Framework Vision

Document version:	***1.2***
Authors:	***Emiliano Casalicchio, Igor Nai Favino, Marco Caselli, David Conrad, Joao Damas, ...***
Content:	***The vision of the framework on DNS Health and Security metrics and measurement***
Related project:	***Mensa***
Date:	***22/07/2011***
Comments:	**---**

Table of contents

1 EXECUTIVE SUMMARY 4

2 DIMENSIONS OF ANALYSIS 5

3 FRAMEWORK CONCEPTS 6

3.1. POINT OF VIEW DEFINITION 7

3.2. MEASUREMENT TECHNIQUES AND TOOLS 8

3.2.1. SPATIAL HORIZON 8

3.2.2. TIME HORIZON 8

4 FRAMEWORK OPERATION 10

5 REFERENCES 12

1 Executive Summary

This document is intended to:

- Give a general view of the framework for the evaluation of the Health and Security (H&S) level of the DNS;
- Describe the main baseline concepts behind the framework
- Give a general description of how the framework can be used and implemented for a specific use case.

This is a living document and it will evolve during the life of the MeNSa project according to the feedback of Advisory Board, experts and stakeholders.

The framework described in this document is intended:

- To provide a methodology for the identification and measurement of H&S metrics
- To provide baseline metrics to measure the Health of the DNS and security level as seen from different perspectives (in the following mainly referred as Point of View (PoV)) and in different threat scenario.

The purpose of the framework is also to establish how the set of metrics identified can be used in the operation of the DNS, for example:

- As a marker, to diagnose the causes of poor end user DNS experience (both in terms of security and performance);
- As a trigger, to inform a DNS user/operator of possible Quality of Service and security level degradation;
- As indicator of risk;
- As a categorisation of DNS systems for further research;
- As an indication of the general state of health of the DNS industry.

This document is organized as follow. Section 2 describes the dimensions of analysis considered by the framework. Section 3 introduce the main concepts of the framework and describes in more details the notion of PoV and measurement techniques and tool. Finally, Section 4 describes how the framework should be implemented and used.

This document is complemented by three more technical reports: [1] describes the reference architecture and models will be used to identify metrics; [4] contains the set of metrics we identified as suitable for the scope of the framework; [5] describes how the framework should be implemented in a Web user use case.

2 Dimensions of analysis

The framework is built along three main dimensions of analysis:

- The Point-of-View (PoV),
- The health indicators
- The threat scenario.

The point-of-view dimension is introduced since each DNS actor has its role in the observation, use and operation of DNS and therefore each actor influences and perceives DNS health in a different way. The main points of view we consider are:

- The End-user, who is mostly unaware of the DNS, e.g. a philosopher surfing the web to make reservations at a hotel
- The Application Service provider, who provide services using distributed applications accessible by web interfaces
- The resolver (forwarder or full resolver)
- The name servers (root, authoritative or not)
- The registrar.

The complete list and detailed description of the PoV considered can be found in [1].

Health indicators (*Coherency*, *Integrity*, *Speed*, *Availability*, *Resiliency, stability*, *security* and *vulnerability*) are introduced in [2] end [3] and must be specialized for each specific perspective. For example, in [5] it is provided a description of how an End User could perceive the H&S level of the DNS.

A part from the PoV, the H&S is also linked to the threat scenario we analyze, that is the goal of the analysis. For example if we consider the system corruption scenario it makes sense to measure the NXDOMAIN detection rate or the Cache Poisoning Probability, while in a Denial of Service scenario it makes sense to measure the Rate of repeated queries or the bandwidth consumption.

Summarizing, each time the H&S level of the DNS is evaluated, must be considered:

- A specific use case[1]; for each use case there are one or more PoVs used to observe the system. (e.g. in the Web user use case we have only the End-user PoV, while in a use case involving the Operators we could have, at the same time, Resolver PoV, Zone PoV, NS PoV)
- A specific threat scenario for the considered use case. It is erroneous to think a general and global H&S evaluation despite a specific scenario.
- The health and security indicators impacted in the scenario.

One of the goals of the framework is to identify which metrics make sense to apply in a specific combination of threat scenario, H&S indicator and PoV.

