RIPE Network Coordination Centre

193.0.0.135 2001:610:240:0:193::202 193.0.0.135

Member Update

September 2005

Information bulletin for the members of the RIPE NCC

www.ripe.net

The RIPE NCC Member Update is intended for LIR contacts.

If you are not the right person to receive this update, please forward it to the appropriate colleague.

How to contact the RIPE NCC:

Postal Address:
RIPE NCC
P.O. Box 10096
1001 EB Amsterdam
The Netherlands

Phone: +31 20 535 4444
Fax: +31 20 535 4445

General Queries
<ncc@ripe.net>

Registration Services
<hostmaster@ripe.net>
<lir-help@ripe.net>

Training Courses
<training@ripe.net>

Become a Member
<new-lir@ripe.net>

Billing Department
<billing@ripe.net>

Whois Database
<ripe-dbm@ripe.net>

RIPE Meeting
<meeting@ripe.net>

Feedback
<feedback@ripe.net>

This publication is available online at:
http://www.ripe.net/membership/newsletter/

On the Report from the Working Group on Internet Governance

By Raúl Echeberría
Executive Director/CEO, LACNIC

The Working Group on Internet Governance (WGIG) has completed its task. Its final report was presented in Geneva on Monday, July 18, 2005. The first conclusion that can be extracted from this process is that the existence of the group itself is of the utmost importance. It has been an unprecedented experience which, in my opinion, establishes a point of no return in terms of the evolution of multi-stakeholder models based on the participation of all interested parties.

The existence within the framework of the UN of discussion processes of this nature, with open working methodologies, organization of public consultation meetings, calls for comments through the Internet, publishing of meetings' scripts and even webcasting represents a historical landmark that will set the foundations for future work not only in the fields of Internet or Information Society, but also for discussion processes in other areas, for which it will surely be an extremely important precedent.

Another important aspect that must be considered is that the WGIG process has made available clearer information about how the existing governance systems work in relation to the different components of Internet, and it has enabled the participation of a larger number of people and organizations, and also the involvement of more governments in the debate.

From this point of view, the situation is much improved as compared to the situation that existed before the WGIG began working. As to the results obtained by the working group, there are some highly relevant conclusions which are highlighted in the following paragraphs:

1) The group has focused on recommendations relating to the policy development level, and not on those relating to the operational level. This implies the existence of a shared vision in the sense that the technical-operational aspects of Internet are working correctly and therefore, from the point of

Continued on page 2

Table of Contents

The mission of the RIPE NCC is to perform activities for the benefit of the membership; primarily activities that the members need to organise as a group, although they may compete with each other in other areas.

Continued from page 1

view of Internet stability and robustness, it would be advisable not to introduce any important changes.

2) A broad vision of Internet Governance is consolidated, with the identification of a series of important issues that stretch beyond domain name administration, IP address allocation or the root server system.

3) One of the recommendations included in the report is very strong, in the sense that no particular government must exercise an oversight role over any Internet Governance component. This implies the conviction that the current situation, in which the United States government has certain specific roles and special prerogatives, both in the oversight of ICANN's functions as well as the root server system, cannot continue.

4) The creation of a global discussion forum is recommended, with the participation of all the interested parties, a forum which would be highly positive in order to achieve better coordination among the existing organizations (both governmental and intergovernmental) and to discuss the issues that are not being considered by any specific organization. This forum would allow the different actors to efficiently follow the international discussion agenda in relation to Internet Governance issues. This is very important for everyone, perhaps even more so for civil society organizations, as they usually have less resources to participate in all of the existing organizations and processes.

If this forum functions efficiently, it will constitute a platform for the creation of initiatives and working groups on specific matters.

Although it would have been impossible for the WGIG report to consider every point of view and therefore some may believe it to be incomplete or insufficient, the agreements which have been achieved must not be underestimated. If during the period of negotiation between governments, which is now beginning until the November summit, we could agree and give concrete form to those points we have mentioned, we would find ourselves faced with a very favourable situation, where transcendental changes in the history of Internet would be decided.

The WGIG report does not include any consensual recommendation regarding one of the most controversial issues: the need of having oversight over Internet resource administration or the lack thereof. For this there are four proposals. One of the positions (identified as Model 2) establishes that it is not necessary to create a specific organization to exercise this oversight.

This proposal is based on the fact that the implementation of the principles that were agreed during the first phase of the summit (transparency, multi-stakeholderism, openness, democracy, and participation) in the different organizations involved in Internet Governance, together with the existence of the new forum, would already allow the community to exercise oversight in a natural manner, based on transparency, and that therefore it would be unnecessary to establish new organizations for this specific purpose.

The other three options present different levels of government involvement in the oversight of the functions mentioned above, ranging from mild to strong involvement of governments in the development of policies relating to the administration of Internet resources.

