OARC 2014 Fall Workshop (Los Angeles)

DNS-OARC
Domain Name System Operations Analysis and Research Center

Report of Contributions

https://indico.dns-oarc.net/e/workshop-2014-10

Contribution ID : **0** Type : **not specified**

Improved NSEC3 performance in DNSSEC

Sunday, 12 October 2014 12:00 (30)

A challenge in DNSSEC is that the 'NSEC3' records used to assert the non-existence of a given domain name can create a significant computational load on the DNS servers. This document describes an application of a cryptographic technique known as a 'time-lock puzzle' to the calculation of NSEC3 records. This provides a means of reducing this load whilst simultaneously increasing the security against DNS record enumeration offered by NSEC3.

Summary

This presentation shows how a 'computationally asymmetric cryptographic hash function' can be constructed from a cryptographic technique known as a time-lock puzzle (http://people.csail.mit.edu/rivest/lcs35-puzzle-description.txt)

We show how such a hash function may be useful in the context of NSEC3 records, by enabling the computational load faced by an attacker to enumerate a zone to be increased without creating a parallel increase in computational load on the DNS server to generate such records or process queries.

Primary author(s) : Dr. TULIANI, Jonathan Tuliani (Microsoft)

Presenter(s) : Dr. TULIANI, Jonathan Tuliani (Microsoft)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **1** Type : **not specified**

Measuring the cost of DNSSEC

Sunday, 12 October 2014 11:00 (30)

The presentation provides some measurements on the incremental cost of signing a domain name. It looks at the profile of additional time taken to resolve a signed name by a dnssec-validating resolver and from the perspective of the authoritative name server quantifies the additional query and traffic load when serving a signed zone as distinct from an unsigned zone. The presentation also extrapolates this load to the situation when all resolvers perform DNSSEC-validation

Summary

Primary author(s) : Mr. HUSTON, Geoff (APNIC)

Presenter(s) : Mr. HUSTON, Geoff (APNIC)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **2** Type : **not specified**

2014 Root DITL Data analysis and TLD popularity analysis

Sunday, 12 October 2014 10:20 (20)

The presentation reports statistics of 2014 DITL root dataset and differences from previous data.
And tries to show popularities of each TLD.
The data may show the share of usage of TLDs in each country.

Summary

Primary author(s) : Mr. FUJIWARA, Kazunori (Japan Registry Services Co., Ltd)

Presenter(s) : Mr. FUJIWARA, Kazunori (Japan Registry Services Co., Ltd)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **5** Type : **not specified**

DNS - the glue in the IoT

Sunday, 12 October 2014 16:00 (30)

In Internet of Things (IoT), the "Things" could be anything from refrigerators to human to books. These "things" should be identified at least by one unique way of identification, for the capability of addressing and communicating with each other. This is made possible by attaching/embedding different data carrier devices such as barcodes,RFID, Sensors etc with the 'things'.

Sensors, for example could be identified by MAC or IPv6 address. Similarly barcodes, RFID tags are encoded with an identifier based on different identification schemes such as Universal Product Code, (UPC), Electronic Product Code (EPC), ucode etc. The basic feature of these identifiers are : they are allocated hierarchically, control is decentralised and the nature of allocation makes sure that there is no duplicity.

The identifier properties described in the previous paragraph are similar to the domain name allocation and management, and thus, identifiers in IoT could leverage the DNS infrastructure and software for allocation and resolution. Leveraging DNS for other uses started with ENUM for telephone numbers, and for IoT, there exists already overlay mechanisms services such as Object Naming Service (ONS) [EPCglobal standard] and Object Directory Service (ODS) [ITU-T standard] which uses the DNS to resolve the IoT identifiers (their respective identification schemes) to its related digital information.

As DNS acts as a "glue" in the current Internet, where its basic feature is to resolve "human-friendly" host names to their corresponding "machine-friendly" IP addresses, in IoT also it is proved, that DNS could be a glue for certain identification schemes.

