DNS as critical infrastructure, the energy system case study

Emiliano Casalicchio

Department of Civil Engineering and Computer Science,
Univ. of Rome 'Tor Vergata',
Via Orazio Raimondo, 18 - 00173 Rome, Italy
E-mail: casalicchio@ing.uniroma2.it

Marco Caselli, Alessio Coletta and
Igor Nai Fovino*

Global Cyber Security Centre,
Viale Europa, 175, 00144 Rome, Italy
E-mail: marco.caselli@gcsec.org
E-mail: alessio.coletta@gcsec.org
E-mail: igor.nai@gcsec.org
*Corresponding author

Abstract: Modern critical infrastructures (e.g., power plants, energy grids, oil pipelines, etc.), make nowadays extensive use of information and communication technologies (ICT). As a direct consequence their exposure to cyber-attacks is becoming a matter of public security. In this paper, we analyse a particular infrastructure, rarely considered as source of threats, on which indeed the majority of network based services rely. the domain name system. Taking as example the power system, we show how deeply a failure (accidental or malicious) of the DNS might impact on the operation of the modern and distributed critical infrastructure.

Keywords: domain name system; DNS; security; power system.

Reference to this paper should be made as follows: Casalicchio, E., Caselli, M., Coletta, A. and Fovino, I.N. (2013) 'DNS as critical infrastructure, the energy system case study', *Int. J. Critical Infrastructures*, Vol. 9, Nos. 1/2, pp.111–129.

Biographical notes: Emiliano Casalicchio is a Researcher at the Computer Science Department, University of Rome 'Tor Vergata'. In 2002, he received his PhD in Computer Science. In 2004 and 2007, he was a Visiting Professor at George Mason University, Fairfax, VA. Since 2008, he is an Affiliate Professor at the University of Roma La Sapienza. He is the author and co-author of more than 60 papers published in international journal and conferences. His research is mainly framed in two fields: performance oriented design and evaluation of large scale distributed systems and analysis, modelling and simulation of critical information infrastructures.

Marco Caselli holds a Master degree in Computer Engineering obtained from the ’Sapienza’ University of Rome (2011). His background is focused on architectures and distributed systems with particular regard on safety and security issues. He has recently published scientific papers on DNS security for international conferences such as IFIP and SATIN. Before entering in the GCSEC team, he did an internship at the ’Engineering S.p.a.’ (2008–2009) as a Researcher and Software Developer and worked as a Consultant for ’Total Consulting System S.r.l.’ (2011).

Alessio Coletta received his Master degree in Computer Science at the University of Pisa and a Diploma in Computer Science at Scuola Normale Superiore di Pisa. He performed activity research in theoretical aspects of Computer Science as PhD student at the University of Pisa. Currently, he works as Scientific Officer of the European Commission at the Joint Research Centre. His main research topic are malware, ICT security, industrial communication protocols, and critical infrastructure security.

Igor Nai Fovino is the Head of the Research Division of the Global Cyber Security Center. He holds a PhD in Computer Security. His research fields belong to the area of ICT Security of industrial systems, intrusion detection, cryptography and malwares. He is the author of more than 60 scientific papers published on international journals, and books. During his career, he worked as a researcher at the University of Milano and as a Professor of Operating Systems at the University of Insubria. From 2005 to 2011, he served as a Scientific Officer at the Joint Research Centre of the European Commission.

This paper is a revised and expanded version of a paper entitled ’The role of the DNS in the secure and resilient operation of CIs, the energy system example’ presented at 6th International Conference on Critical Information Infrastructures Security (CRITIS ‘11), Lucerne, Switzerland, 8–9 September 2011.

1 Introduction

A critical infrastructure is a system that has a strong impact on people’s everyday life and that, if damaged, can cause significant consequences on the safety and security of citizens. An example of industrial infrastructures considered critical are: power plants and energy grids, gas and oil pipelines, nuclear and chemical plants, water treatment systems. Other critical sectors strictly interdependent with the above mentioned infrastructures are transportation, finance, health, and food.

Nowadays the *information and communication technologies* (ICT) are increasingly involved in the development and the management of these infrastructures. This is a positive factor since it is possible to increase the number of available services and to optimise them. With ICT solutions it is also possible to implement distributed mechanisms for self-orchestration and to manage remote installations efficiently. This leads to an important considerations: *the ICT systems that realise these services* (*e.g., public and private network, computational and storage resources, operating* *systems and applications*) *become critical, as they are essential elements of critical infrastructures.* The ICT systems supporting or composing critical infrastructures are usually referred as critical information infrastructures (CII).

This work focuses on the role of the domain name system (DNS) in critical infrastructures. The DNS is a world-wide system that enables the application level internet services to work properly, translating URLs to the IP addresses. Therefore, secure and resilient services of critical infrastructures rely on DNS correct operations. The DNS is seamlessly used to in the maintenance, management and control of a large number of CIs (e.g., to access a networked control system, in management and control of transportation or in the ICT infrastructure supporting stock exchanges). A direct implication of this fact is that a DNS failure might indirectly have a significant impact on the security and safety of the CIs and consequently on general welfare. In this paper, we analyse the effects of possible attacks against the DNS, on the energy CI. Moreover we discuss how an effective monitoring, analysis and understanding of the DNS stability, security and resiliency level can be used to prevent incidents.

Among other industrial infrastructures, the importance of energy smart grids is increasing. In this context, the energy system provides an extremely interesting case study of large-scale critical infrastructures relying on ICT and public networks. In this paper, we first summarise the structure and functions of energy systems from an high level point of view. Then, we analyse the consequences of certain types of DNS vulnerabilities on the operation capabilities of the whole infrastructure. Finally, we present at high level the concept of DNS health and a framework allowing to asses the health level of the global DNS.

2 The DNS: an overview

The internet is the world's largest computing network. There are two important namespaces that allow us to find resources on the web: the IP address system and the domain name hierarchy.

