Introduction to Network Awareness

Mestrado Integrado em
Engenharia de Computadores e Telemática
DETI-UA

deti.ua.pt

Awareness

- **Direct** Awareness
  - By direct observation.
- **Indirect** Awareness
  - By analysis of reactions to events.
- Awareness **by Correlation**
  - Joint analysis of multiple sources of data to detect hidden patterns and relations.
  - Big Data Problem.
- Awareness **by Prediction**
  - Detection of patterns over time.
  - Black Swan Problem!
- Its all an **Inference**, **Validation**, **Correction** loop.

Network Awareness (1)

- Ability to effectively **Acquire Data** by **Monitoring** networks and systems to:
  - Optimize services,
  - Detect and counter-act anomalous activity/events.
- **Analyze/Process** data to know and characterize
  - Network entities,
    - An entity should be understood as a person, a group, a terminal, a server, an application, etc...
  - Data flows,
  - Services and users perception of service.

Network Awareness (2)

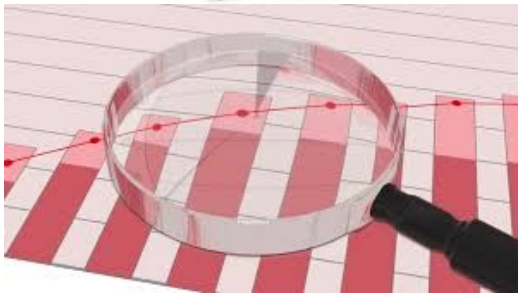
- All data sources are acceptable.
  - Never assume data irrelevance!
- Data may be:
  - Quantitative.
    - Allows for statistical analysis and may serve as machine learning training input.
    - e.g., number of packets, number of flows, number of contacted machines, etc...
  - Qualitative.
    - Can be transformed to quantitative data by counting techniques and statistical characterization
    - e.g., error message X, address Y contacted, packet of type Z, etc...

Network Awareness (3)

- Time is relevant.
  - Relative and absolute.
  - An event occurs in a specific time instant, and it is part of a sequence of events.
- Timescale(s) of analysis must:
  - Include the target characteristics,
  - Allow the perception of the event in time for a response.
- Data may be re-scaled for multiple analysis purposes.

Network Awareness Steps

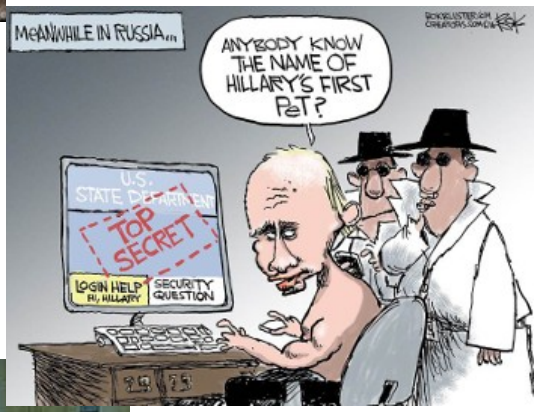
- Data acquisition.
- Data processing.
  - Creation of time sequences with different counting intervals (minimum timescales).
  - Creation of time sequences with different statistical metrics (larger timescales).
- Creation of entities' behavior profiles.
  - Usually time dependent.
- Classification of entities' behaviors.
  - Identification/classification.
  - Anomaly detection.



Network Atack Vectors

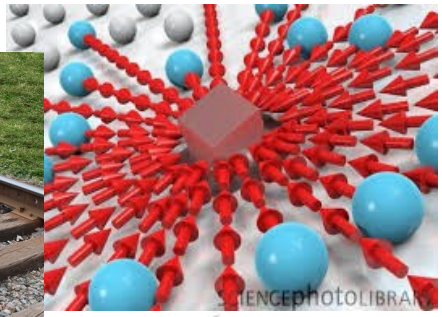
Type of Attacks (1)

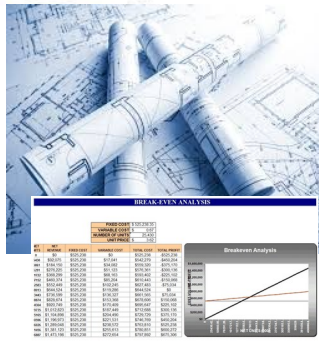
- Objectives:
  - Fun and/or hacking reputation
  - Political purposes
  - Military purposes
  - Economical purposes
  - Other?
- Technical objectives:
  - Operation disruption
  - For data interception
  - Both
    - Disruption to intercept!
    - Intercept to disrupt!



