Stockholm 2013

nSHIELD

SPD Metric
SELEX ES Proposal

ARTEMIS

SPD METRICS

TARGET: Quantify the **ATTACK SURFACE** of the nSHIELD system.

ATTACK SURFACE: The lack of separation between assets and threats

attack
attack
attack
attack

The ATTACK SURFACE shows how much the system can be attacked and it is static against the environment

SPD METRICS

Each system (nSHIELD too) has interactive points, we refer them as **POROSITY**

The interactions of **POROSITY** are classified as:

- Complexity: # of critical system component;
- Access: # of direct entry and exit points;
- Trust: # of indirect entry and exit points.

Access “pores” must be balanced with “**der**” **damage potential – effort ratio**

SPD METRICS

To minimize the Attack surface we introduce **CONTROLS** divided in two categories:

- **Interactive**
- **Process**

CONTROLS:

Authentication
Idemnification

Resilience
Subjugation
Availability

Non-repudiation
Confidentiality

Privacy
Integrity
Alarm

SPD METRICS

Controls minimize the attack surface, but they can themselves add it if they have **LIMITATIONS**

LIMITATIONS affect how well our controls can work

They are classified in five types:

- **Vulnerability**
- **Weakness**
- **Concern**
- **Exposure**
- **Anomaly**

Furthermore the weight of a particular limitation is based of the concept of **attack potential** described in the **Common Criteria** standard and used in pSHIELD SPD metrics.

SPD METRICS

Now Measure our attack surface

- Count the porosity of the system.
    - all that which is visible and interactive weighted with der ratio and all which allows for free interaction between other trusted systems. Critical components.
- Account for the controls in place
    - Determine where any of the 10 controls are in place
- Account for the limitations found in the controls
    - Weighted with attack potential calculated as described in Common Criteria standard

The attack surface is :controls minus porosity minus limitations

SPD METRICS

References:

- OSSTMM 3 the Open Source Security Testing Methodology Manual – ISECOM
- An Attack Surface Metric – Pratyusa K. Manadhata Jeannette M.Wing
- Common Methodology for Information Technology Security Evaluation – CCMB-2009-07-004