confidentiality: Authentication mechanisms, encryption, digital signature
    - Encryption on routing, node access passwords, TCP authentication, route filters, private addressing
  - Data integrity – checksums for transmission and storage
  - Data sharing and resilience – redundancy mechanisms, RAID
-

---

# Semi-open networks security

- System uses only few internet services (protected, unidirectional access)
  - Security
    - Access control – authentication for client
    - Confidentiality – encryption of exported content
    - Data integrity – checksums for transmission and storage
    - Data sharing and resilience – redundancy mechanisms, RAID
-

---

# Thank you

- Contact:  
Aleksandra.Karimaa at teleste.com  
or  
Alkari at utu.fi
-