This talk will concentrate on

[1] How DNS could be leveraged for resolving a 'thing' associated with an RFID based on our experiences in working on the WINGS [WINGS] project and contributing to the ONS 2.0 standard [EPCglobal standard]
[2] The issues involved in using DNS for resolution in the Wireless sensor network (i.e using Sensor devices) based on a recently started collaborative project [WSNProject].
[3] If time permits, IoT standardisation activities at the IETF relating to DNS

[WINGS] http://www.wings-project.fr/
[EPCglobal standard] http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_2_0_1-standard-20130131.pdf
[ITU-T standard] Object Directory Service for Mobile AIDC services (ISO/IEC 29177)
[WSNProject] http://www.labfab.fr/portfolio/lora-fabian/

Summary

Primary author(s) : Mr. BALAKRICHENAN, Sandoche (Afnic)

Presenter(s) : Mr. BALAKRICHENAN, Sandoche (Afnic)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **6** Type : **not specified**

Orient data vertically for faster analysis

Sunday, 12 October 2014 16:30 (30)

Column store databases are a newer entry to the big data realm. They handle structured data like DNS queries exceptionally well and work best with minimal data normalization. Queries execute significantly faster than RDBMS technology (~ 100 times faster).
This talk will outline the technology at a high level and walk through examples of data loading, compression, and reporting using a freely available Column Store DB as well as Nominum's experiences and findings analyzing large amounts of DNS data.

No normalization, fast data loading, no indexing, fast queries and SQL… what's not to like?

Summary

Primary author(s) : Mr. BEAUDIN, Adrian (Nominum)

Presenter(s) : Mr. BEAUDIN, Adrian (Nominum)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **9** Type : **not specified**

The GIft that Keeps on Giving: Open DNS Proxies

Sunday, 12 October 2014 15:30 (30)

DNS DDoS attacks continue, fueled by open DNS proxies. Now they're stressing resolvers and authorities worldwide using pseudo random subdomains. In June of 2014 there was a 400% increase in this traffic and popular domains continue to be targeted. Analysis of recent DNS data reveals other interesting details. For instance, Response Rate Limiting in authorities appears to aggravate attacks.
This presentation will cover the latest attack data as well as tests of the major resolvers showing the impact of capabilities to mitigate them, ranging from changes in recursive behaviors to filtering traffic at ingress.

Summary

Primary author(s) : Mr. WEBER, Ralf (Nominum)

Presenter(s) : Mr. WEBER, Ralf (Nominum)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **10** Type : **not specified**

Reputation Metrics Design to Improve Intermediary Incentives for Security of TLDs

Sunday, 12 October 2014 13:30 (30)

In this presentation, we describe security metrics for Top-Level Domains (TLDs) and we measure their operational values using DNS query data and other data sources such as botnet and phishing feeds. They can serve as publicly available signals to different classes intermediaries such as registries, registrars, or hosting providers and can offer the option to benchmark themselves against their market. There currently exists very little empirical information about the security performance of TLDs and of the overall DNS ecosystem.

We distinguish three types of security metrics, each at a different layer of ab- straction. The top-layer involves the security metrics of an entire TLD such as .nl, .com, or .amsterdam. The second layer of abstraction consists of security metrics for market players under TLDs. These are Internet infrastructure providers, registries, registrars, and hosting providers. Examples of security metrics at this layer include concentration of malicious domains across players and their up-times. The third layer is a break-down of the second layer and involves security metrics for network resources managed by each of the players, such as DNS resolvers, or authoritative name servers. In this presentation, we pay a special attention to the second layer and we develop reputation metrics for registries, registrars, and hosting providers with the respect to the TLD layer.

In our future work, we plan to correlate the abuse rate reflected in the here-proposed reputation metrics with registry policy, such as pricing, the correctness of the whois data, security monitoring of the DNS infrastructure, etc.

Summary

Primary author(s) : Dr. KORCZYNSKI, Maciej (Delft University of Technology)

Co-author(s) : Mr. WULLINK, Maarten (SIDN); Prof. VAN EETEN, Michel (Delft University of Technology)

Presenter(s) : Dr. KORCZYNSKI, Maciej (Delft University of Technology)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **11** Type : **not specified**

DNS Rex: Do you need an aggressive benchmarking tool?

Monday, 13 October 2014 15:00 (20)

DNS Rex: Do you need an aggressive benchmarking tool?