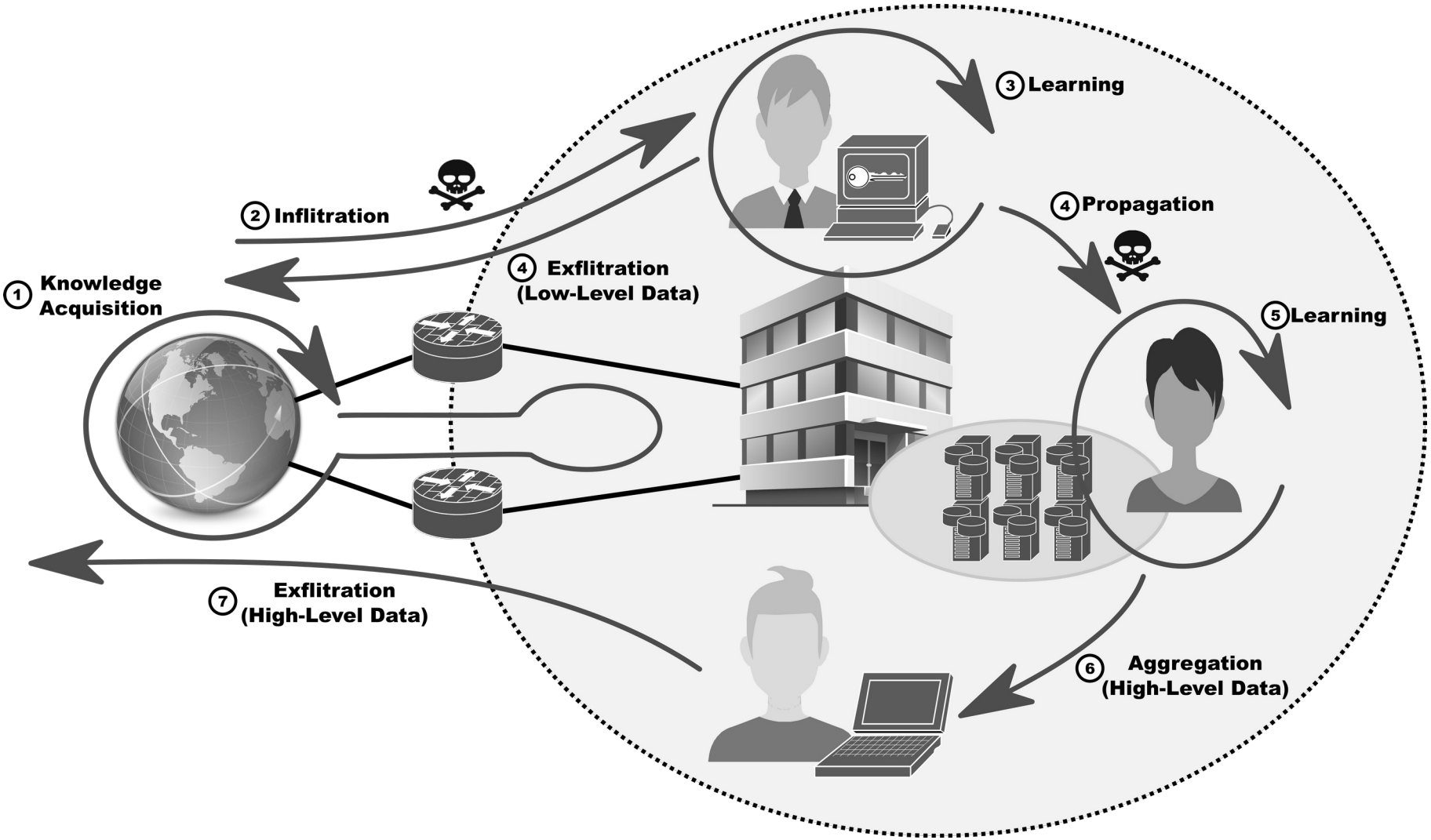
Type of Attacks (2)

- Technical objectives:
  - Operation disruption.
    - (Distributed) Denial-of-Service.
  - Resources hijack.
    - Spam,
    - Crypt-currency mining/masternodes,
    - Platform to other attacks!
  - Data interception/stealing.
    - Personal data
      - As final goal,
      - Or as tool to achieve more value information!
    - Technical data,
      - Usually used to achieve more value information!
    - Commercial data
      - Digital objects, financial and/or engineering plans, ...
- Disruption may be used to achieve intercetpion!
- Interception may me used to achieve disruption (operational or commercial)!