3 Framework concepts

The main concepts behind this framework are:

- A DNS reference model that describes the main components, the domain name resolution processes, and the successful and unsuccessful termination conditions of that processes. This model is described in [1].
- The concept of point-of-view (PoV). A Point of View is intended as the perspective of a DNS actor/component in observing, using, operating and influencing the Global DNS. Each point of view has a different perception of DNS health and security. The PoV has influence on the system model used to evaluate DNS health and security, on the metrics used to quantify DNS health and security and on how those metrics should be measured. The possible PoVs are described in [1].
- A set of use cases[1] that will describe possible uses of the framework in a specific situation. For example: to evaluate how vulnerable a system (e.g. a service provider) is (focusing on the main DNS vulnerabilities); to evaluate if end user Service Level Objectives can be met; to evaluate if, from a specific PoV, some health indicators are moving toward a critical value (for the correct operation of a DNS component) etc. In the first phase of the project we will analyze use cases related to end-users and service providers. In the second phase of the project we will extend the study to NS operators. In [5] we describe the Web User use case.
- The measurement techniques and tools put in place to gather information needed to compute metrics. In section 2.2 we provide a first discussion on the matter.

Figure 1 sketches the main building blocks of the framework and their relationships.

[1] A use case is, in general, a situation where your system is used to fulfil one or more of your's user requirements; a use case capture a piece of functionality that the system provide. In our project, a use case is a specific situation where the DNS is used/operated by one of the DNS actors, the primary actor. Moreover, in a use case there could be one or more secondary actors that interact with the functionality requested.

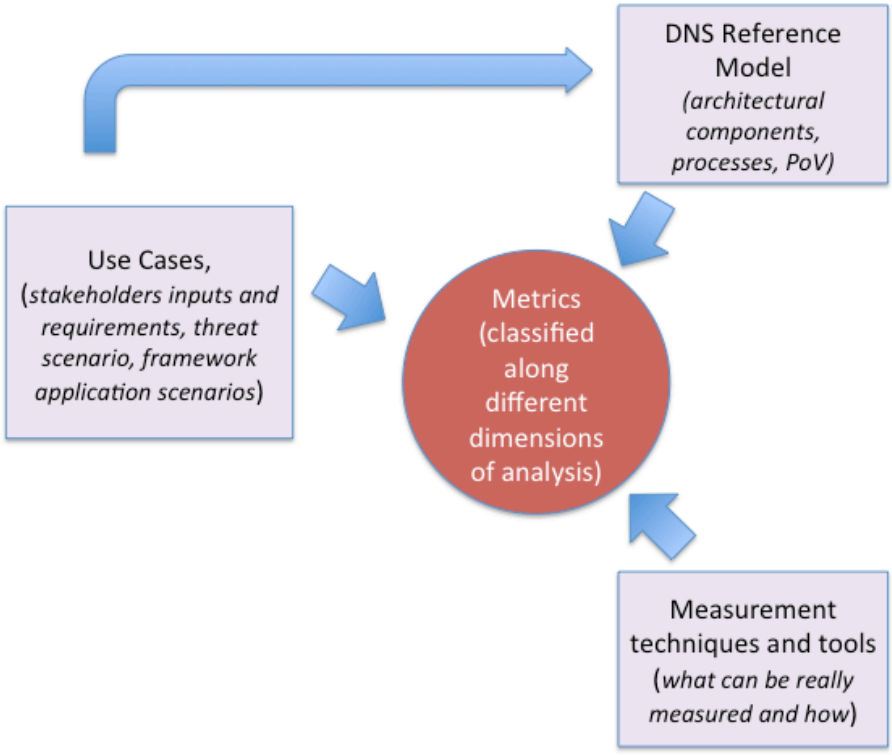

Figure 1 The framework building blocks

3.1. Point of View Definition

The framework for DNS Health and Security evaluation must be capable to respond to the different needs of its potential users. Each potential user fall in one of the categories mentioned in Section 1 (End users, Service providers and Operators) and each potential user can have one or more view of the DNS, depending on the components operated [1].

A Point of View is intended as the perspective of a DNS actor/component in observing, using, operating and influencing the Global DNS. Each point of view has a different perception of DNS health and security.
The six points of view we will consider in the analysis of DNS health and security are:

- *End-User* PoV,
- ASP PoV,
- *Resolver* PoV,
- *Name Server* PoV,
- *Zone* PoV,
- *Global* PoV.

