Security in Motion

Securing telemetry – based applications

Who we are

- Founded in 1999 – Part of G4S global organization
- Greek market leader in Telematics – over 6500 vehicles tracked and managed in Greece
- Deployed the C4i AVL solution for the Olympic Games 2004
- Participates in European research programs in fields of telemetry and biometrics
- Project management & solution provider for tracking of over 13.000 people and vehicles throughout Europe
- TAPA (Transported Asset Protection Association) member

What we offer

- Security consulting (TAPA FSR-TSR, Risk Assessment)
- Monitoring & response
  - Safety of people – lone workers
  - Security of assets – location, environment
- Reports of live and historical metering data
  - locations of the vehicles / assets / persons tracked
  - tracking metering (speeds, routes, stops)
  - security – related data (vehicle driver, doors opened)
  - environmental monitoring / metering (temperature)

What do we want to protect?

- Human life : Somebody **asks** for help – Interactive
  - Driver of a vehicle under attack (jewelry, money …)
  - Lone worker under attack (guard)
  - Elderly, youngsters or disabled people in need
- Assets : Vehicles, merchandise – Automated
  - An asset is moving outside of allowed times / regions
  - A vehicle is moving with its engine off
  - Breach of speed limits

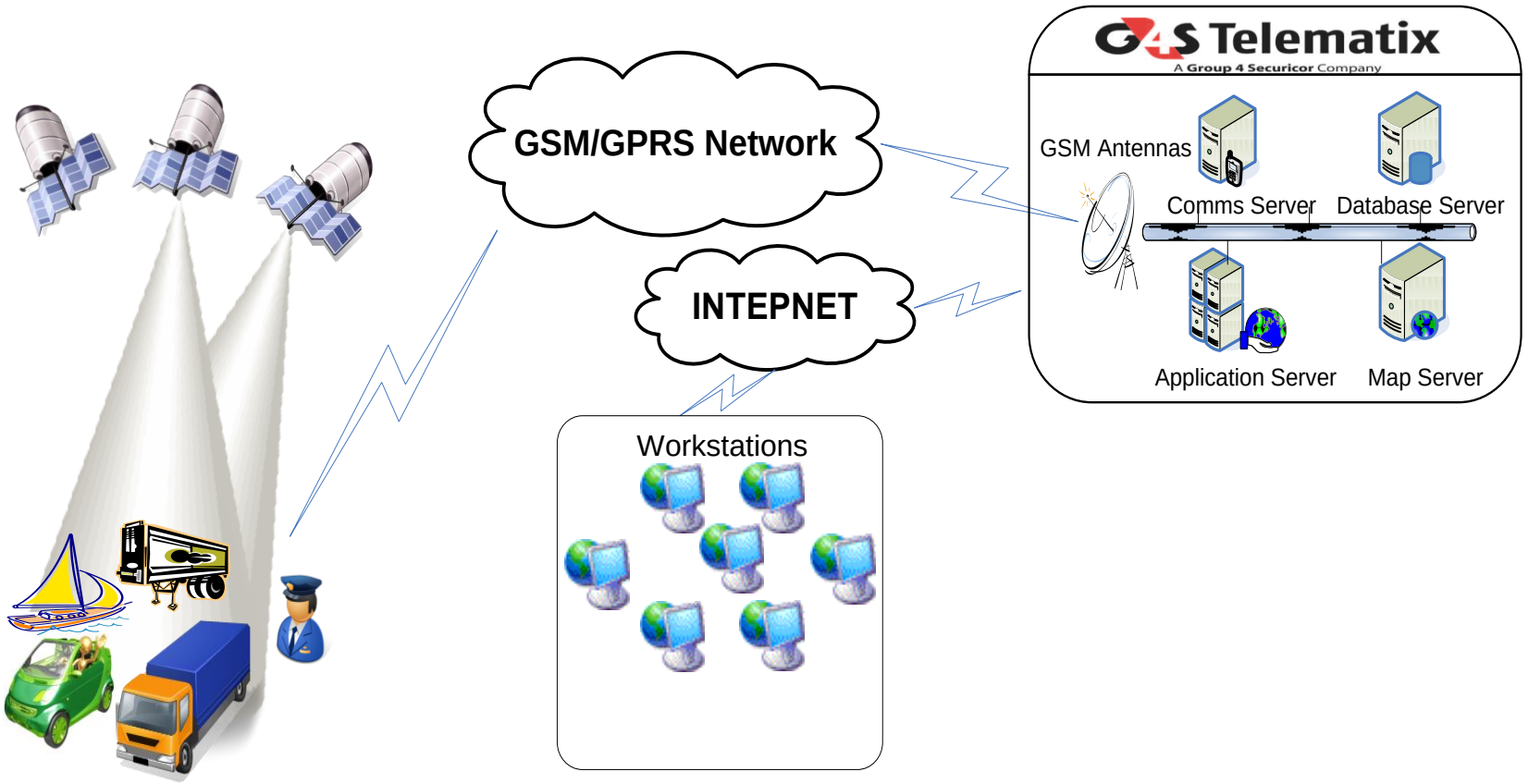
What do we want to protect?

