The Role of the DNS in the Secure and Resilient Operation of CIs, the Energy System Example

Igor Nai Fovino, Salvatore Di Blasi, and Andrea Rigoni

Global Cyber Security Center (GCSEC),
Viale Europa 175, 00144, Rome, Italy
igor.nai@gmail.com

Abstract. The pervasiveness of Information and Communication Technologies in the control and governance of Critical Infrastructures (CIs) (e.g. power plants, energy grids, oil pipelines etc.) makes the Cyber Security problem a matter of citizen protection and safety. In this work, taking as example the Power System, we analyze the impact of malicious attacks agains the Domain Name System (DNS) on the operation of the modern, open and distributed critical infrastructures.

Keywords: DNS, Security, Power System.

1 Introduction

We define as Critical Infrastructure a system having a strong impact on the daily life of a citizen and that, if damaged, might put in danger the safety and the security of the citizen. Examples of critical industrial infrastructure includes Power Plants, Energy Grids, Gas Pipelines, Chemical Installations etc.

Those infrastructures are increasingly incorporating in a massive way *Information and Communication Technologies* (ICT). This trend obviously allowed to enhance and optimize the services provided, to implement distributed self-orchestration mechanisms, to manage remote installations in efficient manners. As a result, we can state that:

- The ICT infrastructure used to realized these services must be considered now as part of the critical infrastructure by itself.
- Since several of these services take advantage of the public network to operate, also the public network and its core elements have became a critical infrastructure.

In this work we concentrate our attention on the core role of the Domain Name System (i.e. the world wide system allowing to the Internet to operate correctly) in the secure and resilient operation of CIs and on its disrupting effect as a likely target in cyber attack scenarios.

On the light of the coming Energy Smart Grid, a continental critical infrastructure making massive use of networking services, we have taken into consideration as use case the Energy System and after analyzing at high level its functional structure, we magnified the effects of some classes of DNS vulnerabilities on the whole operation capabilities of this system.

S. Bologna et al. (Eds.): CRITIS 2011, LNCS 6983, pp. 152–163, 2013.
© Springer-Verlag Berlin Heidelberg 2013

2 Related Works

The ICT security of critical industrial systems is a relatively new field of research. In this context, Adam and Byres [1] presented an interesting high level analysis of the possible threats affecting industrial critical infrastructures.A more detailed work on this topic is presented by Chandia et al. [2]. Some work has been done about the security of industrial communication protocols: for example the DNP3 User Group proposed a "Secure DNP3" implementing authentication mechanisms for certain type of commands and packets. Pothamsetty and Franz (CISCO), released a ModBUS transparent firewall [4] based on Linux Netfilter, however, at the moment it still appears to be in an embryonic stage of development. With specific reference to the ICT security of energy systems, Nai et al. presented an analysis of the cyber vulnerabilities of turbogas power plants [5][6], and a set of cyber-attack scenarios aimed at taking the control of the process network of an energy system [7]. Finally, in 2010 the case of Stuxnet, a malware conceived to directly hit the field devices of nuclear power plants [8], brought definitively under attention of the public opinion the strict interconnection between the security of ICT devices and the security of critical infrastructures. Regarding the Domain Name System, in [11] the authors draw a comprehensive picture of current threats affecting DNS, identifying on a coarse grained fashion data corruption, availability and information exposure issues. In [12] a serious global vulnerability has been discovered at protocol level, showing how DNS resource records (RRs) integrity can be seriously menaced, not having in place any authenticity check mechanisms; DNSSEC [13] has been introduced as a security extension to the DNS protocol, to provide authentication and integrity to DNS data. Despite of the commitment of the DNS community in gradually adopting DNSSEC, there are some open challenges yet to be addressed from both operational and administrative perspective, as evidenced in [14] and [15].

3 Energy System Overview

The Energy System comprises a huge number of subsystems, with different missions, collaborating to maintain a sort of cross-country balance and to provide energy to hundreds of million of people. In the following we provide an high level description of its most important elements and dynamics.

The physical layer of power systems is represented by the network hardware: stations, lines, transformers and circuit breakers. The control strategies maintaining the transmission system operating are transferred to the physical systems through ICT control and communication centers and devices (cyber layer of the system). From a physical point of view it is possible to categorize the elements constituting the power system in:

- *Transmission Stations*: generally operated directly by the Transmission System Operator (TSO).
- *Power Plants*: usually owned by different companies.