In each of the above mentioned PoVs it is possible to directly observe and measure the behaviour of some DNS components while it is not directly possible to measure other not accessible components. To improve the H&S assessment capability the framework takes into consideration the possibility to integrate measurements directly collected with third parties data when and if accessible. The third parties

measures can be used in different ways, for example for H&S level comparison or to identify remote cause of H&S degradation.

3.2. Measurement techniques and tools

Measurement techniques and tools are extremely important for the implementation of the framework (and they will be explored as part of the project).
When talking about measurement we must take into consideration two aspects. First, depending on what can be measured and from where the measure can be operated, we have three different spatial horizons: Global level, ISP level and Enterprise level. Second, depending on the duration of the data collection and on the validity of the measured data we have four time horizons: Instantaneous, short term, medium term and long term.

The combination of the spatial and time horizons determines the type of measurement technique as well as the requirements for the reporting and analysis of the measured data.

In the following we discuss these two concepts of spatial and time horizon.

3.2.1. Spatial horizon

Measurement collection must be adapted to each metric being measured. For instance, availability of authoritative servers can, in most cases, be measured remotely. On the other hand, interaction with recursive caching servers requires the presence of probes in the network for which the server is provisioned. There is therefore a different spatial horizon for each type of measurement.
In general, these classes of spatial horizons will cover the different types of metrics:

- Global, where the service is available and can be measure from anywhere in the Internet
- ISP level, where big recursive servers are provisioned to serve large numbers of customers
- Enterprise, where a Local Area Network provides service to a small-medium sized closed group of users and includes provisioning of DNS services via a recursive caching server or a DNS forwarder.
    - A special case of the enterprise horizon is the home user, where a very small of users is served by an embedded DNS cache or forwarder in the access device (e.g. cable modem/DSL router)

3.2.2. Time horizon

The concept of time horizon is a notion related to the measurement and evaluation. The time horizon has an impact on different aspects of data collection and metrics evaluation, for example:

- Statistical significance of the samples;

- Practical significance of the measured index (e.g. resiliency or availability require a long term evaluation)
- Measurement campaign, data collection, data storage and analysis

The time horizons that will be considered in the framework are:

- Instantaneous: intended to evaluate the metrics values at a specific time instant.
- Short Term: used to evaluate the health and security level over a short time period, e.g. hours.
- Medium Term: used to evaluate the health and security over the medium term, e.g. days, weeks.
- Long Term: Used to evaluate the metrics over a long time period, e.g. Months.

4 Framework operation

In this section we describe the main phases of the framework and how it can be used in an operational environment. To help to clarify some concepts we use the example of an end-user wanting to diagnose the health and security level achievable and/or to evaluate if specific Service Level Objective (SLO) can be satisfied.

The implementation of the framework for a specific PoV should allow to:

- Diagnose, both at preliminary and detailed level, the health and security level perceived;
- Specify desired SLO;
- Evaluate what SLO can be satisfied
- Suggest why SLO cannot be satisfied.

In the framework we isolate the following three phases:

- Preliminary Diagnosis
- Definition of Service Level Objectives and scenario
- Detailed diagnosis and measurement