The report is positive from the point of view of the addressing community, as there is an implicit acknowledgement that the current systems are functioning correctly and it includes only one recommendation in the sense that allocation policies need to guarantee equal access to numbering resources, specifically relating to IPv6. This concern is widely shared and considered by RIRs and their communities in their daily work.

It is important to highlight that the report talks about "equitable access to the resources" and not "equitable distribution of the resources," as had been mentioned previously on several opportunities by some governments in different documents and public positions. This is a significant change, as the expression "equitable distribution" was extremely imprecise and did not clarify what parameters would have to be used to evaluate said equality (population, economy, Internet penetration, or others).

The negotiation phase leading up to the Tunisia summit is only beginning. We must keep a close eye on this new stage of the process, trying to maintain a good level of participation and ensuring that the voice of the addressing community is represented on a permanent basis.

Raúl Echeberría is Executive Director/CEO of LACNIC, the Latin American and Caribbean Internet Address Registry. He also served as a member of the Working Group on Internet Governance.

Reprinted with permission from ARIN Review, Second Quarter, 2005.

Presentation of the Working Group on Internet Governance (WGIG) Report

The Report of the Working Group on Internet Governance was presented in Geneva on 18 July 2005 at a meeting open to all stakeholders.

The WGIG Report was previously transmitted on 14 July by United Nations Secretary-General Kofi A. Annan to the President of the Preparatory Committee of the World Summit on the Information Society (WSIS), Ambassador Janis Karklins, and the WSIS Secretary-General, Mr. Yoshio Utsumi. The document is available from the WGIG website at:
http://www.wgig.org/WGIG-Report.html

The Number Resource Organization (NRO) response to this document is available at:
http://www.nro.net/documents/nro26.html

More details on the meeting and the transcripts from the morning and afternoon session proceedings are also available at:
http://www.wgig.org/index.html

More information on the WSIS process is available at:
http://www.itu.int/wsis/ •

RIPE NCC Membership Survey 2005

Following from the successful RIPE NCC Membership Survey conducted in 2002, the RIPE NCC has conducted a second Membership Survey.

The results of the survey are available at:
http://www.ripe.net/membership/survey2005/results/

The purpose of these surveys is to ensure that the RIPE NCC continues to meet members' needs, and to give all members the opportunity to voice their opinions on the RIPE NCC and the services it provides.

As with the survey held in 2002, the RIPE NCC commissioned KPMG to conduct the RIPE NCC Membership Survey. This enabled the survey to be conducted independently from the RIPE NCC, with all individual responses being sent to KPMG to ensure confidentiality.

The survey was divided into three sections: the first section focused on current RIPE NCC services, the second concentrated on future plans and the third gave respondents the opportunity to make other suggestions.

As with all surveys, the challenge was to encourage members to respond. The RIPE NCC made concerted efforts to ensure that the membership was kept informed and encouraged to complete the survey.

KPMG has informed the RIPE NCC that the response rate to the survey was good, with 279 responses as compared to the 259 responses received for the 2002 RIPE NCC Membership Survey. In addition, it was encouraging to see a wider diversity of members represented this time, with responses coming from more than 50 countries as compared to the 19 countries that were represented in the 2002 survey.

There will be a presentation about the RIPE NCC Membership Survey 2005 at RIPE 51 to be held from 10 - 14 October 2005 at the Krasnapolsky Hotel in Amsterdam, the Netherlands. The results of the survey will be incorporated into the RIPE NCC's long-term strategy. •

European Union Commission Meeting

As a part of the RIPE NCC's efforts to include government and other stakeholders in the Internet's stability and development, two meetings with the European Commission have been held.

The first meeting was held on 16 March 2005. This was a smaller introductory meeting with the Commission for Information Society and Media's Head of Cabinet, Rudolf Strohmeier. The purpose was to introduce the various organisations involved in the development of the Internet in Europe.

Continued on page 4

Continued from page 3

The second meeting was held on 6 June 2005. This meeting was with Viviane Reding, Commissioner for Information Society and Media, and several other members of the EU Commission.

Representing Europe's Information Society were:
Rob Blokzijl, RIPE, Chair
Axel Pawlik, RIPE NCC, Managing Director
Paul Rendek, RIPE NCC, Head of Member Services and Communications
Giovanni Seppia, General Manager, CENTR
Sabine Dolderer, Director, DENIC
Richard Nash, EuroISPA, Secretary-General/Regulatory Affairs Manager
Malcolm Hutty, Regulation Officer, EuroIX/LINX
Veni Markovski, ICANN, Board of Director/ISOC, (Bulgaria) Founder and Chairman
Lynn St. Amour, ISOC, President/CEO
Fay Howard, Nominet UK, Director/EURid, Project Manager

The meetings allowed us to discuss the technical administration structures of the Internet, particularly in light of the current World Summit on the Information Society (WSIS) process. The purpose of the meeting was to exchange views and highlight the positive areas of the current system.