Attack Phases

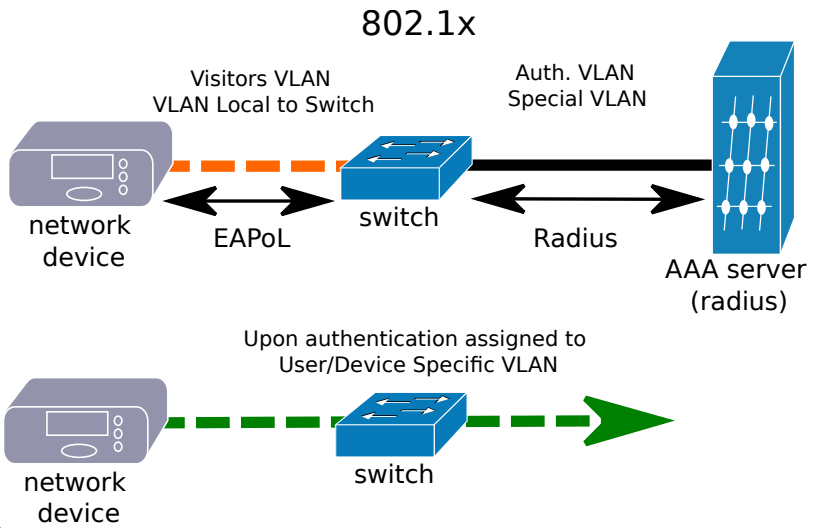


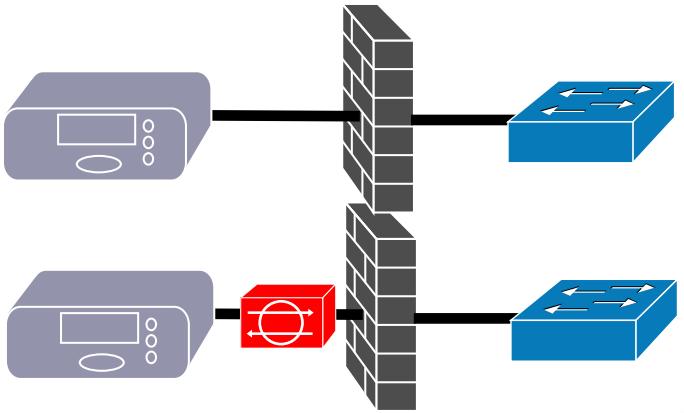
by Physical Interaction

- Ethernet ports at public/unprotected locations
  - With VLAN separation
  - Without VLAN separation
  - Protected by 802.1X
- Network taps at public/unprotected locations
- Network devices access
  - Unprotected serial/console ports, USB ports, etc...
- USB ports (short time access)
  - Long time objectives
    - Trojan/root kits injection.
  - Short time objectives
    - Device data acquisition (contacts, messages, sms, etc...)
- Sitting down at a terminal or with a device!
- Other?

Illicit usage of Ethernet ports

- Common protection:
  - VLAN separation/isolation.
  - 802.1X.
- Unused ports
  - VLAN separation/isolation and/or 802.1x may be enough to mitigate more dangerous attacks (L2 or L3 access to internal machines).
  - Switches MAC flooding attacks and Network overload (Local DoS) are possible.
- In use ports
  - Using an inline device it is possible to break 802.1X using terminal/user authentication.
    - Traffic pass-through.
    - After 802.1X authentication performs inline MAC spoofing.
  - Allows for traffic snooping, injection, and MITM attacks.





Network Tapping

- Switch rogue mirror ports.
  - Allows for traffic snooping and injection, no MITM attacks.
  - Solution: Constant monitoring of configuration changes on network devices.

- Ethernet cable tap
  - Allows for traffic snooping and injection, no MITM attacks.
  - Solution: Electrical variations. Maybe…?