- *Distribution Systems feeders*: these are buses, equipped with transformers, in which a Medium voltage distribution system is originated. Each Distribution System Operator (DSO) owns and operates as a monopolist the distribution system over a certain portion of territory.
- *Large Utilizer*: energy users that demand high power (> 5 MW).
- *End Users*: they are connected to the distributions buses and contitute the leaves of the energy system. With the advent of the modern smart-grid in which each end user can also be an energy producer of course this categorization will change.

To be maintained, such complex system need to exchange a considerable amount of information (real-time data, but also commercial and administrative data) between control centers and substations, and between the different operators.

The cyber-layer of an energy grid is composed of different subsystems:

- *Control Network*: it contains all the Remote Terminal Units (in the following RTU) and Programmable Logic Controllers (in the following PLC). It is directly interfaced with the field network, i.e. the network of actuators and sensors that physically perform the process tasks on the system. Moreover, it is connected with the Process Network described in the following.
- *Process Network*: it is composed of the SCADA servers and all the other systems that gather the data coming from the Control Network and send commands to the Control Network.
- *Exchange Area*: this area usually contains aggregation databases that receive data from the process network. Such data represent the working state of the system and are used by the diagnostic systems also contained this area, to detect anomalies. The operators of the control centers remotely access such databases in order to have a high level view of the process state.
- *Control Centers*: these areas, usually composed of systems that act as remote Human Machine Interfaces (HMI), are used by the operators to obtain information about the process and eventually perform operational sequences to modify the process state.

This view of the system has to be interpreted in a multilayered fashion, where several of these infrastructures owned by different companies, interact in an interleaved manner at different levels.

4 Domain Name System Overview

The Internet is the world's largest computing network. It maintains two namespaces, the IP address system and the Domain Name hierarchy. The Domain Name System (DNS) is in charge of maintaining the Domain Name space and provides the services allowing to map domain names on the correspondent IP addresses. DNS can be considered, at the same time, an Internet critical system, a service, a protocol and information infrastructure.

The DNS infrastructure is composed of entities, geographically and logically organized in a hierarchical shape: the topmost level in the hierarchy is the root domain, represented as a dot (“.”), while the next level is called the top-level domain (TLD). Each TLD, in turn, can have many sub-domains, called second-level or enterprise-level domains.

Each of these entities have authority over a portion of the domain name space: those associated to the root domain are called root operators; the organizations that run name servers related to a TLD are called registries. Country Code TLDs (ccTLDs) are run by registries designated in the respective countries, and gTLDs are run by global registries.

To facilitate this administration process, the DNS defines the concept of ’zone’, which is an administrative building block of the DNS name space, typically used to refer to a domain managed as a single administrative entity (e.g. the root zone, the .com zone).

DNS functions can be mainly summarized in:

- **DNS query/response:** This is the most known and used transaction in DNS. A query originates from a client component, known as stub resolver or resolver, towards either an authoritative or caching name server (the process can be either iterative or recursive). Query/response data are normally sent in plain text thus letting a potential attacker the possibility to intercept and alter response information back to end-users.
- **Zone management:** A zone transfer represents an operation where a secondary slave server refreshes the entire contents of its zone file from the primary master servers. This process enables a secondary name server to keep its zone file in synchronization with its primary name server. A zone transfer process has different security implications because it can expose some more information than a normal query and because it can trigger an increased resource usage of the message for a potential attacker.
- **Dynamic services:** Through this service it is possible to dynamically add/delete a subset of the Resource Records (RRs) for an existing domain, to delete an entire domain or to create new domain.
- **DNS Administration:** This includes all the administrative tasks performed by the responsible entity in order to guarantee an appropriate level of service and assure security.

5 The Role of DNS in Energy System Operations

The previous sections provides an overview of the ICT architecture of the Power System. It is evident how, in a similar infrastructure, a relevant role is played by the ICT networks making the system interconnection possible. Looking at the scientific and operative literature it comes out that in this context, very little attention is paid to the role of the Domain Name System. To understand the deepness of the involvement of the DNS infrastructure in the Power System operation, we have partitioned the system in two views: the “high level infrastructure” and the “low level infrastructure”. For each of these views, we have identified a

set of operation classes. We have then taken into consideration some classes of vulnerabilities traditionally associated with the DNS system: *Repository Corruption, System Corruption, Protocol issues, Denial of Service and Information Exposure.*

On the basis of these classes we have made some high level speculation on the effects of the failure of the DNS on the Energy System.

5.1 DNS and the Power System High Level Infrastructure

We can define as "high level infrastructure" of the Power Framework, the infrastructure used for the so-called high-level operations: *(1) Management of the energy market*, *(2) Links between industrial actors and end users*, *(3) Actions at the customers' premises*, *(3) Links between the power sector and industrial actors*, *(4) Coordination among Power producers*, *(5) Coordination among transmission companies* , *(6) Management of crisis/blackout.*

Each of these functional operations involve in some way the DNS. In the following we provide an overview its role and of the effects of a possible failure.