The *DNS* is the global infrastructure that maintains the domain name hierarchy coherent and manages the translation of domain names in the related IP addresses. We can consider the DNS as a suite of services and protocols as well as an information infrastructure. The DNS concepts and facilities are defined in the IETF RFC 1034 (standard), updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936.

The whole system is organised hierarchically with all the entities geographically and logically distributed. The global DNS database is stored in nodes referred as name servers (NSs).

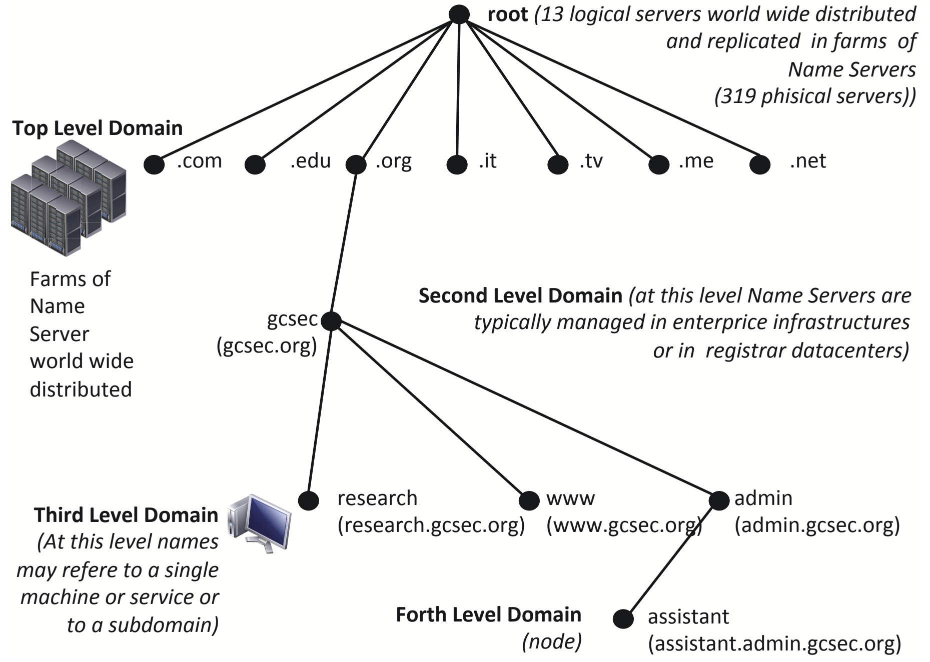
To facilitate administration processes, the concept of DNS 'zone' is defined to describe administrative building blocks of the DNS name space. These are typically used to refer to a domain managed as a single administrative entity.

On top of the hierarchy (see Figure 1) there is the so called root zone. It is represented by the symbol '.' and acts as a junction of all the other zones. The next level consists of the top level domains (TLD) (e.g., .com, .it). From the laters branch off second-level domains, called also enterprise-level domains.

Each of the previous entities have authority over a portion of the domain name space. Companies managing the root zone are called root operators while those operating

NSs related to TLDs are called registries. These last work on national scale (for country code TLDs) or also on a global scale (for global TLDs).

Figure 1 The DNS hierarchy, from root down to the n^{th} level domains (see online version for colours)


root (13 logical servers world wide distributed and replicated in farms of Name Servers (319 phisical servers))
Top Level Domain
.com
.edu
.org
.it
.tv
.me
.net
Farms of Name Server world wide distributed
Second Level Domain (at this level Name Servers are typically managed in enterprice infrastructures or in registrar datacenters)
gcsec (gcsec.org)
Third Level Domain (At this level names may refere to a single machine or service or to a subdomain)
research (research.gcsec.org)
www (www.gcsec.org)
admin (admin.gcsec.org)
Forth Level Domain (node)
assistant (assistant.admin.gcsec.org)

The so called registrars are instead authorised entities entitled to register domain names in a particular TLD to end-users. When the registrar receives a user's registration request, it verifies if that name is available by checking with the appropriate registry that manages the corresponding TLD. If it is, the registrar proceeds registering the name with the registry That, for its part, adds the new name to its registry database and publishes it in the DNS.

DNS main functions are:

- *DNS query/response*: It is the most known and used transaction in the DNS. A query originates from a client that wants to access some DNS services. Components that make queries are called resolvers. Data are normally sent in plain text. This fact obviously allows potential attackers to intercept and modify response information.
- *Zone management*: This represents all the operations used to keep information coherent among zone NSs. The main transaction regards a secondary slave server that refreshes the entire content of its zone file asking for data to the primary master. The zone transfer has many security implications because it exposes much more information than the other transactions (all the information for a specific

zone). Moreover a potential attacker can take advantage of the increased resource usage of this kind of messages.

- *Dynamic services*: These services allow to dynamically add/delete subsets of resource records for existing domains. There is also the possibility to delete entire domains or to create new ones.
- *DNS administration*: This represents the set of administrative tasks performed by operators (or any other responsible entity) used to guarantee security and performance of the services.

3 The energy system: an overview

An energy system can be logically divided in several subsystems with different purposes. These subsystems collaborate to provide energy to hundreds of million of people creating a sort of cross-country energy balance. In what follows, we will describe at high-level the most important elements and relations inside energy systems.

Network hardware like stations, transformers and circuit breakers represent the physical layer of a power system.The operation of the physical layer is managed by ICT control and communication centres and devices that represent the cyber layer of the infrastructure.

From a physical point of view we can categorise power system elements as follows:

- *Transmission stations*: these are generally operated directly by the transmission system operator (TSO).
- *Power plants*: usually these are owned by different companies.
- *Distribution systems feeders*: these are buses equipped with transformers. They are the starting point of the medium voltage distribution system. Each distribution system operator (DSO) owns and operates as a monopolist the distribution system over a certain portion of territory.
- *Large utiliser*: these are those energy users that demand high power (>5 MW).
- *End users*: connected to the distributions buses, they constitute the leaves of the energy system. However with the advent of modern smart-grids the category end user will change a lot since each user will become also an energy producer.