We are encouraged that the discussions have helped to forge a bridge of greater understanding with the EU Commission. The RIPE NCC plans to continue to sustain healthy and open lines of communication in the future. •

RIPE NCC General Meeting, October 2005

The next RIPE NCC General Meeting (GM) will be held adjacent to RIPE 51 in Amsterdam, the Netherlands.

According to the RIPE NCC Articles of Association, the members will be formally asked to approve the Charging Scheme 2006 at the RIPE NCC GM. This document will be published four weeks in advance of the RIPE NCC GM according to the formal requirements.

The RIPE NCC will also present the prospective RIPE NCC Activity Plan and Budget for 2006. Based on discussions at the GM in the RIPE NCC Services Working Group and the respective mailing lists, the RIPE NCC Executive Board will formally approve the final Activity Plan and Budget 2006 documents later in 2005.
More information on RIPE NCC General Meetings is available at:
http://www.ripe.net/membership/gm/ •

RIPE Meetings

RIPE 50

The RIPE 50 Meeting took place from 2 - 6 May 2005 at the Clarion Hotel, Stockholm, Sweden. There were over 375 participants at the meeting. Highlights of RIPE 50 included:

- The successful implementation of the new RIPE Meeting format into three days on operational and technical content, followed by two days on policy related issues.

- An update on the ICANN ASO Address Council. This presentation is available at:
http://www.ripe.net/ripe/meetings/ripe-50/presentations/ripe50-plenary-fri-ac.pdf

- A commentary on the ITU-T Proposal for National Address Registries for IPv6 by Geoff Huston, APNIC. This presentation is available at:
http://www.ripe.net/ripe/meetings/ripe50/presentations/ripe50-plenary-wed-itu-ipv6-proposal.pdf

- Final discussion on the RIPE Policy Development Process.

The RIPE 50 Meeting Report is available at:
http://www.ripe.net/ripe/meetings/ripe-50/report.html

Minutes from all the sessions given at RIPE 50 are available at:
http://www.ripe.net/ripe/meetings/ripe-50/minutes/index.html •

RIPE 50 Plenary Room

Next RIPE Meeting: RIPE 51

The RIPE 51 Meeting will take place 10 - 14 October 2005 at the Krasnapolsky Hotel in Amsterdam, the Netherlands. More information about the upcoming RIPE 51 Meeting is available at:
http://www.ripe.net/ripe/meetings/ripe-51/

Upcoming RIPE Meetings

RIPE 51: 10 - 14 October 2005, Amsterdam
RIPE 52: 24 - 28 April 2006, Istanbul, Turkey •

RIPE NCC Roundtable Meetings

The RIPE NCC has now been involved with two Roundtable Meetings to discuss Internet management issues relevant to governments, regulators and industry partners.

The first RIPE NCC Roundtable for Governments and Regulators was held on 30 March 2005 in Amsterdam. There were 29 attendees from 17 different countries within the RIPE NCC service region.

A summary from this meeting can be found at:
http://www.ripe.net/meetings/roundtable/march2005/summary.html

The positive feedback received during the first meeting led to the RIPE NCC facilitating a Roundtable on IP Addressing held by the NRO in co-operation with the ICANN GAC (Governmental Advisory Committee). This meeting was held on 10 July 2005 in Luxembourg during the ICANN Meeting. The focus of the discussions was Internet governance and management, with particular emphasis on issues of relevance to governments and regulators including:

- IPv4 and IPv6 address policies
- Internet routing
- Competitive addressing registries

Around 70 people attended from all over the world covering 32 countries, with approximately 30 people covering 15 countries from within the RIPE NCC service region. More information about the Joint NRO/GAC Roundtable on IP Addressing can be found at:
http://www.nro.net:/meetings/nro-gac/index.html

More Roundtable Meetings will be organised for 2006. If you have any comments or suggestions please send them to *<roundtable@ripe.net>.* •

RIPE NCC Regional Meeting, Moscow 2005

The RIPE NCC Regional Meeting, Moscow will take place from 15 - 16 September 2005 at the Marriott Grand Hotel in Moscow.

This meeting follows from the previous RIPE NCC Regional Meeting in Moscow, held in June 2004. More information about the June 2004 meeting, including minutes and presentations, is available at:
http://www.ripe.net/meetings/regional/moscow-2004/index.html

For more information about the RIPE NCC Regional Meeting Moscow, September 2005, including registration details and the published minutes and presentations when available, please see:
http://www.ripe.net/meetings/regional/moscow-2005/index.html

RIPE NCC Regional Meetings are specifically aimed at providing participants with a forum to discuss their own regional topics.

