

2nd Annual review

Florence 15 November 2013



Attack surface metrics approach

Responsible of the activity: Andrea Morgagni – Selex-ES
Presenter: Andrea Fiaschetti – Univ. “La Sapienza”



References

BASELINE

OSSTMM 3 The Open
Source security
Methodology
Manual –
Contemporary
security Testing and
Analysis – created by

Pete Herzog –
Developed by
ISECOM – 2010

An Attack Surface
Metric - Pratyusa K.
Manadhata,
Member, IEEE, and
Jeannette M. Wing, -
IEEE Transactions on
Software
Engineering, 2010

Common Criteria –
Common
Methodology for
Information
Technology Security
Evaluation –
Evaluation
methodology,
September 2012,
Version 3.1, Revision
4

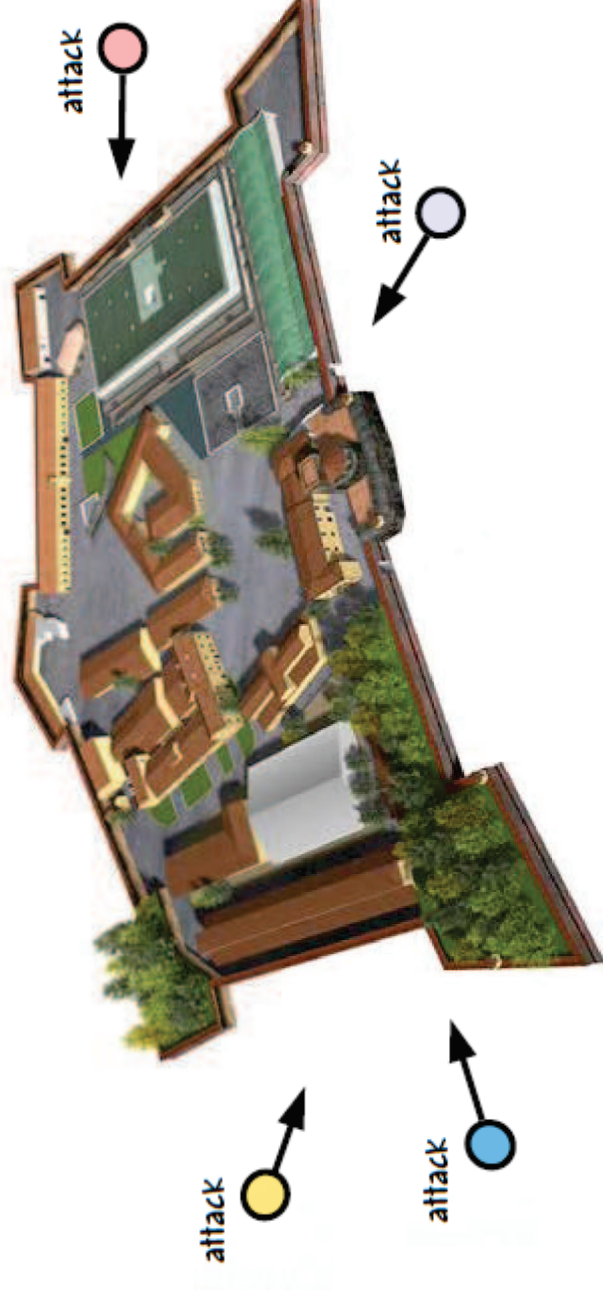
**DAMAGE POTENTIAL-
EFFORT RATIO**

**WEAKNESS
WEIGHTED**

Purpose and base concepts (1/2)

TARGET: Quantify how a nSHIELD system is resistant to **ATTACK** to its **SURFACE** (Actual SPD level).

SYSTEM'S ATTACK SURFACE is the set of ways in which an attacker can enter the system and potentially cause damage.