I would like to present DNS Rex, an open source performance benchmark for DNS servers, with a focus on busy DNS caching resolvers. DNS Rex was created to address several known (and rumored) problems with existing DNS testing tools. Our goals included:

- reliable generation of high query rates,
- reproducibility of test results,
- ability to sustain any configurable cache hit ratio,
- support for long tests without reliance on trace replay,
- independence from a 3rd-party authoritative server,
- DNSSEC support.

DNS Rex has been successfully used for private tests, and is publicly available[1], but we have not promoted its wider use. Besides describing what DNS Rex can do today, I would like to gauge audience interest in continued development of the tool. Is there a genuine need for a better DNS benchmark? What missing features are the most important?

[1] http://rex.measurement-factory.com/

Summary

A presentation about DNS Rex, a performance testing tool for busy DNS caching resolvers. Why was it created? What can it do? Where do we go from here?

Primary author(s) : ROUSSKOV, Alex (The Measurement Factory)

Presenter(s) : ROUSSKOV, Alex (The Measurement Factory)

Session Classification : Monday Joint OARC/Tech Day

Track Classification : Joint OARC/Tech Day

Contribution ID : **12** Type : **not specified**

Preserving case-sensitivity in zone names

Sunday, 12 October 2014 14:20 (20)

In early 2014 a BIND user encountered a problem with some SIP phones, that turned out to be due to the fact that, while compressing zone updates, we were not preserving case-sensitivity. We determined that CamelCasing is allowed, and thus case should be preserved by IETF specification. We then consulted with a number of operating system publishers and agreed on a solution. This brief presentation will explain how BIND handles this situation and introduce others to the issue.

Summary

Primary author(s) : HUNT, Evan (ISC)

Co-author(s) : RISK, victoria (isc)

Presenter(s) : RISK, victoria (isc)

Session Classification : Sunday Workshop (Public)

Track Classification : Lightning Presentations

Contribution ID : **13** Type : **not specified**

A Survey of Current DANE/TLSA Deployment

Sunday, 12 October 2014 14:00 (20)

As adoption of DNS Security Extensions (DNSSEC) grows, DNS-based Authentication of Named Entities (DANE) provides an alternative to traditional CA-based certificate authentication. The DANE TLSA protocol specification was published in 2012. It's generally unknown to the DNS community how widely DANE TLSA has been deployed and how TLSA records are used. In this talk, we present a survey of current deployment of DANE TLSA. We developed PryDane, a tool for actively probing names possibly having TLSA records validating those records with the server certificates. Based on the data we collected, we conclude that DANE TLSA is not widely deployed at this time. Our probing data shows the most common (>80%) usage of TLSA record is: domain-issued cert matching full cert with SHA-256. Our validation results show there are consistently about 7%-10% of DANE-enabled names having invalid TLSA records. We explored the reasons for these mismatches, such as wrong certs and incorrect parameters in TLSA records.

Summary

Primary author(s) : ZHU, Liang (USC/Information Sciences Institute)

Co-author(s) : WESSELS, Duane (Verisign)

Presenter(s) : ZHU, Liang (USC/Information Sciences Institute)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **14** Type : **not specified**

NSEC5: Provably Preventing DNSSEC Zone Enumeration

Sunday, 12 October 2014 14:40 (30)

DNSSEC is designed to prevent network attackers from tampering with domain name system (DNS) messages. The cryptographic machinery used in DNSSEC, however, also creates a new vulnerability–zone enumeration, where an adversary launches a small number of online DNSSEC queries and then uses offline dictionary attacks to learn which domain names are present or absent in a DNS zone.

We propose a new cryptographic construction that solves the problem of DNSSEC zone enumeration while remaining faithful to the operational realities of DNSSEC. NSEC5 can be thought of as a variant of NSEC3 in which the unkeyed hash function is replaced with a deterministic RSA-based keyed hashing scheme.

We also show that a public-key operation is necessary to prevent zone enumeration. Specifically, we prove that security against network attackers and privacy against zone enumeration cannot be satisfied simultaneously unless the DNSSEC server performs online public-key cryptographic operations.