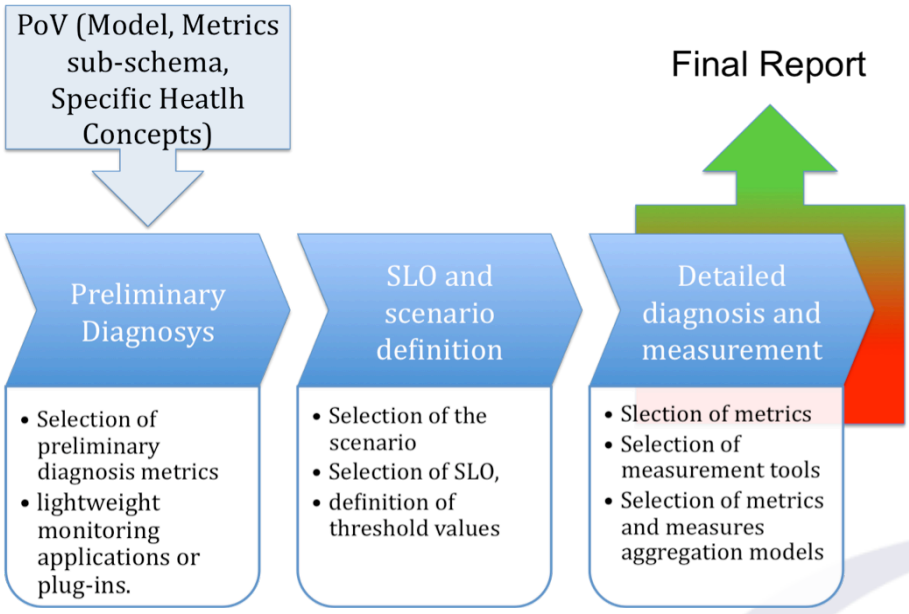

Figure The framework phases

The Preliminary Diagnosis is the phase in which the framework is used to perform a first evaluation of the health level perceived performing simple measurements and assessments. Preliminary diagnosis requires:

- To identify a set of preliminary diagnosis metrics
- To implement/select lightweight monitoring applications or plug-ins.

The definition of the Service Level Objective is related to what it is possible to measure given a PoV. For example, from an end-user point of view it is possible to measure the speed, coherency, availability.

In this phase the framework's user will chose also the threat scenario, i.e. against what the H&S must be evaluated. For example in the end-user PoV can be evaluated the H&S with respect to System corruption threats, e.g. Cache poisoning.

The detailed diagnosis and measurement phase is oriented to identify:

- What is the health and security level of the portion of DNS viewed by the specific PoV, in the threat scenario previously defined;
- What are the SLO achievable and what can not be achieved;
- What are the causes of SLO violation (optional);
- How to improve H&S level(optional).

Let us consider the example of an end-user. The end-user has no control of the DNS and on the Internet. The end-user does control the configuration of its local resolver (e.g., the initial DNS server it uses) and some parameters of the Internet connection. Therefore, the end-user has very limited power to improve the H&S level perceived. However, improving end-user awareness is important. The framework could be used to provide a picture of the health and security level experienced. If the end-user cannot improve its health and security level it can always behave in a more responsible/safe way (is this an utopia?!?!?).

The detailed diagnosis and measurement phase is divided in three more steps:

- The selection of metrics,
- The measurement phase,
- The aggregation phase.

At the end of the project there will be a complete set of metrics filling as much as possible the metrics mapping matrixes introduced in [1]. Therefore, defined the PoV, the threat scenario and the desired H&S indexes, the metrics that must be evaluated are automatically selected. This is the task of the selection of metrics phase.

The measurement phase is related to the collection of data and to the computation of the selected metrics. The order in which measures are collected is very important to have a reasonable evaluation of the H&S level. In [1] and [5] we describe a bottom up measurement model. In the measurement model we propose, information from other PoVs (if needed and/or recommended) are firstly acquired. Then, through the evaluation of indexes such as network reachability or network load it is evaluated if the measurement can be compromised by a critical state of the infrastructure. Finally, the more specific H&S metrics are evaluated and results are aggregated and/or compared with information acquired by third parties and/or lower level metrics.
The Aggregation phase describes how all the measures collected in the previous phase will be combined together to provide a summary of the Health and Security level perceived by the PoV, what are the achievable SLOs, what SLOs cannot be achieved and finally what could be the cause of health degradation and possible solutions.

5 References

[1] E.Casalicchio, M.Caselli, D.Conrad, J.Damas, I.N.Fovino, "Reference Architecture, Models and Metrics", GCSEC technical document, Version 1.5, July 2011

[2] Measuring the health of the Domain Name System, Report of the 2nd Annual Symposium on DNS Security, Stability, & Resiliency, Feb 2010, Kyoto, Japan (Apr. 2010), https://www.icann.org/en/topics/ssr/dns-ssr-symposium-report-1-3feb10-en.pdf

[3] ICANN, Security, Stability and Resiliency of the Domain Name System, Jan. 2009 http://www.gtisc.gatech.edu/pdf/DNSSSRPaper.pdf

[4] E. Casalicchio, D. Conrad, J. Damas, I. Nai Fovino, S. Di Blasi "DNS Metrics Use Case", Internal report, version 0.6, May 2011 –

[5] E.Casalicchio, M. Caselli, D.Conrad, J. Damas, I.Nai Fovino"Framework operation, the Web user PoV", GCSEC report, Version 1.1, July 2011