Stockholm

SPD Metrics

Adopting them to use cases

ARTEMIS

About metrics...

- *"...To measure is to know..."*
- But measuring security is quite expensive
- Environment:
  - Heterogeneous
  - Multi-device and multi-manufacturer
  - User is a human and a system (subsystem)

nSHIELD

Motivation for this model comes from

SPD concepts and functionalities
&
nSHIELD layered arhitecture

Metric in nSHIELD System

- nSHIELD system:

Consider a set of *S* systems that interacts with an Environment with the following properties

$E_{S, M\ (System, Metric)}$ = ‹S, P, D, L› where:

S = Security Level {1..100}

P = Privacy Level {1..100}

D = Dependability Level {1..100}

L = ‹No, Ne, M› where:

No = Node {0..1}

Ne = Network {0..1}

Mi = Middleware {0..1}

Our goal is to define our metrics and therefore NSHIELD system with these properties

nSHIELD

On the other hand

- We have different metrics selected in 2.5 and listed from other channels:
  - See excel
  - And we are working on incrementing this list with an holistic view of SPD functionalities and measurements

We FOUND OUT that

- We have two main problems with metrics:
  - 1: some of the metrics are technology dependent and difficult to measure unless there is a programatic channel to manage it (2.5)
  - 2: other formal metrics are expensive to measure due to complexity for bringing the real value to the equation
    - $f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \quad \frac{n\pi x}{L} + b_n \right)$

See equations of excel as example

nSHIELD

Metric in nSHIELD system

- nSHIELD system:

We have defined for each of the metrics listed in the excel file a set of indicators that should be parameterized by each of the use

Num	SPD indicator	Layer	Name	Description	Formula/implementation	Indicators to be defined by business owners	Categrory
5	(x,y,z)	Overlay--> Networkd	Attack Escalation Speed	Measures the speed (how fast) the attack is consolidated	AES = impacted_nodes/DifT	DifT = time elapsed between the beginning of the attack and the reaching of the worst critical state	Availability

So that

- We are measuring nSHIELD system in terms of: security, privacy and dependability and if the measurements affects to one layer or different layers. The measurement will be supported by:
  - Trasnforming value to NSHIELD properties
  - Aggregation techniques

Transforming value

- Transformation value from metric to nSHIELD Metric = [SPD,L]
- We need to define metrics value unit and range.
- Once doing that we transform that value to % or to range [1..100]
- We divide 300 point (S=100, P=100, D=100) according to individual indicator and Contextual Factor (CF):
  - $R_{LAYER}(x,y,z)$ = Divide Measured_Metric(value, CF)
- We have now a metric in terms of nSHIELD format

Aggregation

- Once we have all results for each of the metrics we can aggregate metrics according to:

FORMULA: ‹ Σ (σS(No, Ne, M),σP(No, Ne, M),σD(No, Ne, M))›

‹ Σ (MEAN S(No, Ne, M),MEAN P(No, Ne, M),MEAN D(No, Ne, M))›

  - Σ explains de aggregation concept of {SPDL} in overall terms
  - Where **σ** SPD is the standard deviation which analyses the spread of measures in (SPD) and compares to indicators (overall indicator)

nSHIELD

Method

- The way forward:
  - Use case owners selects metrics (excel) that thinks are more significant for their use case
  - This is hard to do due to problems identified at the beginning
  - Define indicators for each metric and aggregated indicator
  - This is the subjective area of the multi-metric approach: we need to define indicators as consign for establishing the correct value
  - Transformation equation from metric value to nSHIELD metric properties
  - We compare aggregated metrics values results with overall indicator and the standard deviation value (which consist on an overall indicator)

nSHIELD

Example: Railway Scenario

- Owner should select metrics. In this example we select:
  - Vulnerability Density - VD(related to holistic assurance and evaluation problem)
  - Network Lantency - NL (related to Repetition threat)
- We need to set the range (domain values) for this in the scenario.
  - VD = [1..(N-25%N)]; [1..TotalNodes] N: NºVuln
  - NL = [0..0,5] unit: seconds
- M (measure) is the value obtained by measuring. We have two measures for each of the 2 metrics. We assume that use case owners are able to gather this information from the system.
- M will be in between of the min and max value of the range defined before. We will transform that position to % percentage range [1..100].

nSHIELD

Example: Railway II

- Imagine that we have in one measurement:
  - VD: 50
  - NL: 80
- We transform these units to nSHIELD unit:
  - VD: 68 (50% of SUM(indicators_VD))
  - NL: 88 (80% of SUM(indicators_NL))
- As in this case CF is normal we assign it (as use case owners):
  - $M_{VD\text{-}Network} = \{0, 0, 68\} << \{30, 15, 90\}$
  - $M_{NL\text{-}Network} = \{8, 0, 80\} << \{10, 10, 90\}$
- We calculate the difference:
  - $M_{VD\text{-}Network\text{-}DIF} = \{30, 15, 22\}$
  - $M_{NL\text{-}Network\text{-}DIF} = \{2, 10, 10\}$

nSHIELD

Example: Railway IV

- Finally we will check if:
  - Standard deviation is high and then overall SPD level is weak
  - We will be able to compare means values of metric measures and indicators
  - Have an overall view in terms of nSHIELD vocabulary (SPD, Node, Network, Middleware-Overlay)
  - VALID for all METRICS measuring possible THREATS described in D7.1. Railway scenario:
  - Pshysical tamper, HW/SW faults, Network overload, Access control.....

Aproach

- Easy to ‘understand’
- Formal method to measure multimetrics (mathematical formula)
- Quite complex in the implementation: Difficulties to gather information from some of the metrics:
  - Owners will have to study carefully this.

nSHIELD

Next step

- Possibilities
  - To develop:
  - A tool for selecting good metrics and helping business and security use case owners developing the best metrics
  - This tool should be very graphical
  - Web based
  - Oriented to scenarios
  - Support for certification

nSHIELD

SPD Metrics

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