Internet security: report on ICANN's initiatives and on the discussions in the European Union

December, 2001

Stefano Trumpy (CNR/IAT) and
Christopher Wilkinson (European Commission)*

stefano.trumpy@iat.cnr.it *christopher.wilkinson@cec.eu.int*

Security aspects

The Internet is designed as a highly distributed system, with very few single points of control or failure. The computers that interconnect all the networks world-wide are consequently very numerous and widely distributed globally. They are also owned and controlled by many distinct organisations and individuals Root Servers.

Consequently, general co-ordination of the Internet, and ***a fortiori*** security, depends on widespread co-operation.

One major objective of the distributed architecture of the Internet is precisely that of insulating the networks as a whole from any particular failure. Indeed, as seen, the Internet responded to the 9/11 events very robustly, particularly in the United States and Europe, the loss of a major telecommunications facility adjoining the WTC notwithstanding. But this may not have been the case in more peripheral parts of the Internet; South Africa reported a significant and prolonged outage at the time.

However, certain Internet functions are centralised due to the necessity of unique assignments of names, addresses and protocols. These are the functions that are under the auspices of ICANN itself. Accordingly, should there be vulnerabilities and failures in the future, they might occur in these particular areas.

---

* *Stefano Trumpy is Research manager at CNR/IAT, Italy Responsible of international relations of ".it" registry; Italian delegate in the ICANN Governmental Advisory Committee (GAC). Christopher Wilkinson is Vice Chair and European Commission delegate to GAC and Adviser, Directorate General Information Society, European Commission.*

Rethinking security after September 11th 2001: which role for ICANN?

One by-product of the relative success of the Internet under stress has been a certain sense of complacency among the operators of central Internet functions. Their preferred philosophy is to proceed on the basis of informal co-operation and best practice guidelines for the operation of the Internet infrastructure, such as RFC 2870. However, responsibility for monitoring and enforcing compliance is not sufficiently clear at present and the respective roles of ICANN, governments and/or external auditing need to be clarified.

In the recent ICANN meetings in Marina del Rey (November 10-15th) a wide range of potential problems and issues where discussed; a detailed analysis of the outcome will be prepared in due course by ICANN staff and other participants. The following points were addressed in particular and ICANN can be expected to focus on these matters.

In general, since security and reliability are relative concepts, the consensus was to approach the question systematically through risk analysis and auditing performance with respect to agreed best practices, rather than setting formal, contractual requirements. In any event, absolute security is an impossibility. What is required is to balance the costs and inconvenience of heightened security with the requirements of reliability and confidence.

Discussion of security measures to be adopted by ICANN

During the third annual meeting of ICANN the following arguments were discussed:

1. Vulnerabilities

1.1 Distributed Denial of Service (DDOS)

Certain vulnerabilities are dependent on general problems in the networks. For example, distributed denial of service (DDOS) attacks will continue to be a significant threat in the future. In this context, the Chairman of RIPE drew attention to a large number of mass-produced personal computers that can be connected to the Internet as soon as they are purchased. These are unwary sitting targets for the perpetrators of DDOS attacks. This issue should be taken up with PC vendors. It is not clear whether the Root Server System or the DNS name servers are particularly likely to be a target for DDOS. To date, other more visible large commercial sites have been targeted.

1.2 Complexity

Systems become more vulnerable as their complexity and inter-dependencies increase. This is relevant to the Internet. Modern software packages are much more complex than they were a few years ago. In practice, vulnerabilities have been inadvertently increased by their use. It is probably impossible to avoid bugs and other weaknesses in such systems while correcting errors through “patches” is

now getting out of hand. Increasing standardisation on a few operating systems and major software packages increases overall vulnerability. Lack of diversity is another source of risk. In particular, the software running the Internet centralised functions should be diverse and recoverable from secondary or back-up sites.

1.3 ***Root Server System:***

Currently the Root Server System is still managed by volunteer organisations and individuals among whom are some of the best and most dedicated engineers on the Net, working in close co-operation with each other. These activities are hosted by several different organisations, including the US Department of Defence and other US Government departments. However, commercial users and ccTLD Registries are uncomfortable with the informality of the current regime, and some said that they would expect such a critical infrastructure function to be the subject of a more rigorous and transparent regime such as service contracts. The debate was inconclusive, but there appeared to be a consensus that, in due course, the second generation of Root Server operators should come under a more formal regime.

From the security point of view, the Root Server System currently contains sufficient redundancies to be able to shrug off and survive an attack limited to any one (or a few) of the 13 Root Servers. On the other hand, should all 13 Root Servers be the target of a comprehensive DDOS attack, the situation could temporarily become very serious. The consensus in the meetings was that this would be highly unlikely. However, the Root Server operators should probably assess these risks more systematically and take appropriate precautions if necessary.