The Regional Meetings bring RIPE NCC members from a specific region closer to the RIPE community and encourage their participation in RIPE Meetings, RIPE Working Groups and the policy-making process.

RIPE NCC Regional Meetings are an activity of the RIPE NCC to get direct feedback from its membership about region specific issues. The meetings help to establish direct contact with and among RIPE NCC members.

Attendance to the RIPE NCC Regional Meetings is open to anyone and is free of charge. •

NRO Comments on Proposed Review Procedure for ASO Policy Proposals

On 17 June 2005, the Number Resource Organization (NRO) submitted to ICANN their comments to the updated “Proposed Review Procedure for ASO Policy Proposals”.
These comments can be found on the NRO website at:
http://www.nro.net/documents/nro25.html

The proposed review procedure is available from the ICANN website at:
http://www.icann.org/announcements/announcement-31may05.htm •

Current RIPE Policy Developments

HD Ratio for IPv4

Discussions about introducing the HD Ratio method for IPv4 usage have been ongoing. The last call for contributions was 15 July 2005.

IP Assignments for Anycasting DNS Servers

No clear consensus was reached on this proposal. Discussions will start again when there is a revised version of the proposal.

IPv6 Initial Allocation

Regarding the proposal to change IPv6 allocation criteria, there was no clear consensus to completely remove the 200 customer requirement. Therefore the discussion will be restarted when there is a revised proposal.

IPv6 Address Allocation and Assignment Policy-definition of an "End-Site"

The proposal is to have a clear definition of an "end-site" in order to establish clear internal assignment policies. This was in the discussion phase until 10 August 2005.

Proposal to remove special African policies from RIPE policy documents:

Due to the formal recognition of AfriNIC by ICANN, it has been proposed to remove special African policies from RIPE policy documents. The last call for contributions was 15 July 2005.

Proposal to add regional boundaries to policy documents:

This proposal was withdrawn. •

Recent Updates to the RIPE Database:

Finding Contacts for Abuse Incidents

One of the main uses of the RIPE Database is to find someone to contact for abuse incidents. It was not always clear which information in the database should be used for this.

The RIPE Database has been modified to make it easier to get the correct abuse contact information. The most important changes have been adding the "abuse-mailbox:" attribute, hiding attributes that contain e-mail addresses and modifications to the Incident Response Team (**IRT**) object.

Adding the "abuse-mailbox:" Attribute

This is a new attribute which has the e-mail address to which abuse complaints should be sent. It has been added to the **person, role, mntner,** and **organisation** object types.

Hiding Attributes that Contain E-mail Addresses

Users often send mail to every e-mail address they see in a query result. To avoid this, some attributes that contain e-mail addresses are now hidden by default. These are "notify:" and "changed:". Also, if there is an "abuse-mailbox:" attribute then "e-mail:" will not be displayed. It is possible to see the full object, including the hidden attributes, by using the "-B" flag.

Modifications to the IRT Object

Users had considered it difficult to create **IRT** objects, specifically so people can document the people in their security teams. To make it easier to create the **IRT** object, the "signature:" and "encryption:" attributes are now optional. In addition, a recent modification means that if user uses the special "-c" flag to find contact information, the **IRT** objects are returned in a single command.

More details of these changes are available at: *http://www.ripe.net/db/news/abuse-implemented-20050421.html* •

ARIN Update

Government Involvement Adds Depth to Directory Services Discussion

During open discussion at the ARIN XV Public Policy Meeting in April, 2005, the ARIN community experienced its first participation by government representatives in a policy debate. Several individuals presented interesting perspectives on the use of currently public data from ARIN's WHOIS service. Their contributions to the discussion helped provide added depth to the debate. Speakers included representatives from the U.S. Federal Trade Commission, the U.S. Department of Justice, the U.S. Federal Bureau of Investigation on behalf of the Department of Homeland Security, and remote participation by an official with the Royal Canadian Mounted Police.

In March 2005, Policy Proposal 2005-2, Directory Services Overhaul, was introduced on the ARIN public policy mailing list. After two years of policy proposal discussions regarding the purpose and scope of ARIN's WHOIS database, this new initiative caught the attention of several U.S. government entities and expanded the discussion into an exchange of ideas between the public and private sectors in the ARIN region. This exchange demonstrated the need to study directory services from a broader, requirement-based perspective to determine what data ARIN should collect and how ARIN should maintain and use that data.

The general sentiments expressed by the government representatives were very similar in nature. They stressed the importance of fast access to the data in ARIN's WHOIS to aid Federal, state, and local law enforcement and consumer protection agencies in combating illegal activity while recognizing the concern for privacy issues surrounding this data.

