GCSEC, ICANN and DNS-OARC to meet in Rome to discuss the security of the DNS

October 18th workshop to focus on methods of protecting the Domain Name System.

The DNS is a fundamental element of the Internet and all modern IT systems. It is the world's largest distributed IT archive and is used billions of times each day. Without the DNS, we would not be able to send e-mails or access the web. We could suffer breakdowns in critical infrastructures, such as banks, electrical systems, transportation and telecommunication services.

A new study by the conducted by GCSEC reveals that attacks on the DNS could affect our safety and well-being.

Given the importance of DNS security, the GCSEC Foundation has organized an international workshop, DNS-EASY 2011, to be held on 18 October in Rome with the participation of the world's leading Internet, DNS and Security experts. Organized in collaboration with ICANN and DNS-OARC, the workshop will host a debate on current DNS problems, possible future shortcomings, and solutions designed to guarantee DNS health and security today and in the long term.

The Director General of GCSEC, Andrea Rigoni, addressed the need for the workshop at this time.

"DNS is a vital element for Internet and its critical Infrastructures. It will accompany us through the next 100 years. Guaranteeing its security and stability is a major priority. To do so, we require instruments of measurement and control. Without them, security cannot be guaranteed. Would you define secure a Nuclear Reactor or an airplane not equipped with measurement and control instruments?

With the studies conducted by GCSEC, and with the DNS-EASY workshop, we are making major progress toward new systems of guaranteeing DNS security. What is more, with the adoption of DNSSEC, the DNS community will provide the world with the most secure and largest distributed database available accessible to all, offering opportunities for new and innovative digital services. Managing the digital identities of people, systems, and objects is just one example."

CEO of Poste Italiane and Chairman of GCSEC, Massimo Sarmi, who will open the workshop, will stress the importance of having universal access to secure digital services. With the creation and the support of the GCSEC foundation, Poste Italiane's aim has been to contribute to the study and solution of global problems, such as Internet security.

Paul Mockapetris, the "father" of DNS, will illustrate the importance of, not only keeping DNS secure, but also how DNS can be used to guarantee greater security for web users and for digital services.

Paul Vixie, the inventor of BIND – the world's most widely used DNS server system – will present the results of the first year of operations of the Response Policy Zone, opened in 2010 by ISC. The aim of the Response Policy Zone is to publish information on the reputation of domain names, and is set to be a fundamental element of DNS security both today and in the future.

Richard Lamb, DNSSEC development and policy manager for ICANN, will offer a picture of the current DNS security situation in regards to the development and spread of DNSSEC, explaining how many incidents can be avoided.

The workshop also will include a presentation of studies conducted in twelve separate international research centers in nine countries; the Netherlands, Japan, Italy France, USA, Czechoslovakia, China, Canada and Korea. The results include models for a healthier, more secure DNS, methodologies and applications for a healthier, more secure DNS, and management and viability of DNSSEC. The details of the technical solutions put forward by researchers at the workshop will be compiled and published by GCSEC, and distributed during the conference (will be also available online at http://www.gcsec.org).

Set to take place at the end of the DNS-EASY workshop is the Third Global Annual Symposium on DNS-SSR (19 and 20 Oct.), also jointly organized by GCSEC, ICANN and DNS-OARC. The DNS-SSR part of the workshop on the second day will be held behind closed doors and is reserved for the leading DNS and cyber security stakeholders and providers (Verisign, RIPE-NCC, Nominet, Nominum, Affilias, Google, CAIDA, ISOC, all the providers of the main ccTLD, Microsoft, ISC, GCSEC and many others). DNS-SSR is intended to offer an opportunity for discussion of issues that have a direct impact on the future and evolution of DNS security, resiliency and stability. Specifically, this year's symposium will focus on themes such as the evolution of DNSSEC, and the steps needed to build a more secure Internet, DNSSEC as a service enabling new applications (for example PKI), the current, controversial problem of filtering at DNS and DNSSEC level, and measuring DNS security, stability, resiliency and performance levels.

Global Cyber Security Center Foundation (GCSEC): An international not-for-profit foundation created by Poste Italiane, with the participation of Enel Group, Mastercard and Almaviva. The Foundation deals with studies and advanced research on the theme of Cyber Security and works daily on international levels studying how to improve the security of citizens, governments and businesses.

Based in Rome, the Foundation regularly organizes events and workshops of international scope on Cyber Security issues, such as the security of the internet infrastructure, electricity networks (SCADA and Smart Grid), cloud services and payments. It also deals with studies on governance and security management at both government and international levels.

The Internet Corporation for Assigned Names and Numbers ("ICANN"): A not-for-profit, public-benefit corporation created in 1998, with participants from all over the world, dedicated to keeping the Internet secure, stable and interoperable. The ICANN mission is to coordinate, at the overall level, the global Internet's systems of unique identifiers and, in particular, to ensure the stable and secure operation of those identifier systems. In particular, ICANN coordinates the allocation and assignment of the four sets of unique identifiers for the Internet (Domain Names, Internet protocol ("IP") addresses, autonomous system ("AS") numbers, and Protocol port and parameter numbers). Moreover, ICANN coordinates the operation and evolution of the DNS root name server system and the policy development appropriately related to these technical functions.

DNS Operations, Analysis, and Research Center (DNS-OARC): Brings together key operators and researchers on a trusted platform with the aim of coordinating responses to attacks and other concerns, sharing information and learning together.