As already said, power systems are complex infrastructures and, for this reason, they need massive communication to be maintained in function. Information can be real-time data but also commercial and administrative ones and flow between control centres and substations as well as among different operators.

The cyber layer of an energy grid can be divided in different subsystems:

- *Control network*: it basically contains remote terminal units and programmable logic controllers. It interfaces directly with the field network containing actuators and sensors that physically perform some process tasks. The control network is connected with the process network described below.
- *Process network*: it contains SCADA servers and all the other systems gathering information from the control network. It has also an active task consisting in

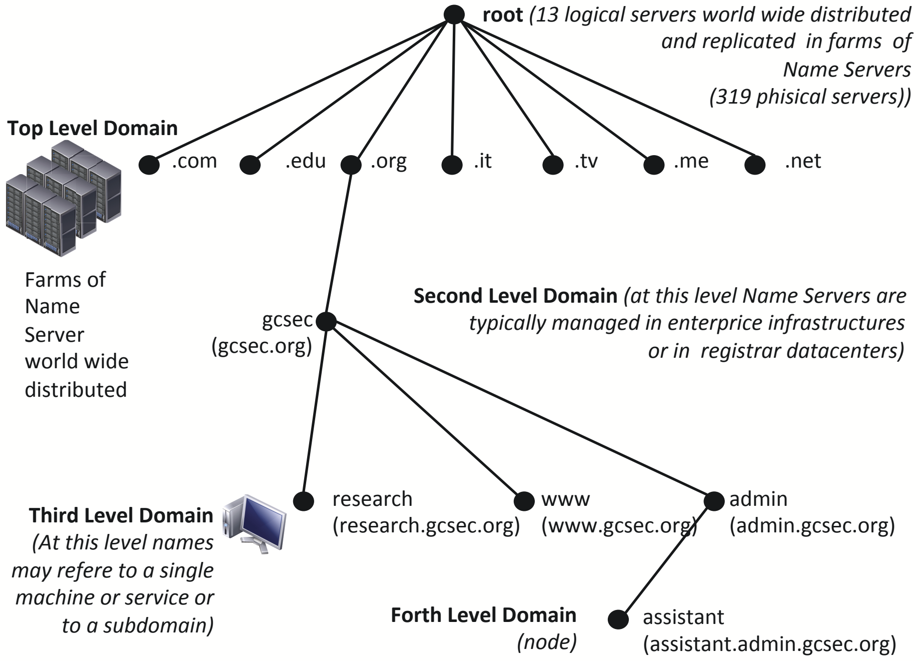
sending commands to the control network, gathering measurements and raising alerts.

- *Exchange area*: this is an area that usually contains aggregation databases. The process network sends to these databases data that represents the working state of the system. This information is used by diagnostic systems to detect anomalies. Control centres operators can remotely access such databases to have a high level view of the process state.
- *Control centres*: they represent the set of remote human machine interfaces (HMI) that are used by the operators to obtain information about processes and to let them perform operational activities to modify the process state.

It is worth noticing that the system view we proposed is multilayered. Different companies own infrastructures and systems described above and these last interact at different levels in an interleaved manner (from the low industrial floor to the higher market and coordination level).

Figure 2 sketches the main building blocks of the network of a generic power plant.

Figure 2 Power plant network schema (see online version for colours)


root (13 logical servers world wide distributed and replicated in farms of Name Servers (319 phisical servers))
Top Level Domain
.com
.edu
.org
.it
.tv
.me
.net
Farms of Name Server world wide distributed
gcsec (gcsec.org)
Second Level Domain (at this level Name Servers are typically managed in enterprice infrastructures or in registrar datacenters)
Third Level Domain (At this level names may refere to a single machine or service or to a subdomain)
research (research.gcsec.org)
www (www.gcsec.org)
admin (admin.gcsec.org)
Forth Level Domain (node)
assistant (assistant.admin.gcsec.org)

4 The impact of DNS on energy system operations

As shown in the previous sections, the typical ICT architectures of power systems adopt traditional ICT networks for interconnecting sub-components. Although standard

ICT technologies are crucial for industrial systems, operational best practices and the scientific literature do not usually take the DNS, which is part of these technologies, with the same attention. Nevertheless, DNS issues may have a big impact on the power system operations. We divided the power system infrastructure into two views in order to better analyse the DNS impact: a *high level* one and a *low level* one, characterised by certain classes of operations explained in the following sections. Moreover, we partitioned the set of DNS vulnerabilities into five classes, as suggested by Santcroos and Kolkman (2007): *repository corruption*, *system corruption*, *protocol issues*, *denial of service* (DoS), and *information exposure*.

An analysis of the impact of each of vulnerabilities on every operation class follows.

4.1 DNS and the power system high level infrastructure

The *high level infrastructure* of a power system is characterised by the following high level operations:

1 management of the energy market

2 links between industrial actors and end users

3 links between the power sector and industrial actors

4 actions at the customers's premises

5 coordination among power producers

6 coordination among transmission companies

7 management of crisis/blackout.

The DNS affects all of these operations. A list of the effects of DNS issues follows.

4.1.1 Management of the energy market

The operations for managing the energy market concern the interactions between the industrial actors, the brokers, the wholesale market, and the marke clearinghouse. DNS issues affect the energy market in a way similar to the ones regarding the web application security. DNS failures and malfunctions have a big impact on the energy market, in terms of availability and stability, and may cause important financial loss.

We describe here some threat scenarios related to the classes of vulnerability concerning the DNS:

- *Repository corruption*: a complex attack could reroute some energy market data to fake servers causing the disclosure of sensible information or to change the perception of market trends. Such an attack can be based on the *corruption of DNS repository* (e.g., authoritative or cache database corruption). Corrupting DNS entries might also affect the energy production: for example, a DNS repository corruption can hijack the acquisition of energy stocks on the market, through the access to fake servers. These attacks might affect the economical and social aspects of a country, in case of possible cuts of energy, at country level or, even worst, at continental level.