This public/private sector dialogue has continued between several of these government agencies and ARIN. Members of the ARIN staff have provided and have planned future tutorial presentations to the staffs of these agencies. Topics have included the Regional Internet Registry (RIR) system and the purpose and use of the WHOIS database. Distributing copies of the "Querying ARIN's WHOIS" computer-based training module has proven quite useful.

Similar discussions have started in other RIR regions and on the global stage. At the recent ICANN meeting in Luxembourg, the ICANN Government Advisory Committee (GAC) sponsored a workshop that focused on the importance of WHOIS data to law enforcement agencies. Throughout many of the presentations and during the question and answer period, the discussion turned to IP addresses and data held in RIR directory services. During its meeting in Vancouver, the GAC pledged to continue its efforts to broaden understanding of other important public policy aspects of WHOIS data, such as the protection of consumers, privacy, and intellectual property.

It is anticipated that this open public/private sector dialogue will continue at the ARIN XVI Public Policy Meeting in October where Policy Proposal 2005-2 will be further discussed. •

APNIC Update

Live Chat Help

A live online chat service is now available as part of the APNIC Helpdesk. This service allows users to chat online with APNIC Hostmasters in real time. Hostmasters can offer assistance in completing resource request forms, updating the APNIC Whois Database, or resolving any other membership or resource issues. The service is accessed by clicking on the APNIC Helpdesk chat logo on the APNIC home page. This launches a chat window, connecting the users directly with an APNIC Hostmaster. Users are also able to save or print transcripts of the chat sessions for future reference. For more information, refer to:
http://www.apnic.net/helpdesk

Online Voting

APNIC recently conducted an online electronic voting trial. The service is available through the MyAPNIC website, which allows the official representatives of current APNIC members to cast votes securely. Many members participated in the trial and the system will now be made available for all future elections on issues such as Executive Council (EC) elections, NRO Number Council elections, and other decisions of the APNIC membership.

APNIC 20

The 20th APNIC Open Policy Meeting (APNIC 20) will be hosted by Vietnam Network Information Centre (VNNIC) in Hanoi from 6-9 September 2005. This will be the first APNIC meeting held in Vietnam. In addition to the normal program of technical and policy meetings, APNIC 20 will also feature an IPv6 workshop, tutorials on spam and security, and panel discussion on the Internet governance debate and the possible implications for the IP address community. Full details are available at:
http://www.apnic.net/meetings/20 •

LACNIC Update

From June 27 to June 30, LACNIC VIII was held in Lima, Peru. The scope of the meeting was highly ambitious, as it not only included the Public Policy Forum, but also LACNIC's Annual Member Assembly, the Fourth Annual Latin American NAPs Regional Meeting (NAPLA), the third Latin American IPv6 Forum (FLIP-6) and the Latin America and the Caribbean IPv6 Task Force Meeting (LAC TF IPv6).

This latest edition of NAPLA concluded with an agreement between its operators on the importance of an interconnection backbone among the region's NAPs. This agreement establishes the guidelines for the development of this regional project.

During the Public Policy Forum the global policy proposal on IPv6 Address Space Allocations from IANA to RIRs was discussed and approved. This proposal is currently in the period of last call for comments (45 days). After this period the proposal will be sent to LACNIC's Board of Directors for its ratification. In addition, proposals were analysed for recovering non-utilized Internet resources and for evaluating additional IPv4 address allocations to ISPs with presence in different countries within the region covered by LACNIC. Finally, the issue of prefix size in IPv6 reassignment was discussed. No decision was made regarding the latter proposals, therefore their discussion continues on the lists.

FLIP-6 is a forum used for exchanging information regarding IPv6 implementation and deployment in the region covered by LACNIC. Significant advances in the deployment of this protocol were observed in relation to prior editions.

On this occasion 12 different presentations from 6 Latin American countries were made. LAC TF IPv6 welcomed a new National IPv6 Working Group. Now Peru has joined Brazil, Cuba and Mexico with the creation of the fourth National Working Group in Latin America. Finally, efforts to promote IPv6 were furthered through a tutorial on the basic elements for IPv6 implementation.

The Annual Member Assembly authorized new modifications to LACNIC's fee structure, reducing the cost of LACNIC's minimum size allocations, established as a /21, and deciding to cancel the IPv6 space fee for those organizations that are already covering their membership by the allocation of IPv4 space. These changes aim at improving the accessibility of Internet resources in Latin America and the Caribbean. The Assembly also approved the 2004 annual report, which includes the activities carried out by LACNIC staff and budget execution.

Continuing with the promotion of IPv6 adoption in our region, during LACNIC VIII the IPv6 Tour was officially announced. During the following five months the Tour will visit eight cities in eight different Latin American countries with the purpose of providing information and promoting the IPv6 protocol.

Lastly, LACNIC IX will be held on the week between 22 May and 26 May, 2006, at a location yet to be decided.