Management of the Energy Market
It includes the interactions between the industrial actors, brokers, and the wholesale market and market clearinghouse. The aspects of these high level operations are, technologically speaking, very close to the traditional Web Application scenarios. It is then evident how DNS plays a relevant role and how its failure can directly impact the availability and stability of the energy market, possibly causing serious financial damages.

With reference to the four classes of vulnerabilities associated to the DNS here we describe briefly some threat scenarios:

- *Repository Corruption*: a DNS repository corruption (e.g. authoritative or cache database corruption) can be part of some more complex attack aiming at rerouting part of the energy market data flow to fake servers, in order to alter the perception of the market trend. In other scenarios, this might also impact the energy production, for example, if an energy producer buys an energy stock on the market, where this is done through dedicated servers, accessing a fake server as the result of a DNS repository corruption. The effect of these operations might have a country level or, even worst, a continental level repercussion, both economically and socially speaking (if the lack of energy forces grid shutdowns and energy cuts).
- *System Corruption and protocol issues*: the same considerations done in the previous case can be made also in these two cases.
- *Denial of Service*: DNS DoS might cause the unreachability of the Energy Market network infrastructure. The impact of this attack, being immediately evident, would be limited, since for a certain amount of time each actor of the energy market can operate without needing the access to the market services. It is however true that in particular cases (e.g. during unexpected peaks of energy requests or similar situations), the unavailability of the energy market could cause unpredictable damages.

– *Information Exposure*: attacks to the DNS aiming at violating the confidentiality of the infrastructure might be part of more complex attacks (see for example the attacks aiming at corrupting the DNS cache). The immediate damage here is mostly null, but if we consider the "big picture", learning how certain DNS nodes involved in the energy market operation are configured might give a powerful knowledge to potential attackers.

Links between Industrial Actors and End Users

This logical operation refers to all the communication phases between energy companies and end-users including meters, billing energy services interface, aggregators of retail energy providers and energy service providers.

An example where DNS might be used here is in the context of smart meters: there already exist several examples of metering infrastructure composed by a mixture of GPRS technologies and classic TCP/IP channels. Normally the communication is "GPRS Based" from the meter to the local aggregation center and "IP based" from the local aggregation center to the Energy enterprise servers. With regards to the IP part of the data control and acquisition architecture, any attack on the DNS can have impact on services such as: remotely turning power on or off to a certain customer, alter energy usage information, disabling service outages detection, favouring unauthorized use of electricity, alter the maximum amount of electricity that a customer can demand at any time, remotely altering the meter's billing plan. Mobile applications already exist that allow consumers to check home energy consumption remotely; also in this case it is probable that DNS is used to make the service accessible from anywhere. In the same way, billing services, just another example of a web application architecture, make use of DNS, to make the frontend servers and the payment servers accessible to users.

DNS Repository Corruption, DNS System corruption and protocol issues, in this case, as a part of a more complex attack, can be used in several scenarios:

– The DNS cache can be corrupted so that it would be possible, at some point in between meters and aggregation servers, to reroute the traffic to a fake server. At the same way these classes of vulnerabilities can be used in a scenario in which the billing process is involved or, in the case of end-user energy production, it can be used in attacks aiming at altering the end-users production records. The damage here would be mostly economical, but, luckily, it would not impact core installations.
– *Denial of Service*: DNS DOS might interfere in the metering and billing process. Again we can speak mostly of economical damages.
– *Information Exposure*: as in the previous caset, the immediate damage here is mostly null, but if we consider the "big picture", this scenario might surely consist in an intermediate step for other attacks.

Actions at the Customers' Premises

In this context we consider operations such as management of appliances, electric vehicles, other related services (gas/water metering), home automation etc.

These operations fall, technically speaking, in the same class of the previous operations, and for that reason the DNS, depending on the underlying communication architecture, might have a relevant role.