Most commentators said that too many of the Root Servers (currently ten out of thirteen) are in the United States. There are engineering constraints on either increasing the number of root servers or on re-locating them in the short term. Physical re-location of a Root Server (for example to a different country) would involve changing its IP address. This would require updating the corresponding information currently encoded in hundreds of thousands of name-servers, world-wide. Increasing the number of Root Servers would require going back to IETF to modify the protocol.

The current philosophy is to develop a MOU among ICANN and the 13 Root Servers and encourage implementation of best practice guidelines based on RFC 2870: “Root Name Server Operational Requirements” dated June 2000. Some commentators argued that RFC 2870 should now be revisited, in view of the increased attention paid to security aspects. ICANN will issue a report on the Root Server system before the end of 2001. This report prepared by RSSAC"[1]

[1] RSSAC-ICANN - ICANN Root Server System Advisory Committee

under the terms of the current ICANN/US DOC CRADA"[2] is awaited with great interest world-wide.

1.4 *DNS Name Servers:*

The name servers replicate all or part of the information derived from the Root Servers and the TLD Registries, that is necessary for routing IP packets throughout the Internet. Following the recommendations of RFC2182, each TLD should have at least two secondary servers and possibly more (in practice, the number varies from 2 to 8), located in different autonomous systems. Most ISPs will cache (copy) some of this data to accelerate resolution of enquiries by their customers. Consequently there are very many name-servers in the DNS. There would appear to be several problem areas here:

- Significant numbers of ccTLD Name Servers also act as secondary servers for several TLDs. Thus secondary servers of other TLDs are maintained on the same TLD server. Furthermore, numerous TLD Name Servers operate obsolete versions of the BIND software, some of which are known to be insecure. It is not clear whether this situation constitutes an additional risk of propagation in the event of a virus or a DDOS attack..

- The underlying quality of registration data from which the Whois data and the Zone Files are derived, leaves a great deal to be desired. Some technical reports[3] suggest that as many as two-thirds of the domain names have erroneous ("mis- configured") data, possibly arising and/or from lax maintenance by Requirements, Registrars and Registries and from the speculative character of a significant proportion of domain name registrations. The Internet continues to function, these shortcomings notwithstanding. However it is difficult to argue that DNS Registration data is relevant to identify perpetrators of DDOS, or eventually for law enforcement, while at the same time condoning such poorly recorded data.

- For some time a new more secure DNS protocol known as DNS-Sec, has been under development. Although DNS-Sec is already implemented and functioning, the new product implies an increase of an order of magnitude in the size of data files, thus imposing remarkable operational overheads. Consequently, DNS-Sec is not yet deployed, and the market does not appear to support it spontaneously. However, the new system will be necessary for building the chain of trust necessary to develop electronic commerce. New versions of the system aimed at reducing these complexities have been developed. In any event, DNS-Sec would facilitate authentication of DNS registration, modifications and queries. It would not address other identified weaknesses in the DNS. . More generally, this is perhaps an illustration of the

[2] CRADA-Cooperative R&D Agreement between ICANN and US DOC/NIST/NTIA
[3] For example, Nice and Men, Reykjavik, Iceland (and URL)

question of how the costs of more secure operation in the Internet will be allocated and paid for.

2 Action to be taken

What has to be considered now is the future security of the Internet in any possible critical situation. The users, the market and the governments are demanding this. The studies to be undertaken are likely to include:

- risk analysis
- locating single points of failure
- disaster recovery
- best practices for operators
- identifying responsibility for implementing and monitoring eventual enforcement.

The roles of ICANN and other Internet participants will need to be defined. ICANN's Chief Executive, Stuart Lynn, argued that ICANN should operate through incentives, transparency and encouraging best practices rather than through contractual obligations and sanctions. In any event, a significant work-programme is anticipated in the near future, coming from the recently created "Standing Committee on Stability and Security."

On January 4th 2002 ICANN published the document "ICANN DNS Security Update #1"; see the URL: http://www.icann.org/committees/security/dns-security-update-1.htm The document contains a summary of the discussions that took place in the meetings of the constituencies and in the plenary sessions dedicated to the theme of security, during last November meetings in Los Angeles. The conclusion is the following: "A fundamental recognition by the ICANN Board is the need to establish an ongoing mechanism within ICANN to coordinate security requirements and priorities. ICANN acts as a meeting point and forum for the various technical, operational, and managerial interests that underlie the security of the DNS and address allocation systems. A properly staffed, ongoing effort is needed to monitor and coordinate the DNS security agenda, to ensure that security threats and risks are properly identified and assessed, and to determine and communicate new requirements and priorities. The Board, therefore, decided to create an ongoing advisory committee charged with perform these functions."

