Annual review ROME 2012

WP2 – SPD Preliminary Metrics

Lessons learned

Motivation

- pSHIELD contained a non formal and non linked SPD metrics gathering and design process
- nSHIELD requires a quantitative solutions linked to the architecture and 4 scenarios
- Connection to SPD requirements is a must. Formalisation also ends with a CC SFR convergence

Achievements

- Approx. 60 types of SPD metrics have been identified across 4 nSHIELD layers: Node, Network, Middleware and Overlay
- Formalisation has been developed though requirements-metrics mapping and convergence to other documents such as, the architecture and scenarios

Quantitative solution

- The following table specifies the format and structure of nSHIELD SPD Metric, emphasizing on the quantitative solution

Metric	//Name together with an optional code name
Description	//Provide a short description about the metric
System component(s)	//It should define the system component(s) where the metric is applicable, i.e.[node | network | middleware | overlay | all], where all also denotes a single nSHIELD node. The field also has the meaning of the data source.
Formula	//Type of value and how it is calculated
Target	//It defines the target value if available
Frequency	//How often should measurements be collected or value checked
Applicability	//It should define whether it is a global metric or bound to a specific scenario
Requirements	//It lists the requirements that this metric satisfies
CC Functional requirements/Classes	//It does the mapping between this metric and the applicable CC functional requirements to facilitate assessment against protection profiles' requirements.

Example of nSHIELD SPD Metric

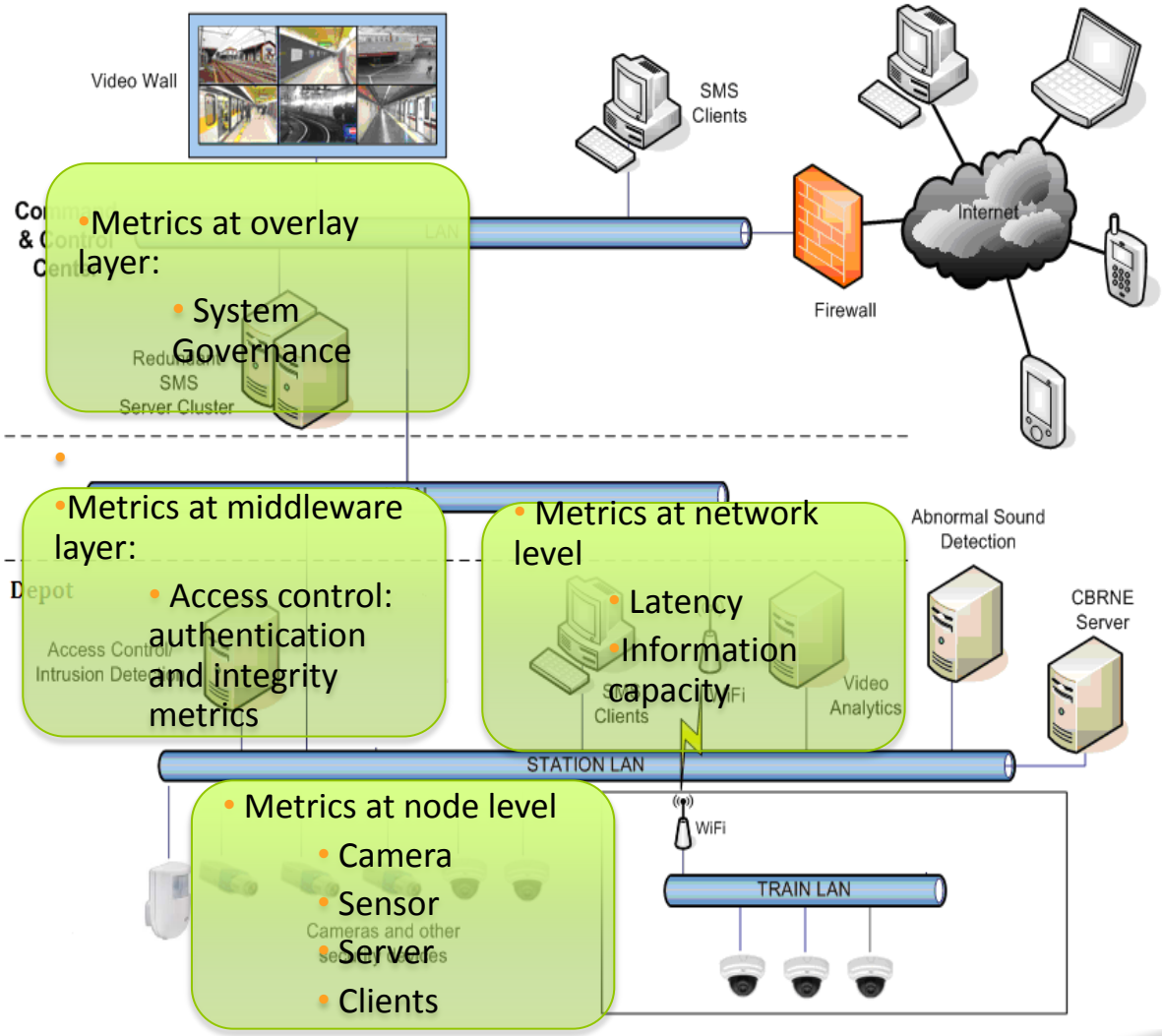
Table 43: Metric – Network Information Capacity

Metric	Information Capacity
Description	This is a performance metric used for measuring the network's capacity, which shall be large enough to allow the necessary traffic to go through. As a rule of thumb, at normal operation, the traffic should be about 60-70% of the network's capacity, so as to avoid bottlenecks when there will be traffic peaks. Measuring capacity is quite a complex task [14]. However, the approach of "IP-type-P Path Capacity" seems to be rather straightforward to implement in the nSHIELD network.
System component(s)	Network
Formula	C(P,T,I) = min {1..n} {C(Ln,T,I)}, P: Packet type, T: Time, I: Interval, Ln: Link AP: RFC 5136,
Target	
Frequency	Scenario specific (It depends on whether the network topology is dynamic or not).
Applicability	Global
Requirements	REQ_D2.1.1_21103.A Information Capacity REQ_D2.2_SH1 (Enabler) REQ_D2.2_NW21
CC Functional requirements /Classes	FMT. Security management

Sistematisation

- A 7 steps methodology has been defined for SPD Metrics Design process
- This will help to formalise metrics design and moreover to deploy them correctly in the following use cases
  - Railroad Security scenario
  - Voice/Facial Verification scenario
  - Dependable Avionics System Scenario
  - Social Mobility and Networking Scenario

Application example: Railway Scenario



- In order to manage
  - Security level (physical and logic)
  - HW and SW faults
- Composition of different metrics in order to assure an high SPD level.

Future work

- SPD Metrics composition are still under consideration. (A first explanation of possible alternatives has been made.)
  - Deliverable 2.8 should select one of them
- Link to scenarios should be implemented and validated in deliverable 2.8
- New iterations and metrics refinement with respect to architecture and requirements documents should be reviewed as validation progress goes on

SPD Preliminary Metrics

More info on wiki:
http://nshield.unik.no/wiki/D2.5