- Physical security : access control of moving assets
  - An unauthorized driver attempts to start a vehicle
  - A combination of actions is identified indicating intrusion
- Environmental metering and security
  - Environmental readings have changed over a threshold
  - Somebody's utility consumption is raising unusually
  - Automatic metering for charging

Requirements

- Data is measured
- … and it is sent over the air
- … to be properly evaluated
- … so that actions are taken
- … and required reports are produced

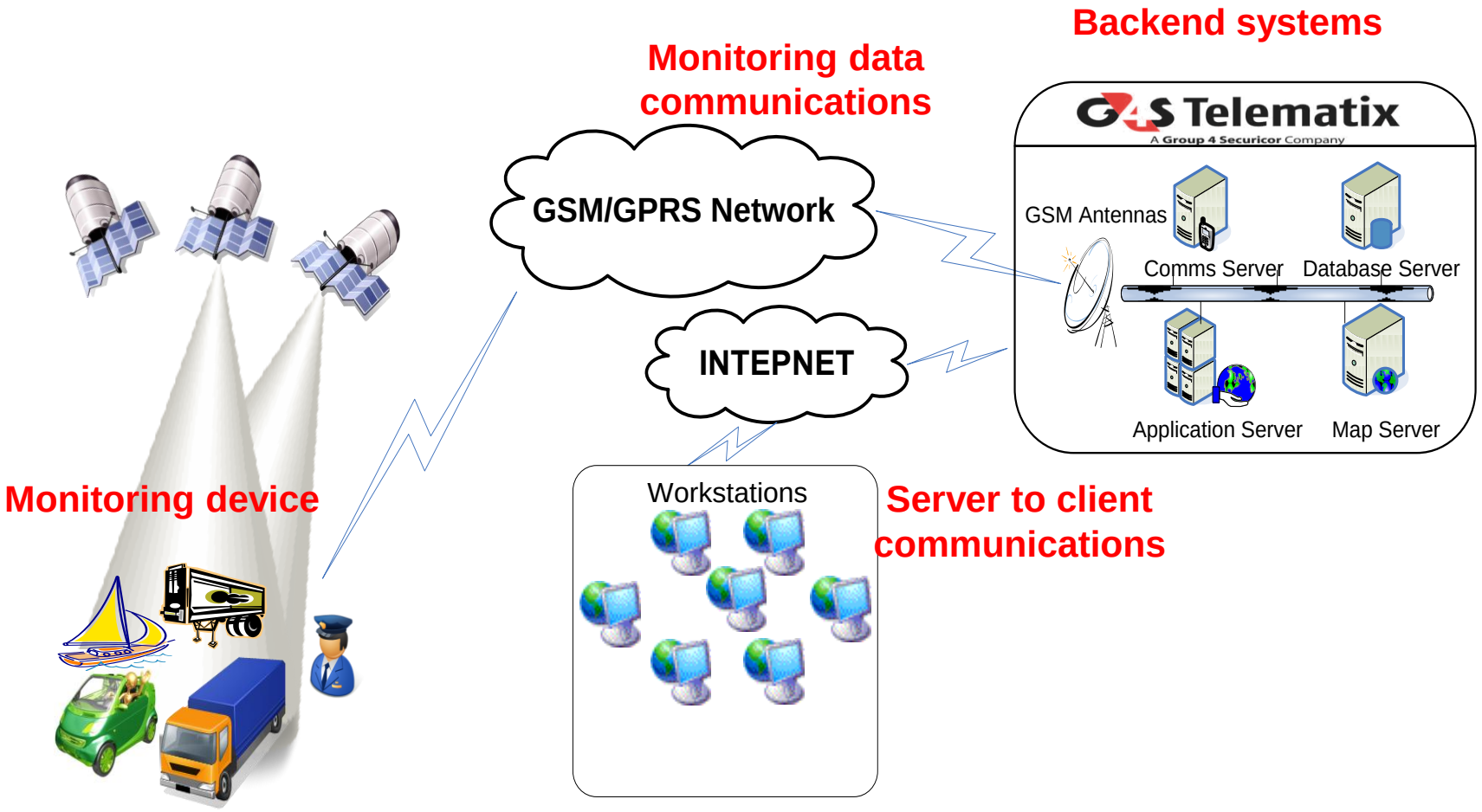
Solution Architectural Diagram



Possible Threats

- Availability
  - Monitoring devices
  - Back end systems
  - Data communications
- Confidentiality
  - Unauthorized access
  - Data leakage
- Integrity
  - Data modification