3. Position of the Governmental Advisory Committee

The Chair of the GAC, Paul Twomey, stated that, in the event of serious problems with the Internet infrastructure, the focus – and the blame – would be on governments, and not on ICANN or the Internet operators. Governments have a direct interest in the quality of the operation, the results of risk analysis and the nature of the improvements proposed.

Arguably, national governments will be more sensitive to the security aspects of the DNS than in the case of other aspects of Internet management, due to their broader responsibilities for network security. They also have a clear interest in the ccTLD Registries operating within their jurisdictions, whereas ICANN might be expected to take the lead with the Root Servers and the generic Top Level Domains.

However, the overall picture is far from straightforward. Several countries' ccTLDs are operated from other locations, including in the US and, in a few cases, the EU. Many ccTLD name servers are naturally located in other parts of the world. Establishing a chain of responsibility and accountability in these circumstances may be technically, if not politically, complex. The level of public responsibility for the many name servers operated by the ISP industry is also moot.

The consensus in the GAC was that governments should emphasise mutual responsibility rather than sovereignty and unilateral authority in these areas.

Security measures taken by the European Union

The European Union Telecommunications Council has adopted a Resolution on a common approach and specific actions in the area of network and information security. The resolution to be adopted is a comprehensive position, which rests on a number of previous recommendations and directives adopted in the recent past.. Some of the main areas of concern in that context and proposed actions are presented, below:

1. networks and communications systems have become a key factor in economic and social development and their availability and integrity are crucial to essential infrastructures, as well as to most public and private services and the economy as a whole;

2. in the light of the increasingly important role played by electronic services, the security of networks and information systems is of growing public interest;

3. the complex nature of the network and information security means that in developing policy measures in this field, public authorities must take into account a range of political, economic, organisational and technical aspects, and be aware of the decentralised and global character of communication networks;

4. the Internet infrastructure should provide the greatest possible availability and be managed and operated in a robust and transparent manner;

5. network and information security means:

    - ensuring the availability of services and data

    - preventing the disruption and unauthorised interception of communications

- confirmation that data which have been sent, received or stored are complete and unchanged
- securing the confidentiality of data
- protection of information systems against unauthorised access
- protecting against attacks involving malicious software and securing dependable authentication

The Member States are asked:

- to launch or strengthen information and education campaigns to increase awareness of network and information security;
- to promote best practices in security policies based, where appropriate, on internationally recognized standards;
- to review national arrangements regarding computer emergency response, taking the necessary action as regards their ability to prevent, detect and react efficiently at national and international levels against network and information system disruption and attack;

The Commission is invited:

- to facilitate an exchange of best practice regarding awareness-raising actions and to draw up an initial inventory of the various national information campaigns;
- to reinforce the EU dialogue and co-operation with international organisations and partners on network security, in particular on the implications of the increasing dependency on electronic communication networks;
- to propose a structure for a more open and transparent operation of critical parts of the Internet infrastructure, including the root server system;

to set up a " Cyber - Security task force" **International cooperation in Internet Security.**

Several aspects of Internet security identified during the ICANN meetings could usefully be included in the agenda of European international consultations with other countries. These could include:

1. Confirmation that Internet Security is a joint, co-operative task for the private sector and governments. It is not technically possible for any individual government to achieve the necessary results unilaterally. The EU will address these issues for the

critical facilities for which we are responsible, in conjunction with the Member States and the private sector, but the practical outcome will require international cooperation with other governments and with ICANN.

2. Moving towards a more balanced and transparent Internet management system, including a clarification of ICANN's role and responsibilities. Achieving a more balanced geographical distribution of the current 13 Root Servers, taking full account of current and future Internet traffic flows. Many countries are looking forward, with great anticipation, to the actions that ICANN will take on the basis of the forthcoming report on the Root Server System.

3. More generally, we expect ICANN to initiate an action programme to follow up on the results of the Marina del Rey meetings. The EU will keep in close touch with further work in this area, directly with ICANN and through the Governmental Advisory Committee (GAC).

Migrating from an Internet based on best effort towards a network with guaranteed level of performance

This is a very complex question. Internet was born and subsequently has grown up generally based on best effort criteria. The routing is assured by a best effort approach; the services on the network are assured on the same criteria, based on the availability of the end to end bandwidth. Electronic commerce and professional services need to foresee an evolution of the network towards a globally guaranteed level of services/ availability. This will imply higher costs and the co-operation of many actors for which the quality of service is essential in their operations. This will imply a remarkable effort to define new organisational models. Also the quality of service will have to be assured by new contract-based conditions involving the key partners. Perhaps a best effort network at lower costs will survive for those users with simpler needs or who are unable to afford the costs of the network with guaranteed level of performance.