- Optical cable tap
  - Allows for traffic snooping and injection, no MITM attacks.
  - Solution: Quantum cryptography

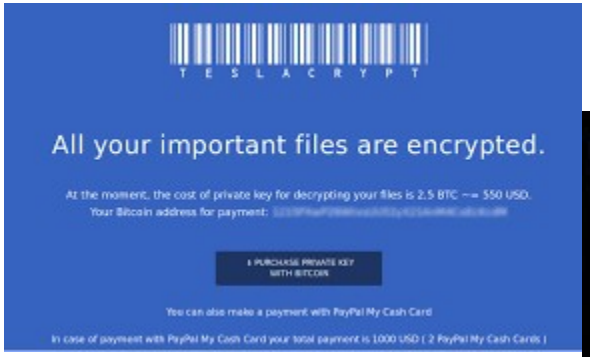
universidade de aveiro

Wireless

- Rogue APs
  - WPA PSK and WPA2 PSK are not compromised.
    - Unless device associates to networks with (fake) SSID of known networks with different credentials and/or secure protocols.
      - Decision to connect based only on stored SSID and not other parameters.
  - WPA Enterprise and WPA2 Enterprise security may be compromised on 2nd phase authentication.
    - Credentials not recoverable (maybe with MSCHAPv2).
    - Permits “accept everyone” strategy for MITM attacks.
  - Open+Web-based authentication are very vulnerable.
    - Fake entry portals.
  - Allows DoS.
    - Force user to search other networks. Make user choose insecure/fake network.
- Wireless Interception (possible injection).
- Electromagnetic effects
  - Wireless mouses, keyboards, …
    - Solution: additional information to scramble data.
- By Sound
  - Keystrokes sounds.
- Jamming
  - Pure disruption, or
  - Disruption to activate secondary channels (more easily compromised).

Remote Software Installation or Service Activation

- Attacks to routing (MP-BGP)
- E-mail
  - Office macros
  - Executables
- Social Networking
- Software downloadable
  - Sources:
    - Cracks
    - Non-certified software stores
    - …
- Attacks:
  - Ramsomware
  - Trojan Horse



Distributed DoS

- Multiple slow/small devices generating traffic to a target
  - TCP vs. UDP
- Purpose of disruption
  - By political/economical/"reputation"
  - Redirection to other service/location?
- Solution at target
  - Load-balancers
  - For TCP, maybe its possible to survive making active (with licit client validation) session resets (server/firewalls)
    - White list solution, for completed session negotiation
  - For UDP/DNS, block requests for known external relay/redirection DNS servers (blocks attack amplification, IP target spoofing)
    - Doesn't work with large botnets and direct requests to target
- Solution at source
  - Anomalous behaviors detection
    - Low traffic variations hard to detect
    - Time and periodicity changes are easier to detect
    - Destinations of traffic changes
    - With "really low" data rates is impossible to detect