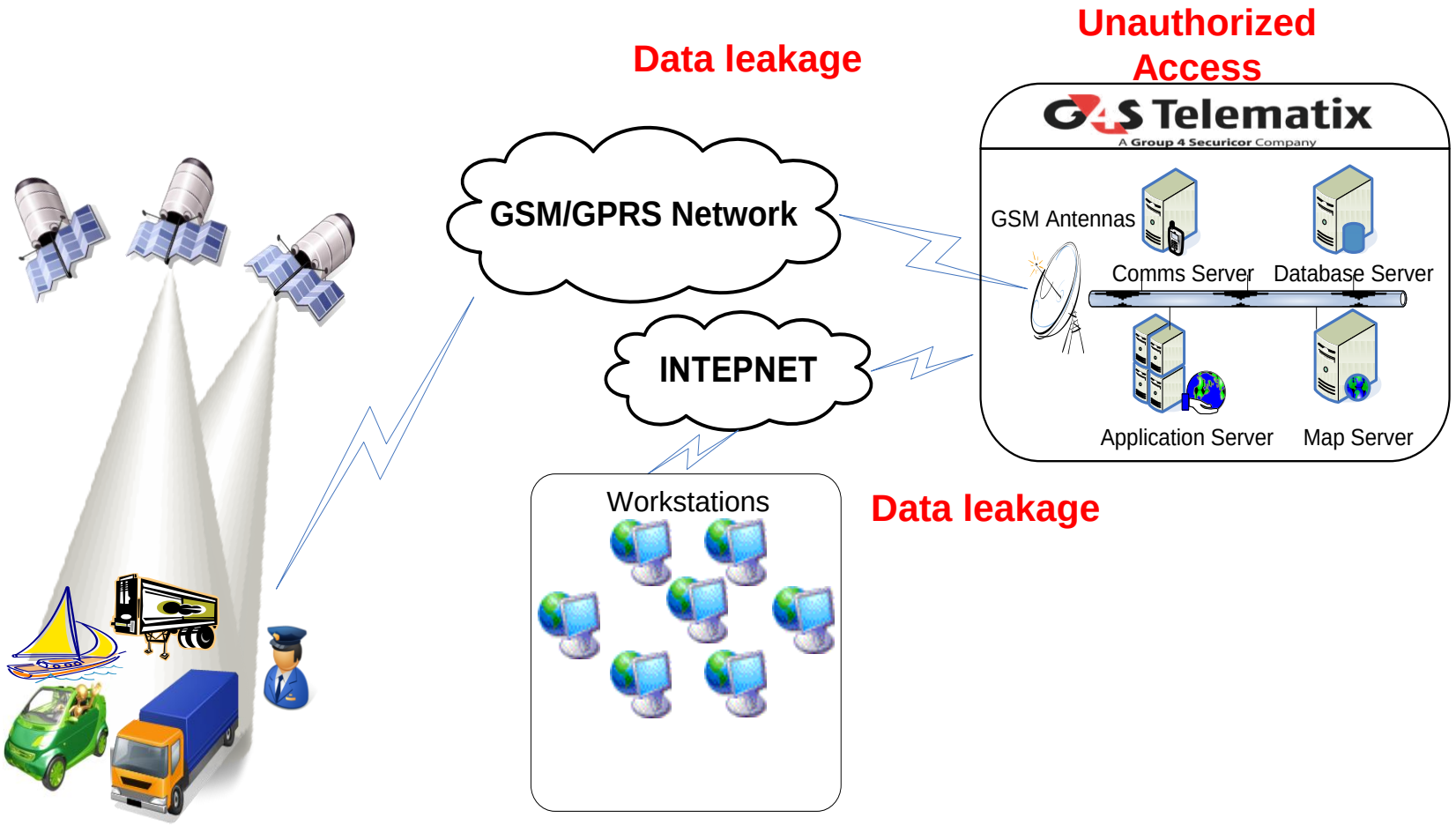
Availability Threats



Risks on availability

Threat	Probability	Mitigation options
Monitoring device failure	Low	✓ Two distinct devices
Monitoring data communications failure or temporary loss	Medium	✓ Two devices using distinct providers ✓ One device with alternate connections ✓ Plain GSM (SMS/CSD) option in cases that GPRS is not available ✓ Devices log generated messages and send them later
Server to client communications failure or temporary loss	Low	✓ Redundant network connections
Backend systems availability	Low	✓ Redundant / high availability servers ✓ Tier-III Datacenter