Information on LACNIC VIII:
http://lacnic.net/pt/eventos/lacnicviii/index.html

Information on the IPv6 Tour:
http://ipv6tour.lacnic.net •

Changes to RIPE NCC Online Payments

As part of its continued efforts to provide secure and efficient interaction mechanisms, the RIPE NCC has transferred its online payment system to Triple Deal, a reliable third party. The main advantage of this online payment system is that it offers the payee improved payment security and immediate verification of credit card payment or non-payment.

From mid-July 2005, Triple Deal has been handling all credit card payments (Amex, EC/MC and Visa) made to the RIPE NCC. It is also possible to make bank transfers through Triple Deal if the bank is located in certain countries.

How to pay invoices

All invoices sent by the RIPE NCC include a unique payment URL. By clicking on this URL, the payee will be directed to the payment screen where they can complete their credit card payment or bank transfer. Alternatively, the payee can pay the invoice using their RIPE NCC LIR Portal account.

The RIPE NCC LIR Portal is available at:
https://lirportal.ripe.net/

Using the LIR Portal, the payee should click on the 'Pay Now' button to enter their payment details.

For more information, or if you have any questions, please contact: *<billing@ripe.net>* •

Introducing DNSSEC

With the help of a "potential" news story, Olaf Kolkman, NLnet Labs, explains why the Internet needs DNSSEC, how it works, and what is needed for its full-scale implementation.

The scenario as described in the made-up article is not as far-fetched as it may seem. In virtually all interactions between computers on the Internet, services are located using the DNS. E-mail recipients are identified using the DNS; web services are found using the DNS; and applications like messengers, stock tickers, and Internet telephony all use the DNS to find the machines that one needs to connect to for interaction.

The DNS is vulnerable to attacks where the name-to-address mapping is being modified by an attacker. This problem was identified years ago.

Since then, engineers have joined forces in the Internet Engineering Task Force (IETF) to develop extensions to the DNS that allow these name-to-address mappings to be secured. The security extensions are known as DNSSEC and were published as RFCs (Request for Comments, the IETF's standard documents) in March 2005.

The Malta Business Tribune

BE-rt and erNie merger stung in DNS scam

Malta, 33 November 2005

The Maltese branch of Interpol's cyber crime department has arrested five individuals that are supposedly linked to the US$50 million stock fraud that occurred last month in relation to the merger of BE-rt Inc and erNie Ltd. The gang operated by exploiting weaknesses in the Domain Name System (DNS). The DNS is the system that is used to translate names like www.ripe.net into the addresses of the computers. The DNS is used whenever a user uses a name to access a service on the Internet.

An Interpol spokesman explained: "The gang used exploits in the DNS to reroute and intercept e-mails that related to the merger between the two companies.

After obtaining prior knowledge on the stock rate and the date of the merger the gang used the same DNS exploits to reroute a stock ticker service. By inserting false stock rate information for BE-rt Inc, they managed to influence the stock market on the day prior to the merger in a way that maximised the gang's prior knowledge. Through clever trading of stock options, these guys earned 50 million euros".

Insider knowledge was suspected when complaints about the false stock ticker information surfaced. Only after a full audit of the erNie Ltd computer environment was it shown that the information was not consciously leaked by the senior management of the two companies.

After many years of development, DNSSEC has reached production quality in both specification and implementation. Recent versions of open source nameserver software such as BIND 9.3.1 and NSD 2.3.0 implement DNSSEC. DNSSEC is now ready for the public Internet.

DNSSEC is based on public key cryptography mechanisms and allows DNS data to be verified for integrity and authenticity. In other words, by using DNSSEC one can tell whether or not somebody inserted a fake IP address for the mail server for "BE-rt Inc" and that the IP address for the stock ticker service was replaced. DNSSEC would have prevented the mail and the stock-ticker service redirect in the above made-up example.

One could argue that this attack would not have been possible if the mails between the two companies had been encrypted and if the stock ticker server had used secured http. But in reality, encrypted e-mail and secure stock tickers hardly happen.

Deployment of DNSSEC raises the bar for a large set of attacks on all kinds of applications for which maintaining security on application level may be too expensive to do correctly. Many End Users do not use mail encryption because it is too difficult or too expensive. It is expected that DNSSEC deployment will slowly pick up in 2005.

As with all early deployment, there will be a few hurdles that need to be negotiated: tools for DNSSEC administration are in their infancy and the benefits of early deployment are small as there are very few signed zones and very few

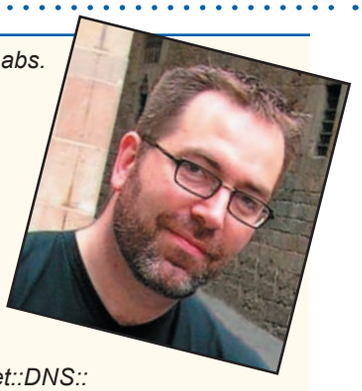
Continued on page 10

Continued from page 9

validating name servers.