- *System corruption and protocol issues*: the same issues of the previous case also apply for the corruption of the whole DNS or for vulnerabilities of the DNS protocol.
- *DoS*: A DNS DoS is usually capable of making a service unreachable. Thus, it might cause the unreachability of the energy market network infrastructure. DoS attacks are easily visible, so they usually do not last very long. For this reason the effects of a DNS DoS on the energy market are limited, because the actors can avoid accessing the market services for a short amount of time. Nonetheless, if DoS attacks make the services unreachable during critical operations or during unexpectedly high requests of energy, the financial loss may be high as well.
- *Information exposure*: some attackers may be interested at discovering important details about the energy infrastructure, for example in order to carry out other attacks such as corrupting the DNS cache. The actual harm of information disclosure is insignificant in the first place, but precise insights about DNS nodes in the energy infrastructure might lead to more complex attacks.

4.1.2 Links between industrial actors and end users

This class of operations concerns the communications between energy companies and end-users. Among these: meters, billing energy services interface, aggregators of retail energy providers, and energy service providers.

Smart meters deserve special consideration. Many smart meter solutions employs both GPRS technologies and TCP/IP channels. Usually, the connection from the meter to the local aggregator is GPRS-based, while from the aggregator to the enterprise servers is IP-based. A DNS attack may be effective on the IP-based part of the data control and acquisition architecture. For example, it may allow to switch off the power of a user, to alter the customers' bill, to disable the detection of malfunctioning services causing illicit usage of the infrastructure, and so on. Lately, mobile applications enables the users to remotely control home energy consumption, and DNS is likely necessary for the availability of these applications. Similarly, the websites of the energy companies needs the DNS to provide the customers with billing or payment services.

In this context, some complex attacks can be based on DNS repository corruption, DNS system corruption, and protocol issues, for example:

- Corrupting the DNS cache along the communication path between the meters and the aggregation servers may enable to deviate the traffic to a fake server. The billing process can be affected as well. The end-user energy production case is even more important, because a fraudulent customer may be willing to change his energy output records, leading the energy company to money loss. However, in this case the DNS attacks do not harm the energy infrastructure.
- DNS DoS attacks may be annoying or dangerous for the the metering and billing process. In this case, the damage is likely only economical.
- Unauthorised information disclosure (information exposure) between the energy enterprise and the end-user do not cause any immediate damage. Nevertheless, an attacker may need that information to carry out more complex and effective attacks.

4.1.3 Actions at the customers's premises

This class of operations deals with the user appliances and service. These operations are similar to the ones regarding the links between industrial actors and end users from a technical point of view. Also in this case DNS may have a relevant role. Examples of operations of this group are: management of appliances, electric vehicles, other related services (gas/water metering), home automation, etc.

4.1.4 Links between the power sector and industrial actors

Energy companies usually rely on tight links and business connections with the producers of power devices for the maintenance of their infrastructures. Device producers typically provide remote support services, which are based on VPN connections through public networks and access the process control network of the power enterprise. These operations rely on DNS, used for the resolution of names of the servers involved. Any related issue, like DNS unavailability or corruption, might interrupt maintenance operations on the physical installations. Once a VPN tunnel is established, two DNS systems acting at both sites of the connection take in charge the name resolution processes of internal NSs. Generic misconfigurations or any other issues related to either the producer or the energy company sites affect the security of the whole system. A possible consequence could be the hijacking of operation flows to bogus servers or the blocking of the entire communication. It is worth noticing that the DNS plays a twofold role as infection dozer and actuator. The first regards situations in which the hijacking of connections towards fake sites triggers a silent installation of malicious code that will produce damages later. The second describes a direct impact on the company installation sub-network services (e.g., availability of those services).

4.1.5 Coordination among power entities

This category includes the following actions:

- The coordination among generation companies. This is mainly related to the amount of energy to be produced and is based on operations and communications that increasingly uses ICT technologies. As a consequence, the impact of the DNS on these actions is very high. For example power companies might not be able to communicate properly energy production plan details to each other and a possible effect could be an energy shortage.
- The coordination among transmission companies. Similar to the previous case, we can do almost the same considerations.
- The management of crisis/blackout. Traditionally there are well structured plans and procedures to coordinate energy actors during crisis (e.g., during a blackout). However it is important to emphasise that the use of the public network (e.g., mailing systems and other applications) in support of coordination policies is increasing. Also in this case, DNS is deeply involved. The impact of DNS repository corruption, system corruption and DoS is potentially heavy. For example, messaging delays during a blackout emergency can lead to dramatic situations where entire countries are left without energy. The situation described

can be considered, at this level, the most sensible operation in term of impact on the citizen life.

4.1.6 High level layer impact conclusions

Basically, all these high level power infrastructure operations rely on web-services or applications that use the internet to exchange information, perform transactions, and provide services. In the cases described above the DNS plays often a relevant role since its failure or corruption might have a dramatic impact. A noteworthy example could be the influence that DNS issues can have on pricing and availability of the energy market. Similarly, a DNS failure during an energy crisis (e.g., blackout) can impact the high level control centres collecting field data, and indirectly slow down the definition of a proper contingency plan. The coordination among power producers is really important to guarantee the stability of an energy grid and a failure of the DNS could damage this process.

4.2 The impact of DNS on the industrial installations

In the previous section we showed how a DNS failure might have an impact on the higher level of the power system. Unfortunately the DNS is heavily used also in the operation of what we call here *low level infrastructure* i.e., the industrial installation. Effects of a failure here might have a huge impact not only on the operation of the installation, but also on the citizen life.

When referring to power control systems, we generally indicate the control system of generation plants, i.e., those systems used to control turbogas power plants, geothermic plants, etc.

Traditionally the control system of these type of industrial installations was considered a completely closed environment. The control of the field network was based on serial communication protocols and everything was monitored and managed locally. In the last ten years however, thanks to the diffusion of TCP/IP, the architecture of these installations changed dramatically becoming more and more similar to the architecture of generic IT corporate infrastructures. Also the traditional serial networks have been slowly substituted with more generic switched TCP/IP based networks (usually embedding the original industrial protocols as application layers within the TCP/IP suite). Today, basically every active element in the modern energy control system is associated with an IP address. Studies conducted in the field (see for example, Creery and Byres, 2007) have shown how it is becoming more and more common for power systems to rely on the DNS for the resolution of the server involved in the control process.