Summary

See attached file.

Primary author(s) : Prof. GOLDBERG, Sharon (Boston University)

Co-author(s) : Mr. ZIV, Asaf (Weizmann Institute); Mr. PAPADOPOULOS, Dimitrios (Boston University); Dr. REYZIN, Leonid (Boston University); Dr. NAOR, Moni (Weizmann Institute); Mr. VASANT, Sachin (Boston University)

Presenter(s) : Prof. GOLDBERG, Sharon (Boston University)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **15** Type : **not specified**

Analysis of TCP traffic in DITL data

Sunday, 12 October 2014 09:00 (30)

The historical archive of DITL data is analyzed for trends in TCP traffic, answering some of the following questions: are TCP sources representative of UDP sources? Does TCP always follow a UDP TC=1 response? Do TCP and UDP sources have similar query type distributions? Are response sizes increasing over time, leading to more TCP? What do TCP connections indicate regarding latency?

Summary

Primary author(s) : WESSELS, Duane (Verisign)

Co-author(s) : THOMAS, Matthew (Verisign)

Presenter(s) : WESSELS, Duane (Verisign)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **16** Type : **not specified**

DNSViz - powerful and extensible DNS analysis

Monday, 13 October 2014 11:30 (20)

DNSViz has been developed as a Web-based tool for analysis, visualization, education, and troubleshooting DNS and DNSSEC. The tool has recently been reworked for extensibility and portability, including a downloadable library and tool suite available via an open source license–and a revamped Web site. We discuss the new features available with DNSViz, future plans, and how to get involved.

Summary

Primary author(s) : Dr. DECCIO, Casey (Verisign Labs)

Presenter(s) : Dr. DECCIO, Casey (Verisign Labs)

Session Classification : Monday Joint OARC/Tech Day

Track Classification : Joint OARC/Tech Day

Contribution ID : **17** Type : **not specified**

Measuring the Leakage of Onion at the DNS Root

Monday, 13 October 2014 12:10 (20)

The Tor project provides individuals with a mechanism of communicating anonymously on the Internet. Furthermore, Tor is capable of providing anonymity to servers, which are configured to receive inbound connections only through Tor (more commonly called hidden services). In order to route requests to these hidden services, a namespace is used to identify the resolution requests to such services. A namespace under a non-delegated (pseudo) top-level-domain (TLD) of .onion was elected. Although the Tor system was designed to prevent .onion requests from leaking into the global DNS resolution process, numerous requests are still observed in the global DNS.

In this talk I propose to present the state of .onion requests received at the global public DNS A and J root nodes, and a complementary measurement from the DITL (day in the life of the Internet) data repository. I will also present potential explanations of the leakage, and highlights of trends associated with global censorship events.

Summary

Primary author(s) : Dr. MOHAISEN, Aziz (Verisign Labs)

Co-author(s) : THOMAS, Matthew (Verisign)

Presenter(s) : Dr. MOHAISEN, Aziz (Verisign Labs)

Session Classification : Monday Joint OARC/Tech Day

Track Classification : Joint OARC/Tech Day

Contribution ID : **20** Type : **not specified**

A country level Analysis of the OARC DITL root traces 2009-2014

Sunday, 12 October 2014 10:00 (20)

I would like to present an analysis of a country level breakdown of the DNS traffic captured by the OARC members on the DITL traces between 2009 and 2014.

Summary

Primary author(s) : HUFFAKER, Bradley (CAIDA/UCSD)

Presenter(s) : HUFFAKER, Bradley (CAIDA/UCSD)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **22** Type : **not specified**

Low-Cost Threshold Cryptography HSM for OpenDNSSEC

Monday, 13 October 2014 11:50 (20)

The DNS Security Extensions (DNSSEC) add a new layer of security based on public-key infrastructure: each DNS record is digitally signed to verify the authenticity of the answer. However, the introduction of DNSSEC has an impact in the operational workflow of DNS systems: (i) signatures have an expiration date, hence the records must be periodically signed and (ii) key management tasks can be overwhelming. These are problems specially for DNS zones with several records (for instance a Top Level Domain).
The adoption of Hardware Security Module (HSM) is an option to provide highly secured keys and signature management. Nevertheless HSM is expensive and hardware can fail. We present a novel system based on threshold cryptography to support the operational signing workflow of DNSSEC. This approach significantly improves security and availability of the overall system since the secret key is never stored in a single place; it is spread among the nodes of the
system.