Data Acquisition

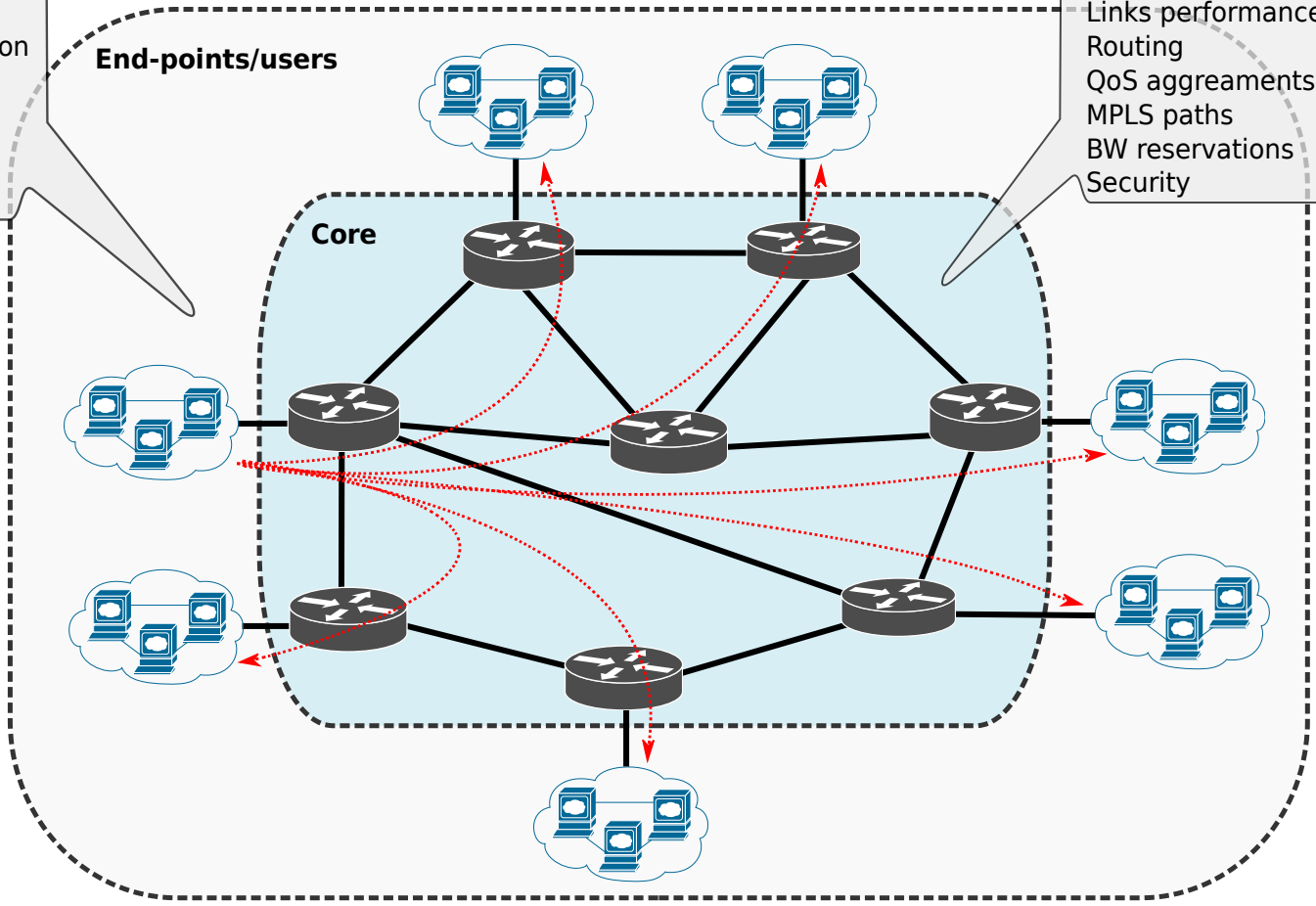
Core and End-to-End Monitoring

End-to-end measurements
- delay
- jitter
- throughput
- losses
- BW reservations
- reserved paths validation

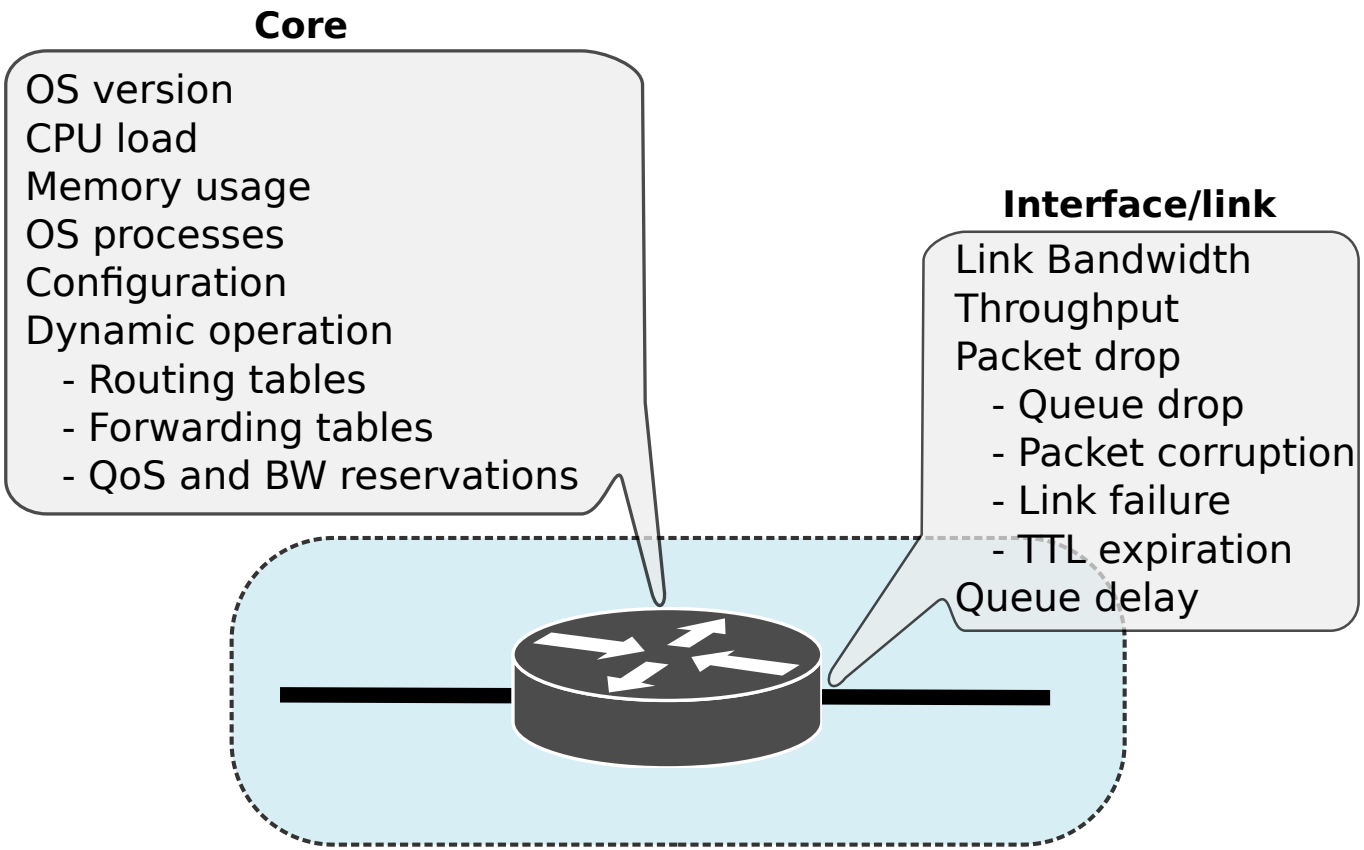
Demands per destination
- global
- per service/app
- per QoS usage