On the other hand, early deployment may provide competitive benefits in case DNSSEC deployment becomes urgent. Numerous parties, including top-level domain (TLD) registries are planning pilot projects for the deployment of DNSSEC and the Regional Internet Registries are actively tracking developments while planning for deployment.

Although the protocol and implementation details of DNSSEC are somewhat esoteric the principles are fairly simple. As noted above, the protocol is based on public key cryptography. Public key cryptography schemes are base on "key-pairs" consisting of a private and a public key. Users generate such pairs, publish the public key to other users and keep the private key securely secret. •



Olaf Kolkman works for NLnet Labs. Prior to 1 September 2005, he was a System Architect in the New Projects Department of the RIPE NCC. Among other things, he is co-Chair of the IETF DNSEXT Working Group that developed the DNSSEC standard and is author of the Net::DNS::SEC Perl library and maintainer of the Net::DNS Perl library.

DNSSEC Deployment at the RIPE NCC

Deployment of Domain Name System Security Extensions (DNSSEC) is the second (and last) phase of the Reverse DNS restructuring project. During the first phase of the Reverse DNS restructuring project, the RIPE NCC:

- modified internal databases to make the RIPE Whois Database the authoritative source for zone file generation
- changed the interface for creation and maintenance of delegation of reverse domains
- introduced the "mnt-domains:" attribute
- cleaned up inconsistent data
- simplified the requirements for reverse delegation

The focus is now on deployment of DNSSEC on the reverse tree. During this phase we will:

- enable DNSSEC support on our DNS server infrastructure
- introduce the infrastructure and procedures for maintaining the keys needed to sign DNS data
- introduce the mechanisms and tools for the exchange of key information between child and parent

Steps in DNSSEC Deployment at the RIPE NCC:

• Zone Signing

Keypairs are needed to sign zones. The private keys must be protected, while the public keys must be added to the zones. The keys need to be maintained. For more information about this, see:
http://www.ietf.org/internet-drafts/draft-ietf-dnsop-dnssec-operational-practices-04.txt

The RIPE NCC will build a signer application that can be used to maintain the private keys and sign the zones. We will base this on existing tools.

We have drafted a key maintenance procedure. It describes how we will replace keys and how we will let people know about changes to the keys used.

• DNS Server Architecture

Primary and secondary servers will need to support the DNSSEC protocol. As we do not control most secondary servers we are relying on the operators that do. We are arranging an upgrade of the infrastructure. For more information about the DNSSEC protocol and specifications, see RFC4033, RFC4034 and RFC4035.

• Provisioning of Secure Delegations

Maintainers of reverse zones will need to get a secure delegation. These are represented through Delegation Signer Resource Records (DSRRs) that appear in the parent zone. The DSRRs point to DNSKEY Resource Records. You can get a secure delegation by submitting domain objects to the RIPE Whois Database.

Continued on page 11

Continued from page 10

For more information about this, please see the RIPE NCC Procedure for Requesting DNSSEC Delegations, at:
http://www.ripe.net/rs/reverse/dnssec/registry-procedure.html

The RIPE NCC intends to provide a web interface to help you create domain objects. When you submit new domain objects with secure delegation requests, the delegation checker will look at them. We explain the requirements for this in the RIPE NCC Procedure for Requesting DNSSEC Delegations.

You can find more detailed information in the Delegation Checker modifications page available at:
http://www.ripe.net/cgi-bin/delcheck/delcheck2.cgi

There will be no change to existing authentication mechanisms. Key exchange will be based on the authentication of domain objects. For authentication mechanisms based on public key cryptography (PGP and X.509), we will introduce additional checks on the timestamp of signatures.

• Current Status of DNSSEC Deployment at the RIPE NCC

The RIPE NCC has made a start with signing some of its zones. By the end of 2005 a number of reverse zones will be signed and it will be possible to secure delegations from these domains. •

New Instances of RIPE NCC Operated K-root Server

The RIPE NCC operates the K-root server, one of the 13 root name servers in the world. These root name servers are a crucial part of the Internet DNS infrastructure. The RIPE NCC has operated the K-root server since 1997 when the first server was installed at the London Internet Exchange (LINX) in London, UK. In 2003, the RIPE NCC deployed the first anycast instance at the Amsterdam Exchange (AMS-IX) as described in ripe-268.

The RIPE NCC has continued to deploy more instances of the K-root server. Since August 2004, instances of the K-root server have been deployed in:

- Milan, Italy
- Reykjavik, Iceland
- Helsinki, Finland
- Poznan, Poland
- Geneva, Switzerland
- Budapest, Hungary
- Brisbane, Australia
- Abu Dhabi, United Arab Emirates

The main objective of this effort is to improve local service quality to the K-root server for a significant local ISP community. In addition, it isolates the impact of an "external" Denial of Service (DoS) attack and localises the impact of a "local" DoS attack.