Summary

Primary author(s) : Mr. CIFUENTES, Francisco (NIC Chile Research Labs)

Presenter(s) : Mr. CIFUENTES, Francisco (NIC Chile Research Labs)

Session Classification : Monday Joint OARC/Tech Day

Track Classification : Joint OARC/Tech Day

Contribution ID : **23** Type : **not specified**

DNS Name Collision Risk Mitigation

Sunday, 12 October 2014 09:30 (30)

Starting August 2014, new gTLDs have been required to insert certain records in their DNS zone to manage name collision risks. This presentation provides a description of the mitigation measures and operational experiences regarding the management of risks related to name collisions in the DNS associated with the introduction of new TLDs.

Summary

Primary author(s) : ARIAS, Francisco (ICANN)

Presenter(s) : ARIAS, Francisco (ICANN)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **26** Type : **not specified**

Test cases for domain checks – a step towards a best practice

Sunday, 12 October 2014 17:00 (20)

Zonemaster is an upcoming tool for controlling DNS zones. It is designed to replace the .SE DNSCheck and the .FR ZoneCheck with better performance, modularity and scalability. One of the design goals is to have explicit test cases for the tool. I.e. exactly what are the requirements of the tested zone that tools should test? What outcomes should return pass and what outcomes should return fail? Those explicit specifications, i.e. the test cases, will at the same time be the ground the validation of the tool.

The goal of the test cases is more than being the requirements for Zonemaster, our ambition is to develop a best practice for zone delegations by having transparent and publically available specifications that are independent of the test tool. The Zonemaster test tool could be seen as one implementation of those specifications.

The test cases should not only capture a completely valid delegation, but they should also be ground for meaningful error messages when things are more or less bad.

I will in my presentation present the major test cases for the tool and some test cases where the outcome need considerations and where discussions and suggestions could help the development.

The material for the project is publicly available at Github, https://github.com/dotse/zonemaster

Summary

Primary author(s) : DUFBERG, Mats (.SE (The Internet Infrastructure Foundation))

Co-author(s) : Mr. BALAKRICHENAN, Sandoche (Afnic)

Presenter(s) : DUFBERG, Mats (.SE (The Internet Infrastructure Foundation))

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **27** Type : **not specified**

OARC's Technical Report

Sunday, 12 October 2014 11:30 (30)

Report from William Sotomayor about the work being done by OARC Technical team since last workshop.

Summary

Primary author(s) : Mr. SOTOMAYOR, William (DNS-OARC)

Co-author(s) : Mr. MITCHELL, Keith (DNS-OARC)

Presenter(s) : Mr. SOTOMAYOR, William (DNS-OARC)

Session Classification : Sunday Workshop (Public)

Track Classification : Public Workshop

Contribution ID : **28** Type : **not specified**

TechDay Opening Remarks

Monday, 13 October 2014 10:30 (10)

Summary

Presenter(s) : Dr. LISSE, Eberhard Wolfgang (Namibian Network Information Centre)

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **29** Type : **not specified**

Introduction from OARC Chairman

Saturday, 11 October 2014 14:00 (15)

Summary

Presenter(s) : Mr. FILIP, Ondrej (CZ.NIC)

Session Classification : Saturday Members-only/AGM

Contribution ID : **30** Type : **not specified**

OARC President's Report

Saturday, 11 October 2014 14:15 (30)

Summary

Presenter(s) : Mr. MITCHELL, Keith (DNS-OARC)

Session Classification : Saturday Members-only/AGM

Contribution ID : **31** Type : **not specified**

OARC Treasurer's Report

Saturday, 11 October 2014 14:45 (15)

Summary

Primary author(s) : POUNSETT, Matthew (Rightside)

Presenter(s) : POUNSETT, Matthew (Rightside)