In the following we describe the impact of a malicious DNS failure on this part of the *power system*. The outcomes can be easily applied also to other type of industrial installations involved in the energy system operations as those used in the transmission grid and in the distribution network.

4.2.1 Process communication flows

The core of every industrial installation is the process network, i.e., the network hosting all the servers playing a role in the control and monitoring of the processes running in the plant. The process network, roughly speaking, contains SCADA servers, diagnostic servers, OPC (open link and embedding – OLE – for process control) gateways mapping control flows into commands understandable by field devices, etc. In modern power plants, it is quite common to rely on an internal DNS for the resolution of the server names. The effects of a failure of the DNS, in that case, might impact several vital functions of the installation, from the detection of anomalies (e.g., the impossibility for a diagnostic server to detect a broken valve in the plant or to deliver the related alert), to the impossibility for a SCADA server to control the process and the system state. In the first case an undetected anomaly (for example a variation in the rotation of a gas turbine) can cause physical damage to the system and a system stop. In the second case, losing the control capabilities of the SCADA servers could make it impossible to react sufficiently rapidly to a critical change in the system state.

4.2.2 Debug, upgrade and maintenance operations

Industrial installations, especially those complex as power plants, require a huge effort in term of maintenance and upgrade. A quite common practice, in modern plants, is that of outsourcing these operations to external actors, e.g., system integrators and vendors, to limit the need of having in-house experts and maintenance teams. While in the past these contractors were used to deliver their maintenance services on site, with the advent of modern ICT technologies, it becomes more and more common to see these services delivered remotely.

The standard procedure consists of:

1 establishing a site-to-site VPN connection between the external company network and the network of the plant owner

2 accessing the power company domain through a radius authentication

3 accessing the installation sub-network

4 performing the required maintenance operation.

It is evident how, in all this procedure, DNS plays a relevant role. In fact, to map both external entry points and internal servers it is reasonable to use DNS. In this case, a repository corruption attack, a cache poisoning seizure or a DNS DoS can be used by an attacker for:

1 rerouting the maintenance flow between the device producers site and the local plant network site

2 making hard or impossible for an operator to establish a connection with a remote site, and then making the maintenance of key elements of the system impossible.

The aims of these attacks can be twofold:

1 to cause a corrupted state of the real system while showing false data to the operator

2 to prevent a maintenance operation to be correctly performed.

In both cases the impact on the installation might be extremely heavy. Dealing with critical devices such as gas turbines, high voltage lines, or in the worst case, nuclear power plant, a missed maintenance operation might have dramatic effects.

4.2.3 Process monitoring

The monitoring of the plant processes is not completely auto-driven. Human operators use the HMI to monitor the activities of the process system. HMIs have different means for presenting to the operator the state of the system. They can connect themselves directly to SCADA servers or they can access *historians*, i.e., real-time databases that aggregate information coming from the field network, presenting to the HMI only the relevant views or set-points. The number of servers to be accessed by HMI is increasing and for that reason in modern installations is quite common to use names instead of IP addresses. Moreover, in several situations these activities are performed remotely in the broader sense, i.e., from operators located in a completely different place, using an external network and relying on the internet to reach the access point of the installation sub-network. Again, the DNS plays a role in making the connection possible as in the case of the maintenance operations, and again, its failure or its corruption might make it harder or impossible to control the process system remotely. Fovino et al. (2010) show how a DNS poisoning attack could be used as part of a complex cyber attack against a turbo-gas power plant to re-route the operator on a false SCADA server.

4.2.4 Centralised monitoring

In the modern power grid, plant installations are controlled not only locally, but also remotely by a limited number of control centres. These centres are in charge for the *multiple orchestration and synchronisation* of the different installations. The different applications hosted in the control centres generate query/response flows from the local HMIs to the remote RT-Databases of the installations and to the diagnostic servers. Also in this case it is evident how the DNS plays a relevant role. Keeping track of all the servers involved without relying on a DNS would be hard and not efficient. Moreover in this way, operations as the remapping of the address of a server can remain basically seamless to the control software, since everything can be managed at DNS level. Another important function of control centres consists in delivering the daily production plans specifying the energy production, hour by hour for each power plant of the system. These plans are automatically delivered to each plant by using

a a dedicated network

b the public network in combination with the use of VPNs and MPLS features.

A failure of the DNS here might have significant effects on the definition of reaction plans against energy crisis or might compromise the energy production plan.

In these last scenarios, further attention should be also paid to the role of DNS as a vehicle for establishing unfiltered covert channels with already infected hosts within the energy company sub-networks: exfiltration of data from control systems or exchange networks, be it measurement data, performance reports, operational plans or critical assets inventory, can lead to severe security risks for the continuity of operations.

Typically, even though company sub-networks are isolated from public networks, they need a set of basic services such as the resolution name service, and when a target host within a company sub-network is already compromised, data exfiltration can be achieved through forwarded DNS queries, which resolve to a NS actually under the attacker control; in this way, the malicious application, running over the infected machine, can send ad-hoc queries to a specific URL, which will issue for example the transfer of sensitive data archived in the sub-network to the attacker NS, without having application level firewalls or intrusion detection/prevention systems to actively log suspect HTTP traffic. Deep DNS queries and responses inspection should be ensured in order to mitigate this risk.

4.3 Industrial installation impact conclusions

As described in the previous subsections, the DNS plays a relevant role in several of the daily operations performed in a typical power plant. What is important to underline is the stratification of this phenomenon: DNS is involved into completely different operations, dealing with scopes and with environment completely heterogeneous. DNS is involved for example in the communication between field devices and control systems, in the information gathering process, in the maintenance operations, etc. This fact magnify even more its relevance. An attack against the DNS in that case would be able to impact several different layers of the installation, causing a huge number of different damages.