Core configurations
- Node awareness
- Service awareness

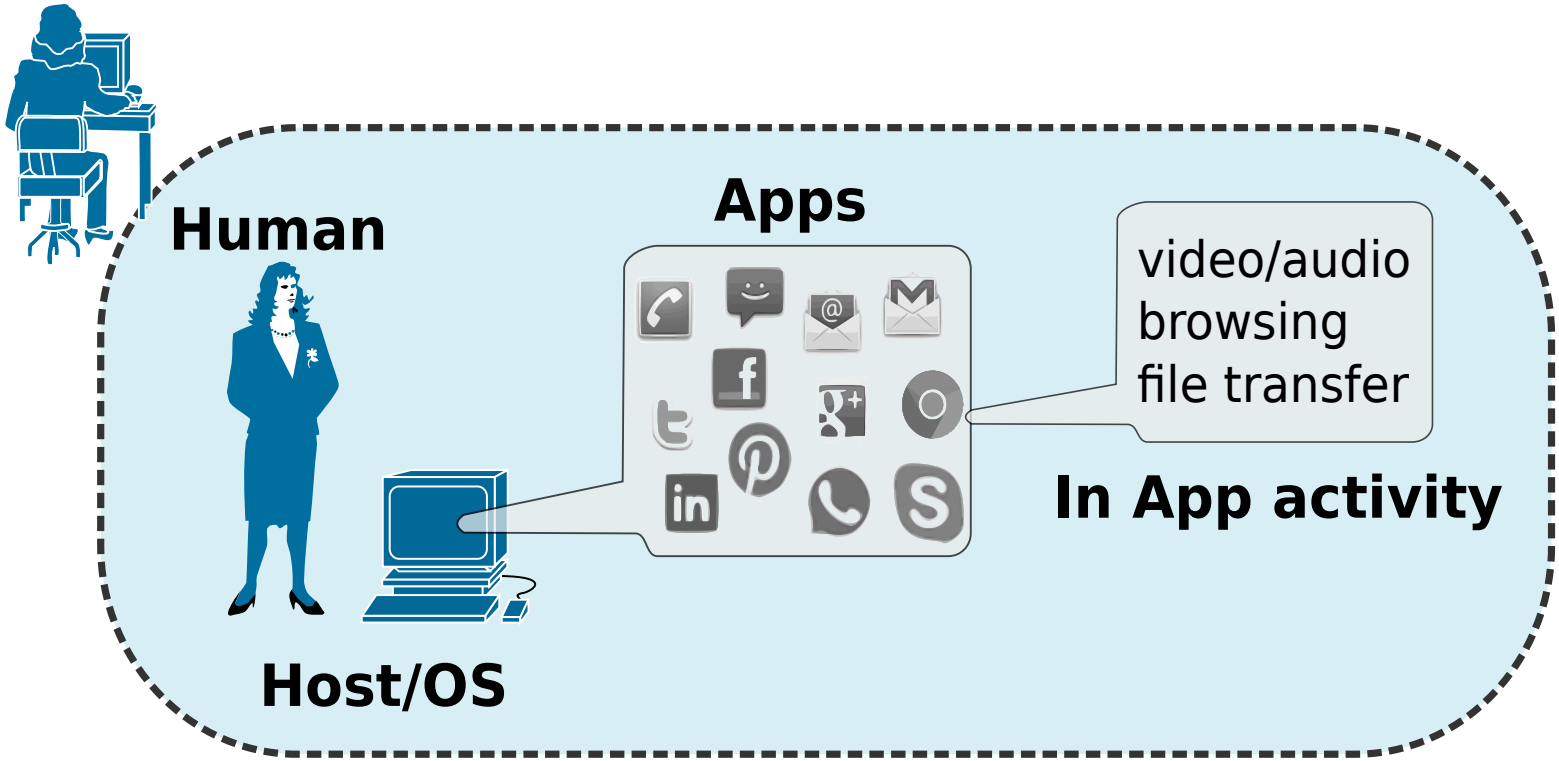
Nodes performance
Links performance
Routing
QoS aggreements
MPLS paths
BW reservations
Security