Links between the Power Sector and Industrial Actors
To maintain their core infrastructure (power plant, transmission centers etc.), energy companies are tightly linked with the power device producers. It's quite common for the device producers to provide remote maintenance support. This, normally, is implemented by the establishment of a VPN connection (through the public Internet) from the device producer home site to the power company installation sub-network, allowing remote operation of the local process control system. In this case, DNS is involved in the resolution of the names of the servers involved, and any unavailability, corruption or disruption might prevent a required maintenance operation on the physical installation. When a site-to-site VPN tunnel is established, the name resolution process of internal name servers is achieved through the two DNS systems acting at both sites: misconfigurations, internal corruption or availability issues on either the producer or the energy company site affect inevitably the whole system security, with the consequence that operations flow can be redirected to bogus servers or can be prevented at all. It is also important to understand how DNS can play the twofold role of infection dozer (e.g. by transparently redirecting users request to fake sites and consequently triggering a silent installation of malicious code which will then produce the real damages, when in action) and infection actuator (for example by directly impacting the availability of the company installation sub-network services).

Coordination among Power Entities
In this category we consider:

- The coordination among power companies, mainly related to the amount of energy to be produced, which is increasingly making use of the Internet infrastructure. The impact of DNS on these operations might be then considered high over these information exchange services, as for example power companies might not be able to communicate properly energy production plan details to each other.
- The Coordination among transmission companies: the same considerations of the previous point are valid here.
- Management of crisis/blackout: traditionally the coordination among energy actors during crisis (e.g. during a blackout) is well structured and defined by a set of operational policies. The use of the public network, mailing systems and other applications to coordinate the actions during an energy crisis are increasing. Also in this case, DNS might be involved. In this case the impact of DNS repository corruption, System Corruption and DoS is potentially heavy. A delay in the coordination of a blackout emergency can lead to dramatic situations where entire countries are left without energy. This can be considered, at this level, the most sensible operation in term of impact on the citizen life.

High Level Layer Impact Conclusions
Essentially, all of these high level power infrastructure operations rely on web-services/applications making use of Internet to exchange information, perform transactions, and provide services. In all these cases, the DNS plays a relevant role. A failure or a corruption of the DNS might have a dramatic impact, for example affecting pricing or availability in the energy market. Similarly, if during the management of an energy crisis (e.g. blackout risks) the DNS fails, this might impact the high level control centers collecting field data, and indirectly slow down the definition of a proper contingency plan. The coordination among power producers is necessary to guarantee the stability of the energy grid. A failure of the DNS could impair this process.

5.2 DNS and the Power System Low Level Infrastructure

In the early '90s, the Power control system 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. With the increasing use of TCP/IP, process engineers decided to port all the serial industrial protocols to TCP/IP (usually embedding these 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 [1]) 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.

Here some examples of common operational activities in which the DNS might be involved and some speculations on the effects of a DNS failure on these activities.

Maintenance Operations
Power plants, transmission substations, and other power system elements require constant maintenance. These activities are typically outsourced to external companies. These companies perform several of the maintenance operations 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.

To resolve the addresses of the different servers involved in the process both internal and external DNS at both sites are normally used. A failure of the DNS during these operations, might impact the safety and stability of the power system. Repository Corruption and protocol issues (allowing for example to perform a DNS cache poisoning) can be used as part of complex attacks aiming at rerouting the maintenance flow between the device producers site and the local plant

network site. DNS DoS can be used to make harder to establish a connection between the remote site and one of the server on which perform the maintenance operations.

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 the two cases the impact of 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.

Process Network Interactions
The process network contains all the servers controlling the industrial processes (e.g. energy production, energy transmission etc.). It is quite common to rely on an internal DNS for the resolution of the server names. In this case, a failure of the DNS might impact the detection of anomalies in the process network of the power system or on the control capabilities of the SCADA servers. 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 (a very expensive mistake given an average power plant costs around 2 million euros per day). In the second case, losing the control capabilities of the SCADA servers could make it impossible to react sufficiently rapidly to a change in system critical state.

Operator Monitoring
Human operators use the HMI to monitor the activities of the process system. To perform this activity, they often access the history servers contained in the exchange network. More rarely, they directly access the SCADA servers; finally, the trend of accessing servers and services using names instead of IP addresses is increasing. 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. In[7] Nai et al. 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.

Control Center Operations
Control centers manage simultaneously multiple installations of the Power System. The different applications hosted in the control centers generate query/response flows from the local HMIs to the remote RT-Databases of the installations and to the diagnostic servers. DNS is again used to resolve the name of the entry

points of the different remote subnets, and to resolve the names of the remote servers. Another important function of control centers 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 nameserver 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 nameserver, 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.

6 The DNS Health Measurement Framework

This use case demonstrates the need to develop and standardize metrics for what Security, Stability and Resiliency (SSR) of the DNS actually means. 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. The outcomes of the analysis of the SSR data would allow operators improve the understanding of the security level of their DNS infrastructure; moreover, a configurable and modular framework supporting "what-if" and impact analysis of DNS re-engineering and DNS policy making would again make easier to understand their potential effects on the power system.