5 The DNS health measurement framework

The presented case demonstrates how critical the DNS is for the operation of the energy system. Knowledge about its security level and about the impact of its failure on their systems would greatly help operators in planning and adopting contingency plans. This knowledge can be obtained only developing a framework defining a set of metrics and methods for the evaluation of the DNS security, stability and resilience (SSR).

A similar set of metrics would be extremely useful in the power system context, to assess the SSR level of the DNS system involved in the power operations, as well as, more generally, it would be useful to all those entities involved in the operation of critical infrastructures. The outcomes of the analysis of the SSR data would allow operators to understand and measure the security level of their DNS infrastructure; moreover, a configurable and modular framework supporting ‘what-if’ and impact analysis of DNS reengineering and DNS policy making would again make easier to understand their potential effects on critical infrastructures. The efforts of ICANN provided a highly useful foundation for further studies on the SSR of the DNS. The results of ICANN (2010) DNS SSR Symposium 2010 introduced the concept of DNS health as a set of high level indicators expressing the level of healthiness of the global DNS. However, the definition of security metrics in the DNS remains at a primitive stage and metrics for DNS stability and resiliency are largely uncharted territory.

Under this light, the *Global Cyber Security Centre* is coordinating and supporting an international initiative with the aim of creating a framework allowing to provide an answer to these questions. In the following we provide a brief overview of a measurement framework we are building at this purpose (for more details please see Casalicchio et al. (2012).

The framework is built along three main dimensions of analysis:

- the point-of-view (PoV)
- the health indicators
- the metrics.

The *point-of-view* dimension is introduced since each DNS actor has its role in the use and operation of DNS and therefore each actor influences and perceives DNS health in a different way (see Figure 3. Taking as example the energy use case, it is evident how the health of the DNS is perceived differently if, for example, we consider the DNS operator point of view or if we consider the end user (the power plant) point of view. The DNS components we have taken into consideration are grouped in three main categories:

- *End-users*, who are mostly unaware of the DNS, e.g., a philosopher surfing the web.
- *Service providers*, who provide services using distributed applications accessible by web interfaces. A service provider can totally or partially control the infrastructure used to run the distributed application. We mainly refer to web applications, web services technologies, and service oriented systems.
- *Operators*, who manage and operate the DNS, namely: root NS operators, TLD NS operators, internet service providers managing large NS caches, authoritative NS operators for second level domains, non-authoritative resolvers (e.g., OpenDNS or GooglePublicDNS).

Health indicators (coherency, integrity, speed, availability, resiliency, stability, security and vulnerability) are introduced in ICANN (2009, 2010) and must be specialised for each specific perspective.

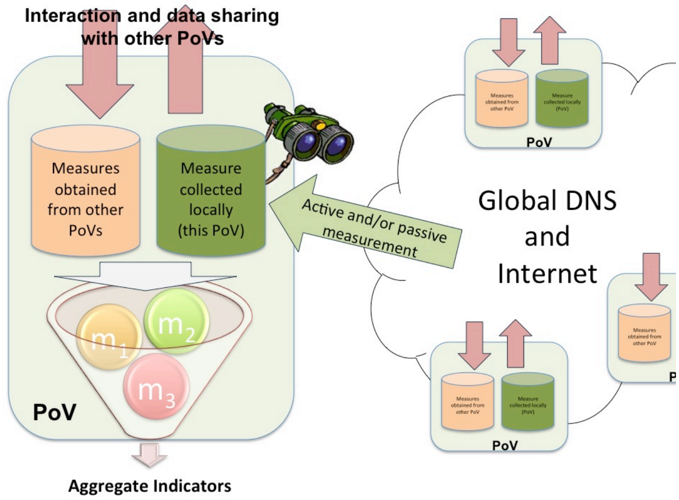
A part from the PoV, the health and security (H&S), is also linked to the threat scenario considered in the analysis. For example, if we consider the system corruption scenario it makes sense to measure the *non-existent domain detection rate* or the *cache poisoning probability*, while in a DoS scenario it makes sense to measure the *rate of repeated queries* or the *bandwidth consumption*.

Summarising, each time the H&S level of the DNS is evaluated, the framework consider:

- A specific use case; 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.
- The H&S indicators impacted in the scenario.

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

Figure 3 Concept of PoV (see online version for colours)


Interaction and data sharing with other PoVs
Measures obtained from other PoVs
Measure collected locally (this PoV)
m_1
m_2
m_3
PoV
Aggregate Indicators
Active and/or passive measurement
Global DNS and Internet
Measures obtained from other PoV
Measure collected locally (PoV)
PoV
Measures obtained from other PoV
Measure collected locally (PoV)
PoV
Measures obtained from other PoV

Notes: The PoV creates its own knowledge of the health state of the DNS mixing local and remote information. Locally collected information are shared with other PoVs.

A good way for identifying the suitable metrics is first of all to analyse the vulnerabilities they should be able to identify. The most common *DNS vulnerabilities*, present in many threats scenarios can be grouped into the following classes: *cache poisoning*, *distributed DoS*, *response modification route injection*, *origination modification*.

Such vulnerabilities, and many more, can be classified into the five main threats categories introduced above (see Section 4). In this paper, vulnerability metrics are organised along five categories that match the main DNS vulnerabilities mentioned above.

Metrics characterising security of the DNS, defined as the ability of the DNS to limit or protect itself from malicious activity, have yet to be defined. The framework contains a set of metrics that, taken together, can contribute to the evaluation of DNS security readiness with respect to a possible set of attack scenarios.

DNS resiliency is defined to be the ability of the DNS to effectively respond and recover to a known, desired, and safe state when disruption occurs (e.g., response and recovery after a distributed DoS attack). Resiliency is viewed by users as availability and viewed by providers as a combination of detection, response, resistance and recovery processes that increases the overall confidence in relying on and investing in the internet over the long-term. As resiliency metrics we use a set of metrics aimed at measuring the resiliency of a generic ICT system and apply those metrics to the resiliency of the DNS.