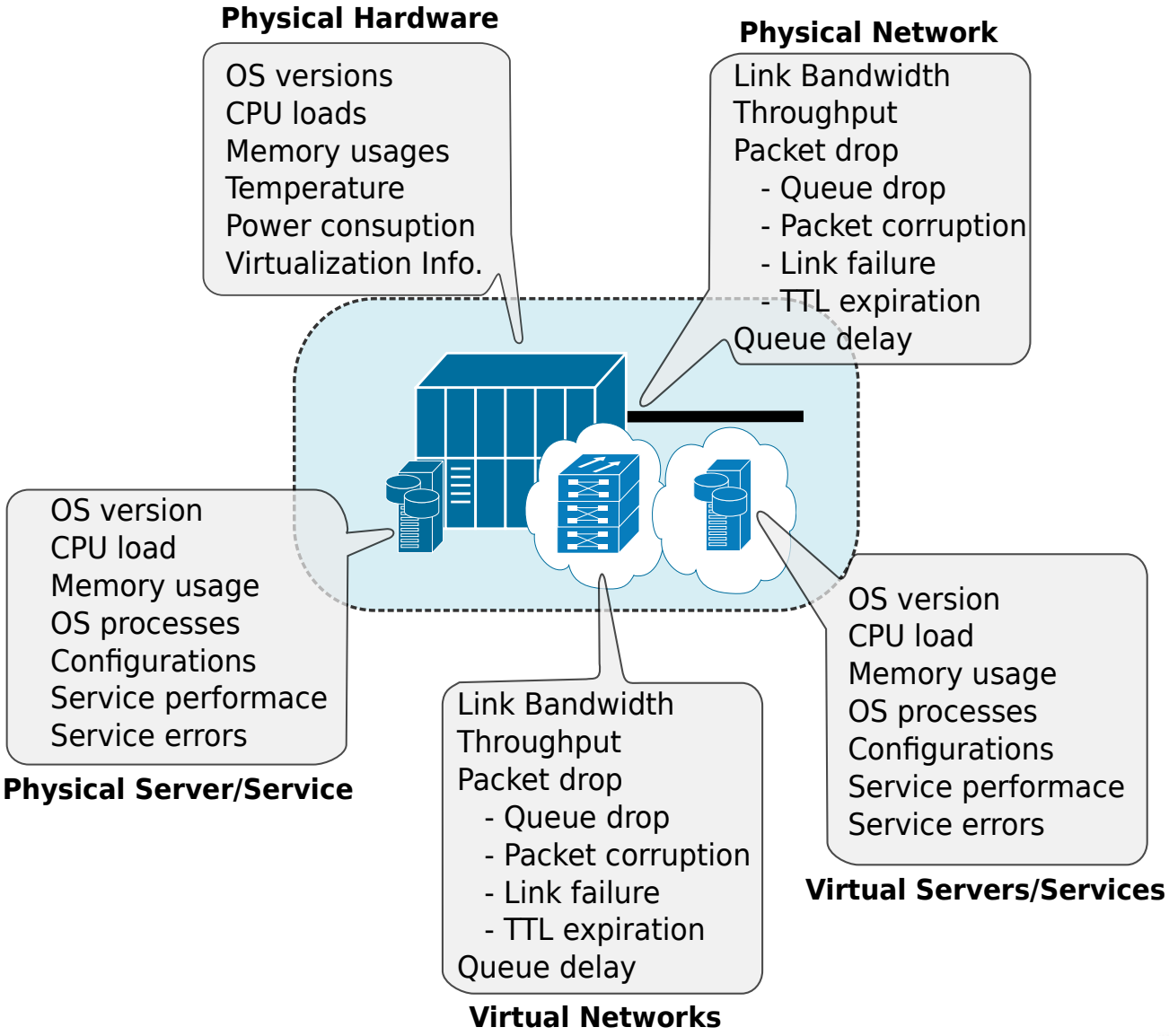
Node Monitoring



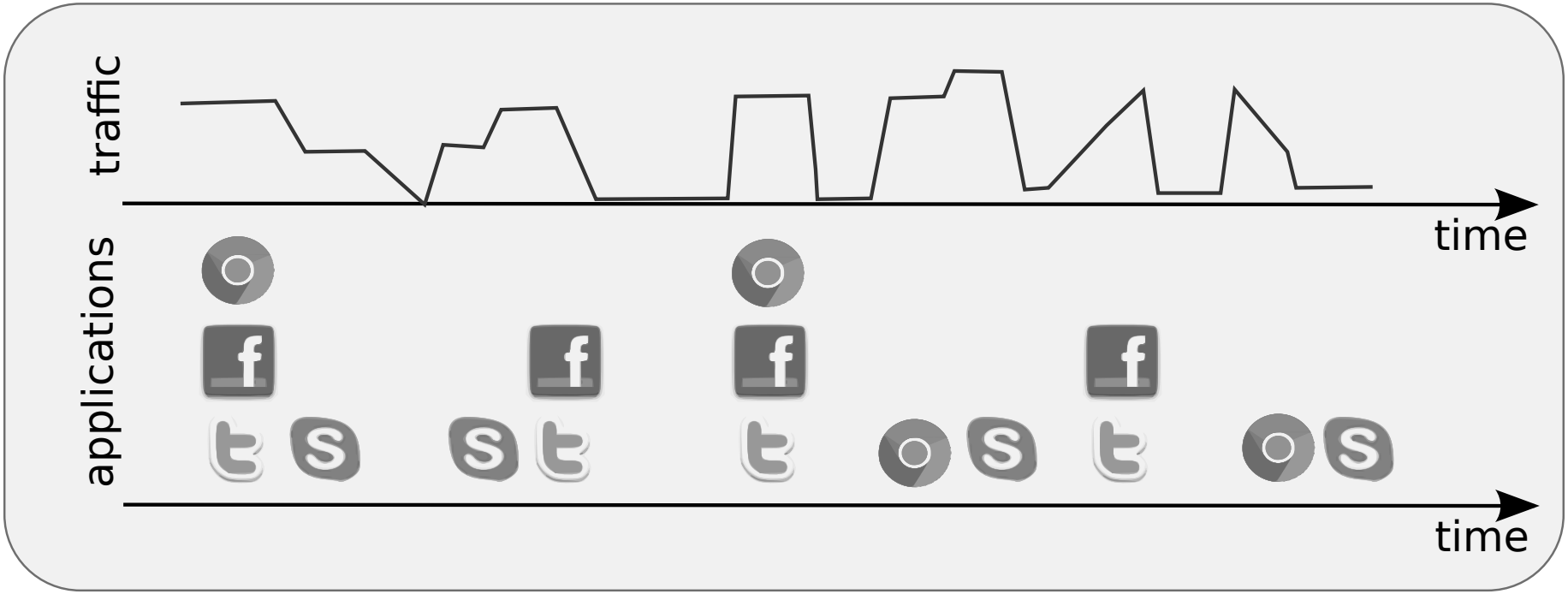
End-User/Host/App Monitoring



Server/Service/Cloud Monitoring



Overtime Monitoring



Data Sources

- SNMP
  - Used to acquire knowledge about current states of nodes/links/servers.
  - Local information. May be used to extrapolate to global information.
  - (Often) Requires the usage of vendor specific MIBs.
- Flow exporting
  - Used to characterize users/services in terms of amount of traffic and traffic destinations.
  - Medium and large time-scale information.
  - Protocols: Cisco NetFlow, IPFIX – Standard, Juniper jFlow, and sFlow
- Packet Captures / RAW statistics / DPI vs. SPI
  - Used to characterize users/services in small time-scales.
  - Requires distributed dedicated probes.
- Access Server/Device logs and/or CLI access.
  - Used to acquire knowledge about past and current state.
- Active measurements
  - Introduces entropy on network and requires (for many measurements) precise clock synchronization
  - E.g., one-way delay/jitter, round-trip delay/jitter.