In the context presented in the previous section, the efforts of Internet Corporation for Assigned Names and Numbers (ICANN) provided a highly useful foundation for further studies on the Security, Stability and Resiliency (SSR) of the DNS. The results of the ICANN DNS SSR symposium 2010[10] introduced the concept of "DNS Health" that includes the concept of DNS SSR.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. The open points and unanswered questions we identify after a reasoned analysis of the report [10] are related to:

1. The need of viable indicators of DNS health and security for the different DNS actors (Root server operators, Operators of non-root authoritative name servers, recursive caches, open DNS resolver,end users);
2. The need to understand and refine proper methods and techniques for the measurement of DNS health and security indicators;
3. The need to refine and improve existing metrics (and measurement approaches) for coherency, integrity, speed, availability, resiliency, vulnerability and security;
4. The need for metric threshold levels that allow the DNS community to know, possibly in advance, when DNS health and/or security are being compromised.

Answer to these open questions is mandatory to define a global and coherent action to enforce at every level the security of the DNS providing at the same time to the critical end users the tools for evaluating their exposure to DNS threats.

7 Conclusion

For decades, considered a totally closed system, the powes 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. For that reason it will soon be necessary to assess and evaluate the security, stability and resiliency of those DNS elements providing services to this system. We envisions that it would be beneficial for all the actors of critical infrastructures impacted by the DNS, to have a broadly adopted, cooperatively achieved model for DNS Security, Stability and Resiliency (SSR) measurement and benchmarking based on the notion of DNS health. On the basis of the outcomes of this work, we are planning to design a layered and multi-perspective framework for the measurement and benchmarking of the DNS SSR level. 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. The goal of this work will be to refine the current concept of DNS SSR and to enhance the awareness among the "critical" end-users of the DNS and among the private DNS operators.

References

1. Creery, A.A., Byres, E.J.: Industrial Cybersecurity for power system and SCADA networks IEEE Industry Application Magazine (July-August 2007)
2. Chandia, R., Gonzalez, J., Kilpatrick, T., Papa, M., Shenoi, S.: Security Strategies for SCADA Networks. In: Goetz, E., Shenoi, S. (eds.) Critical Infrastructure Protection. IFIP, vol. 253, pp. 117–131. Springer, Boston (2008)

3. Nai Fovino, I., Carcano, A., Masera, M., Trombetta, A.: An experimental investigation of malware attacks on SCADA systems. International Journal of Critical Infrastructure Protection 2(4) (2009)
4. http://modbusfw.sourceforge.net/ (last access May 28, 2010)
5. Nai Fovino, I., Masera, M., Guidi, L., Stefanini, A.: Cyber Security Assessment of a Power Plant. International Journal of Electric Power System Research 81(2), 518–526
6. Leszczyna, R., Nai Fovino, I., Masera, M.: Security Evaluation of IT Systems Underlying Critical Networked Infrastructures. In: Proceeding of the 1st International Conference on Information Technology, Gdansk, Poland, May 18-21 (2008)
7. Nai Fovino, I., Masera, M., Guidi, L., Carpi, G.: An Experimental Platform for Assessing SCADA Vulnerabilities and Countermeasures in Power Plants. In: Proceedings of the IEEE 3rd International Conference on Human System Interaction, Rzeszow, Poland, May 13-15 (2010)
8. http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (last access: May 14, 2011)
9. Nai Fovino, I., Masera, M., Leszczyna, R.: ICT Security Assessment of a Power Plant, a Case Study. In: Proceeding of the Second Int. Conference on Critical Infrastructure Protection, Arlington, USA (March 2008)
10. Measuring the health of the Domain Name System, Report of the 2nd Annual Symposium on DNS Security, Stability, & Resiliency, Kyoto, Japan (February, April 2010), https://www.icann.org/en/topics/ssr/dns-ssr-symposium-report-1-3feb10-en.pdf
11. Santcroos, M., Kolkman, O.: DNS Threat Analysis, NLnet Labs (May 2007)
12. Kaminsky, D.: It's the end of the cache as we know it. Blackhat, USA 2008 (August 2008), http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf
13. IETF RFC 2535 "Domain Name System Security Extensions", http://tools.ietf.org/html/rfc2535
14. Chandramouli, R., Rose, S.: Open issues in Secure DNS Deployment. US National Institute of Standards and Technology (NIST)
15. Osterweil, E., Zhang, L.: Interadministrative challenges in managing DNSKEYs. IEEE Security and Privacy: Securing the Domain Name System (September 2009)