For a list of the metrics identified during the first phase of the study and more details about their definition and about the way they can be measured or calculated, we point the readers to the deliverable of the MeNSa project (GCSEC, 2011).

Figure 4 sketches the main building blocks of the framework and their relationships. The metrics and the point of view are the core of the framework. By using the PoV it would be possible to define the best set of measurable metrics, and to aggregate them in order to obtain useful indicators of the DNS health in a given scenario.

Concerning the framework operation, it is organised in three macro phases:

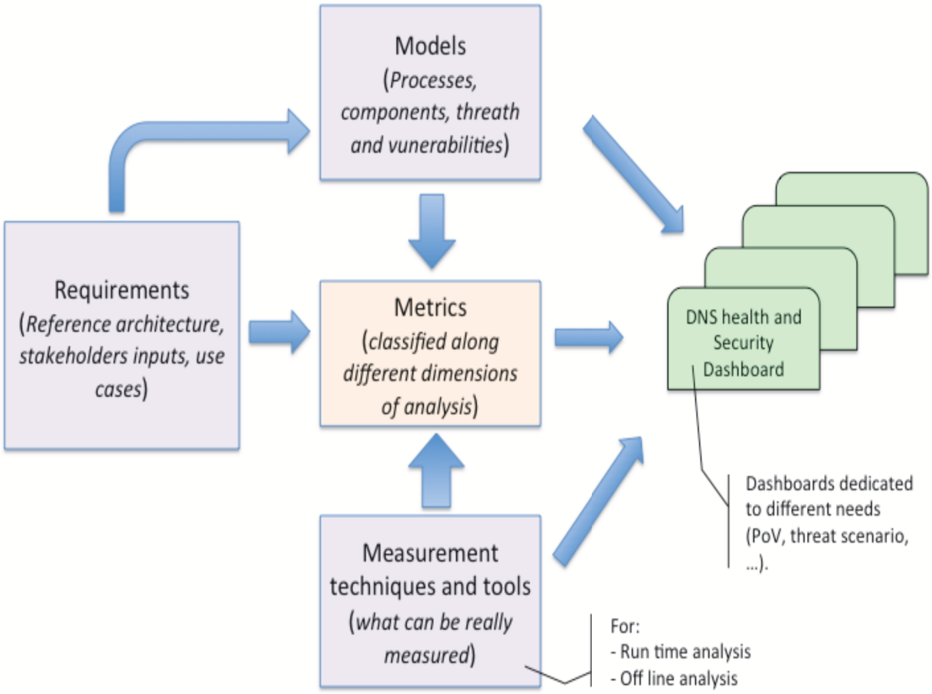
1 *preliminary diagnosis* that, chosen the PoV, performs a first evaluation of the health level perceived conducting simple measurements and assessments

2 the *definition of the service level objectives (SLOs) and scenario* phase, given the PoV, selects one or more threat scenarios and the measurable and representative indexes

3 the *detailed diagnosis and measurement phase* assess: the health level perceived; the achievable SLOs; the causes of SLO violation and improvement actions.

The detailed diagnosis and measurement phase is organised in three stages: selection of metrics, measurement and aggregation.

Figure 4 The framework building blocks (see online version for colours)


Models
(Processes, components, threath and vunerabilities)
Requirements
(Reference architecture, stakeholders inputs, use cases)
Metrics
(classified along different dimensions of analysis)
Measurement techniques and tools
(what can be really measured)
DNS health and Security Dashboard
Dashboards dedicated to different needs (PoV, threat scenario, ...).
For:
- Run time analysis
- Off line analysis

At the *aggregation* stage, all the measures collected are combined to provide aggregated indexes summarising the health level perceived by the PoV, what the achievable SLOs are, and finally what the cause of health degradation could be and possible solutions.

Details about the aggregation process and the results of a first measurement campaign are formally described in Casalicchio et al. (2012).

The presented framework is still embryonic, but apparently, according to the scientific literature, is the only work performed within the DNS community trying to achieve the goal of assessing the health of the DNS.

6 Related works

Security of critical industrial systems is a field of research that only recently has been studied from an ICT point of view. First rigorous works on the topic can be collocated around 2002. For example, Creery and Byres (2007) presented a high level analysis describing some possible threats affecting industrial critical infrastructures. Some following and more detailed works entered in deep on the subject. We point at the work of Chandia et al. (2007) as example. In literature, there are also works specifically focused on industrial communication protocols such as the 'secure DNP3' presented by the DNP3 user group and proposing some authentication mechanisms for certain kind of commands and packets. For completeness, we cite also works belonging to Fovino et al. (2009) and Heo et al. (2007) that present a secure implementation of the Modbus protocol and other similar approaches respectively. Pothamsetty and Franz (2010) (CISCO), released a ModBUS transparent firewall based on Linux Netfilter, however, at the moment it still appears to be in an embryonic stage of development. Specifically on the energy systems' ICT security there are interesting works on the analysis of cyber-vulnerabilities of turbogas power plants (Fovino et al., 2011; Leszczyna et al., 2008) and examples of cyber-attack scenarios aimed at taking the control of the process network of an energy system (Fovino et al., 2010). The arrival of Stuxnet in 2010 definitely raised the public opinion attention on the importance of keeping critical infrastructure secure also from an ICT point of view. An interesting description of this malware, conceived to directly hit the field devices of nuclear power plants, can be found in Falliere (2010). Some reasearch efforts present mathematical methods for modelling and analysing critical infrastructures (Svendsen and Wolthusen, 2007). Some works specifically focus on securing SCADA systems for the energy sector (Alcaraz et al., 2011).