Purpose and base concepts (2/2)

- **Threat** is the origin of the fault chain (fault -> errors -> failures) for the dependability concerns and as the potential for abuse of protected assets by the system for security concerns.
- The **Attacker** is the threat agent, it is a malicious human activity or non malicious event
- An attacker uses **nSHIELD's entry and exit** points to attack the system.
- It is introduced an **entry and exit point framework** (formally modeled through I/O automata)
- A threat, to be effective, must interact either directly or indirectly with the asset. To separate the threat from the asset we need to avoid a possible interaction. Therefore it is possible to have **total (100) SPD level** if the threat and the asset are completely separated from each other. Otherwise SPD level indicates **a measure for assurance protection of the asset** which is provided by the controls you put on the asset or the **degree to which you lessen the impact of the threat.**

Actual SPD level definition (1/3)

Each system has interactive points, we refer them as **POROSITY** which is further categorized as one of 3 elements:

- **Complexity:** number of components critical for the dependability of the nSHIELD system;
- **Access:** number of different places where the interaction can occur (direct entry and exit points);
- **Trust:** each relationship that exists where the system accepts interaction freely from its component or another system within the scope (indirect entry and exit points)

Access “pores” leads to define the concept of **damage potential – effort ratio (der)**, which is a consistent measure of the lack of separation that each access pore introduces.

Actual SPD level definition (2/3)

To minimize the Attack surface we introduce **CONTROLS** divided in 2 classes and 10 categories:

Class	Category
Interactive controls	Authentication
	Idemnification
	Resilience
	Subjugation
	Availability
Process controls	Non-repudiation
	Confidentiality
	Privacy
	Integrity
	Alarm

Actual SPD level definition (3/3)

Controls minimize the attack surface, but they can themselves increase it if they have **LIMITATIONS** (particular events that affect how well our controls can work)

LIMITATIONS are classified in five types:

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

In Actual SDP level definition it was considered the introduction of a weight of a particular limitation (Vulnerability) which is based on the concept of **attack potential** described in the **Common Criteria** standard and used in pSHIELD SPD metrics.

Actual SPD level calculation (1/2)

In this approach was used an operational metric and so must be considered the usual problems that this choice can lead.

The SPD level is a scale measurement of the attack surface, the amount of uncontrolled interactions with a target, which is calculated by the quantitative balance between operations, limitations, and controls.

Its calculation can be divided in two phases.

Actual SPD level calculation (2/2)

1. Data collection (see Data Collection Form) - for each component, subsystem and finally for the whole nSHIELD system must be considered:

- Porosity data (complexity, access and trust attributes);
- Controls in place;
- Limitations found in the control (weighted with attack potential calculated as described in Common Criteria standard)

2. Insertion of data collected in the calculation engine (see Actual SPD Level calculation engine) – The output of this phase is the Actual SPD Level calculated through the following formula (defined in D2.8)

$$ActSPDL = 100 + ActSPDL\Delta - 1/100 \times (OpSec_{base} \times FC_{base} - OpSec_{base} \times SecLim_{base} + FC_{base} \times SecLim_{base})$$

Data Collection Form

[illegible]

- owl:Thing
 - Ontology1300273978:Control
 - Ontology1300273978:Class_A
 - Ontology1300273978:_Authentication
 - Ontology1300273978:_Continuity
 - Ontology1300273978:_Identification
 - Ontology1300273978:_Resilience
 - Ontology1300273978:_Subjugation
 - Ontology1300273978:Class_B
 - Ontology1300273978:_Alarm
 - Ontology1300273978:_Confidentiality
 - Ontology1300273978:_Integrity
 - Ontology1300273978:_Non-Repudiation
 - Ontology1300273978:_Privacy
 - Ontology1300273978:Limitations
 - Ontology1300273978:Anomalies
 - Ontology1300273978:Concerns
 - Ontology1300273978:Exposures
 - Ontology1300273978:Vulnerabilities
 - Ontology1300273978:Weaknesses
 - Ontology1300273978:SPDFunctionality
 - Ontology1300273978:AtomicSPDFunctionality
 - Ontology1300273978:_Access
 - Ontology1300273978:_Complexity
 - Ontology1300273978:_Trust
 - Ontology1300273978:_System
 - Ontology1300273978:Access
 - Ontology1300273978:Complexity
 - Ontology1300273978:Trust
- owl:Datatype
 - owl:AIDISointClasses



Conclusions

- Simple approach based on standard
- Technology Independent
- System scale Independent
- Fully deterministic
- Machine readable and machine executable (ready for automatic execution)
- The initial effort needed to identify parameters is balanced by the flexibility in future deployment
- An I/O automaton, $A = \langle sig(A); states(A); start(A); steps(A) \rangle$ is used to model the attack surface (entry/exit points): Forma Modelling

Thank you