In April 2005, the RIPE NCC deployed a new mirror instance of the K-root Internet root name server in Tokyo, Japan. This mirror server was the first global node of the K-root name server outside of Europe and should help stabilise the Internet infrastructure in the Asia-Pacific region. Other global nodes were added in July 2005 in Miami, the United States, and in August 2005 in Delhi, India, bringing the total number of global nodes to five. The other global nodes are situated in London and Amsterdam.

Since August 2004, the K-root server is also IPv6 transport enabled on one of the global nodes located in Amsterdam. It is answering on IPv6 address 2001:7fd::1 and is connected to two Internet Exchanges: AMS-IX and NL-IX.

More information about the RIPE NCC's operation of the K-root name server is available at:
http://k.root-servers.org •

RIPE NCC Training Courses

LIR Training Courses

Madrid, Spain
Friday, 23 September 2005

Moscow, Russia
Tuesday, 27 September 2005

Nuremberg, Germany
Thursday, 6 October 2005

Amsterdam, Netherlands
Friday, 7 October 2005

Tirana, Albania
Friday, 21 October 2005

Rome, Italy
Friday, 11 November 2005

Geneva, Switzerland
Friday, 18 November 2005

Ankara, Turkey
Friday, 25 November 2005

Paris, France
Friday, 2 December 2005

London, United Kingdom
Monday, 5 December 2005

London, United Kingdom
Tuesday, 6 December 2005

Amsterdam, Netherlands
Friday, 9 December 2005

Kuwait City, Kuwait
Monday, 12 December 2005

DNSSEC Training Courses

Moscow, Russia
Wednesday, 28 September 2005

Amsterdam, Netherlands
Thursday, 6 October 2005

Damascus, Syria
Monday, 14 November 2005

London, United Kingdom
Friday, 2 December 2005

Lisbon, Portugal
Friday, 16 December 2005

Routing Registry Training Courses

Sofia, Bulgaria
Friday, 21 October 2005

Oslo, Norway
Friday, 28 October 2005

Edinburgh, United Kingdom
Friday, 4 November 2005

Munich, Germany
Friday, 25 November 2005

Conference Calendar

Conferences and meetings that may be of interest to RIPE NCC members, September 2005 – April 2006.

06 - 09 September 2005
APNIC 20
Hanoi, Vietnam
http://www.apnic.net/meetings/

15 - 16 September 2005
RIPE NCC Regional Meeting
Moscow, Russia
http://www.ripe.net/meetings/regional/

19 - 30 September 2005
WSIS Phase II PrepCom III
Geneva, Switzerland
http://www.itu.int/wsis/preparatory2/pc3/index.html

10 - 14 October 2005
RIPE 51
Amsterdam, the Netherlands
http://www.ripe.net/ripe/meetings/ripe51/index.html

23 - 25 October 2005
NANOG 35
Los Angeles, USA
http://www.nanog.org/

26 - 28 October 2005
ARIN XVI
Los Angeles, USA
http://www.arin.net/meetings/index.html

06 - 11 November 2005
64th IETF
Vancouver, Canada
http://www.ietf.org/meetings/0mtg-sites.txt

16 - 18 November 2005
WSIS Phase II
Tunis, Tunisia
http://www.itu.int/wsis/tunis/index.html

30 November - 4 December 2005
ICANN
Vancouver, Canada
http://www.icann.org/meetings/

12 - 14 December 2005
AfriNIC III
Cairo, Egypt
http://www.afrinic.net/meeting/index.htm

16 - 24 January 2006
SANOG 7
Mumbai, India
http://www.sanog.org/future.htm

17 - 19 January 2006
RIPE NCC Regional Meeting
Doha, Qatar
http://www.ripe.net/meetings/regional/

22 February - 3 March 2006
APRICOT 2006
Perth, Australia
http://www.2006.apricot.net/

28 February - 3 March 2006
APNIC 21
Perth, Australia
http://www.apnic.net/meetings/

19 - 24 March 2006
65th IETF
TBD
http://www.ietf.org/meetings/0mtgsites.txt

22 - 24 March 2006
NZNOG
Wellington, New Zealand
http://www.nznog.org/

27 - 31 March 2006
ICANN
Wellington, New Zealand
http://www.icann.org/meetings/

24 - 28 April 2006
RIPE 52
Istanbul, Turkey
http://www.ripe.net/ripe/meetings/ripe52/index.html

If you are interested in having a RIPE NCC speaker at one of your own events or conferences, please contact <*speaker@ripe.net*>.