While some works try to analyse the overall security issues and requirements of critical industrial system (Alcaraz et al., 2012), other works focus on specific ICT solutions employed, e.g., Alcaraz and Lopez (2010) analyse the security implications of wireless sensor network in critical systems. Speaking about the DNS it is useful for our purpose to recall works on the main threats affecting the system as Santcroos and Kolkman (2007). In this paper authors identify and describe deeply DNS issues related to data corruption, information exposure and services availability. A protocol level global vulnerability is presented in Kaminsky (2008). This threat regards DNS resource records integrity and shows how is relatively simple to affect this integrity without any mechanism of authentication. DNSSEC (Eastlake, 1997) is an extension of the DNS that wants to overcome this type of problems but there are some challenge regarding its implementation and deployment as well explained in Chandramouli and Rose (2009) and Osterweil and Zhang (2009).

7 Concluding remarks

For decades, considered a totally closed system, the power system is now quickly evolving toward a completely open, heterogeneous, interconnected and distributed model. This Copernican revolution will deeply impact our society, introducing new economic models and new services. The backbone of this model will increasingly be based on ICT networks. In this context, it is evident how the DNS plays more and more a strategic role in maintaining reachability of all nodes of this large, distributed system. In this paper, after describing at high level both the power system and the DNS, we qualitatively showed how a failure of the latter might heavily impact the former at different levels.

This example poses a serious problem: in the modern society, as for the case of energy systems, basically all the critical infrastructures rely in some way on the services provided by the DNS. As per transitivity that means that also DNS must be considered as a critical infrastructure, indeed the most distributed critical infrastructure of the world. For that reason it is necessary to assess and evaluate the SSR of those DNS elements providing services to all the other critical infrastructures. We envision that it would be beneficial to have a broadly adopted, cooperatively achieved model for DNS SSR measurement and benchmarking based on the notion of DNS health.

For that reason in the paper we presented at high level the basic elements of a framework designed ad-hoc with this scope in mind. This framework is intended to support risk analysis, what-if analysis and impact analysis of changes to the DNS infrastructure as well as DNS policy-making. DNS is basically a seamless system, invisible to the majority of the end-users, and for that reason rarely taken in consideration when speaking about cyber-security. With this paper we aimed at raising the attention of the readers on its relevance and on its role in our digital and real life.

References

Alcaraz, C. and Lopez, J. (2010) 'A security analysis for wireless sensor mesh networks in highly critical systems', *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, July, Vol. 40, No. 4, pp.419–428.

Alcaraz, C., Fernandez, G. and Carvajal, F. (2012) 'Security aspects of SCADA and DCS environments', in *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*, Vol. 7130, pp.120–149, Springer-Verlag, Heidelberger.

Alcaraz, C., Lopez, J., Zhou, J. and Roman, R. (2011) 'Secure SCADA framework for the protection of energy control systems', *Concurrency and Computation: Practice and Experience*, Vol. 23, No. 12 pp.1431–1442.

Casalicchio, E., Caselli, M., Coletta, A., Di Blasi, S. and Fovino, I.N. (2012) 'Measuring name system health', in *Proc. of the Sixth IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, Washington DC.

Chandia, R., Gonzalez, J., Kilpatrick, T., Papa, M. and Shenoi, S. (2007) 'Security strategies for SCADA networks', *IFIP International Federation for Information Processing*, Vol. 253, pp.117–131, Springer, Boston.

Chandramouli, R. and Rose, S. (2009) 'Open issues in secure DNS deployment', *Security & Privacy, IEEE*, Vol. 7, pp.29–35.

Creery, A. and Byres, E.J. (2007) 'Industrial cybersecurity for a power system and SCADA networks – be secure', *IEEE Industry Applications Magazine*, July, Vol. 13, No. 4, pp.49–55.

Eastlake, D. (1997) *Domain Name System Security Extensions*, available at http://www.ietf.org/rfc/rfc2065.txt (accessed on 26/07/2012).

Falliere, N. (2010) 'Stuxnet introduces the first known rootkit for industrial control systems', Symantec Web Site.

Fovino, I.N., Carcano, A. and Masera, M. (2009) 'Secure Modbus Protocol, a proof of concept', *Proc. of the 3rd IFIP Int. Conf. on Critical Infrastructure Protection*.

Fovino, I.N., Guidi, L., Masera, M. and Stefanini, A. (2011) 'Cyber security assessment of a power plant', *Electric Power Systems Research*, February, Vol. 81, No. 2, pp.518–526.

Fovino, I.N., Masera, M., Guidi, L. and Carpi, G. (2010) 'An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants', in *IEEE 3rd International Conference on Human System Interaction*, May, pp.679–686, Rzeszow, Poland, IEEE.

GCSEC (2011) 'Measuring the naming system (mensa) project'.

Heo, J., Hong, C.S., Ju, S.H., Lim, Y.H., Lee, B.S. and Hyun, D.H. (2007) 'A security mechanism for automation control in PLC-based networks', in *IEEE International Symposium on Power Line Communications and Its Applications*, pp.466–470, IEEE.

ICANN (2009) 'Security, stability, and resiliency of the domain name system', Technical report.

ICANN (2010) 'Measuring the health of the domain name system', Report of the 2nd Annual Global Symposium on DNS Security, Stability and Resiliency, February.

Kaminsky, D. (2008) *It's the End of the Cache as We Know it*, Black Hat, USA.

Leszczyna, R., Fovino, I.N. and Masera, M. (2008) 'Security evaluation of IT systems underlying critical networked infrastructures', in *1st International Conference on Information Technology*, May, pp.1–4, IEEE.

Osterweil, E. and Zhang, L. (2009) 'Interadministrative challenges in managing DNSKEYs', *IEEE Security & Privacy Magazine*, September, Vol. 7, No. 5, pp.44–51.

Pothamsetty, V. and Franz, M. (2010) 'Transparent Modbus/TCP filtering with Linux', available at http://modbusfw.sourceforge.net/ (accessed on 26/07/2012).

Santcroos, M. and Kolkman, O.M. (2007) 'DNS threat analysis. Technical report', NLnet Labs.

Svendsen, N.K. and Wolthusen, S.D. (2007) 'Analysis and statistical properties of critical infrastructure interdependency multiflow models', in *Information Assurance and Security Workshop, IAW '07*, IEEE SMC, pp.247–254.