Session Classification : Saturday Members-only/AGM

Contribution ID : **32** Type : **not specified**

Revised OARC Participation Agreement

Saturday, 11 October 2014 15:30 (45)

Summary

Session Classification : Saturday Members-only/AGM

Contribution ID : **33** Type : **not specified**

OARC Board Elections

Saturday, 11 October 2014 16:15 (45)

Summary

Session Classification : Saturday Members-only/AGM

Contribution ID : **34** Type : **not specified**

IDNA 2008 & Unicode

Monday, 13 October 2014 12:50 (20)

Summary

Presenter(s) : FALTSTROM, Patrick

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **35** Type : **not specified**

Keynote Address

Monday, 13 October 2014 11:00 (30)

Summary

Presenter(s) : MOCKAPETRIS, Paul

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **36** Type : **not specified**

PKI News

Monday, 13 October 2014 17:00 (20)

Summary

Presenter(s) : ROWLEY, Jeremy (Digicert)

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **37** Type : **not specified**

Disturbance in the DNS

Monday, 13 October 2014 10:40 (20)

Summary

Primary author(s) : Mr. BALAKRICHENAN, Sandoche (Afnic)

Presenter(s) : Mr. BALAKRICHENAN, Sandoche (Afnic)

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **38** Type : **not specified**

Facebook CSIO Update

Monday, 13 October 2014 14:20 (20)

Summary

Primary author(s) : SULLIVAN

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **39** Type : **not specified**

MS DNS Server Data Mine

Monday, 13 October 2014 14:00 (20)

Summary

Presenter(s) : Mr. ASHUTOSH, Kumar (Microsoft)

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **40** Type : **not specified**

DNS Bake-off

Monday, 13 October 2014 15:20 (100)

Summary

Presenter(s) : LATOUR, Jacques (CIRA)

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **41** Type : **not specified**

Yahoo CSIO Update

Monday, 13 October 2014 14:40 (20)

Summary

Presenter(s) : STAMOS, Alex (Yahoo)

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **42** Type : **not specified**

Closing Remarks

Monday, 13 October 2014 17:20 (10)

Summary

Presenter(s) : Mr. FILIP, Ondrej (CZ.NIC)

Session Classification : Monday Joint OARC/Tech Day

Contribution ID : **43** Type : **not specified**

PGP Signing Session

Sunday, 12 October 2014 13:00 (30)

Summary

Primary author(s) : POUNSETT, Matthew (Rightside)

Presenter(s) : POUNSETT, Matthew (Rightside)

Session Classification : Sunday Workshop (Public)

Contribution ID : **44** Type : **not specified**

Bumblebee Demonstration

Saturday, 11 October 2014 17:15 (30)

This demonstration-based talk will cover various results of Nominet's analytics efforts over the last four years.

The talk will discuss various incidents, misconfigurations, bugs, attacks and malware behaviour we have uncovered by visualizing and interacting with DNS data. I'll go through a few stories:

1) The limitations we had using existing tools, and the requirements we had when building our analytics tool.
2) How we found CVE-2011-2464 (BIND bug) by understanding how a secondary nameserver should behave, and subsequently looking for abnormalities.
3) How we spot suspicious behaviour and subsequently track a botnet.
4) How we spot abnormal behaviour and subsequently track crypto locker.
5) How two bugs in different implementations amplify eachother. A story about Google and BIND.
6) The effect of RRL during an attack.
7) How OpenDNS improved on their shutter time.
8) The importance of interaction *and* visualisation (and as a natural consequence, timeliness).

Summary

Presenter(s) : ARENDS, Roy (Nominet)

Session Classification : Saturday Members-only/AGM

Contribution ID : **45** Type : **not specified**

SECIR Trust Platform Support

Saturday, 11 October 2014 17:00 (15)

Summary

Presenter(s) : LATOUR, Jacques (CIRA)

Session Classification : Saturday Members-only/AGM

Contribution ID : **46** Type : **not specified**

Host Presentation

Monday, 13 October 2014 12:30 (20)

Summary

Presenter(s) : Mr. PETER, Marx (Los Angeles City Council)

Session Classification : Monday Joint OARC/Tech Day

Track Classification : Joint OARC/Tech Day