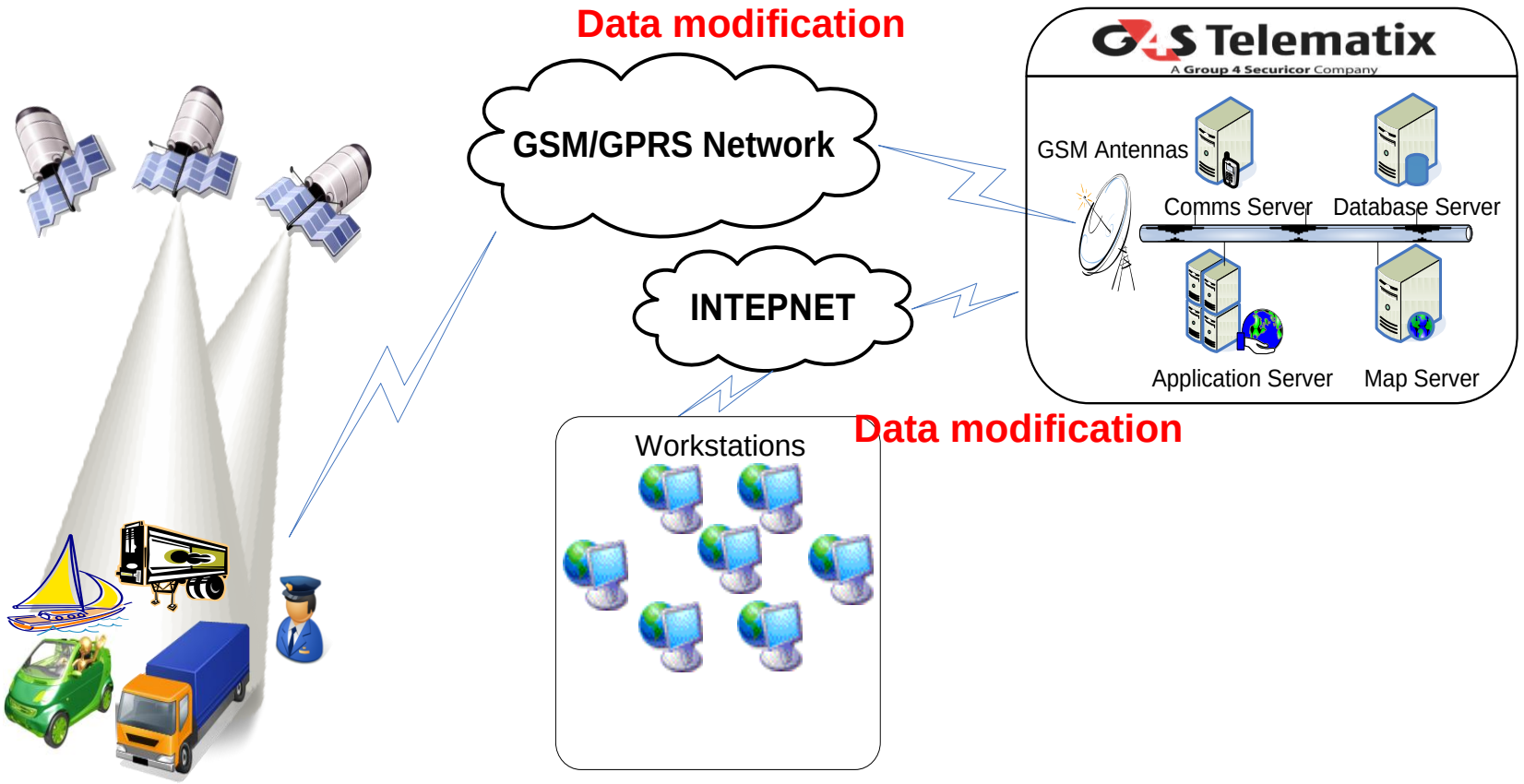
Confidentiality Threats



Risks on confidentiality

Threat	Probability	Mitigation options
Leakage of messages sent over GPRS	Low	✓ Standard GPRS security – encryption and authentication ✓ Proprietary and encrypted communication protocol ✓ Own APN / GGSN ✓ End to end VPN
Data / reports sent to the end users	Medium	✓ SSL – based communication (HTTPS) ✓ Client (certificate based) authentication
Unauthorized access	Medium	✓ Firewall ✓ Network and Host Intrusion Detection Systems ✓ Physical security

Integrity Threats



Risks on integrity

Threat	Probability	Mitigation options
Alteration of messages sent over GPRS	Low	✓ Standard GPRS security – encryption and authentication ✓ Proprietary and encrypted communication protocol ✓ Own APN / GGSN ✓ End to end VPN ✓ Application – level integrity check ✓ Application – level logic
Alteration of the data / reports sent to the end users	Medium	✓ SSL – based communication (HTTPS) ✓ Client (certificate based) authentication

Identification methods

Problem	Identification
Faulty or compromised devices	✓ Continuous checks for devices that do not send messages for a time period over a standard threshold
Data is not received from a communication channel	✓ Continuous checks for the amount of data sent over communication channels
Server to client communications failure	✓ Automatic failover to redundant connection and alarm generation
Backend systems failure	✓ Automatic failover to redundant system and alarm generation
Backend systems intrusion attempt	✓ Network and Host Intrusion detection systems

Contact details

G4S Telematix:

http://www.telematix.gr

Michalis Kamprianis

Technology Manager, G4S Telematix

michalis.kamprianis@gr.g4s.com

Thank you for your attention