Draft WGIG issue paper on Network and Information Security

This paper is a 'draft working paper' reflecting the preliminary findings of the drafting team. It has been subject to review by all WGIG members, but it does not necessarily present a consensus position nor does it contain agreed language accepted by every member. The purpose of this draft is to provide a basis for the ongoing work of the group. It is therefore not to be seen as a chapter of the final WGIG report, but rather as raw material that will be used when drafting the report. This draft working paper has been published on the WGIG website for public comment, so it will evolve, taking into account input from governments and stakeholders.

Introduction

Network and Information Security is becoming increasingly important as Information and Communication Technologies (ICT) develops to be the backbone of modern societies and economies.

Whilst only a couple of years ago Governments regarded security- including network and information security - as purely national domain, security has entered the political mainstream of public policies during the last years.

In fact, security may be seen as a *merit good*. It induces, when put in place by each individual, externalities to the Society as a whole bringing benefits to other people as well as to the person concerned. Education and health-care are two other common examples of goods where general interest and overall Societal benefit emerges (when people are healthy it will help to reduce epidemic disease spreading, and when they are educated it will increase the economic growth).

The issue of how exactly should Society provide, and bear the costs of, this type of goods is highly relevant from an economical point of view. The recent liberalisation taking place in many sectors related to communication infrastructures and the new regulatory framework raise important issues on the balance that has to be strived between the supply of security as a “public policy” and the need to ensure a competitive and open market relying on the Internet as infrastructure.

Network and information security can be looked at from different angles. One can stress the network and information security aspects or, from another angle, one can use the perspective of the users (i.e. business or the citizens/consumers). A third angle looks at the implication security has in the governance/management of networks and information.

Issue (what?)

Please identify an issue listed on the table “Inventory of Public Policy Issues” and describe this issue

Network and Information Security:

The Internet has proved to be remarkably resilient to date, mainly because of its decentralised infrastructure and the highly responsive culture within the Internet community to any real or perceived threats to the infrastructure. The style and scope of the threats posed to Internet-based systems are changing however.

The increasing dependence of economies on the Internet however, has also resulted in an increasing potential for serious economic and social damage if the Internet’s stability were to be threatened. To date, the operators of the Internet’s infrastructure have proved reasonably responsive to such threats but governments may find it appropriate to take additional steps to contribute to reinforcing the Internet's long-term reliability.

Threats to the proper functioning of networks concern different building elements of the network: physical infrastructure, transport protocols, server and client software, etc. To increase robustness and dependability, different components of the Internet need to be reasonably secure: network nodes, (routers, switches, management tools), the transport infrastructure, the traffic that flows on the network and the software running on hosts and connected devices.

Availability and security are essential requirements for network operators. The commonly accepted reference for high availability telecommunication systems is an unavailability rate of less than 0,000005 per year, or bout 3 minutes per year.

In order to deliver a full functioning service, the information exchanged on networks or stored in various servers has to comply with strict security requirements. Network normal operation need to guarantee integrity, confidentiality, authentication, availability and non-repudiation. Security and dependability of networks embrace a broad area of issues like (1) Network organisation and management; (2) Increase complexity and need for scalability, in particular with evolution to networks supporting full-mobility; (3) Evolution towards intelligent, active networks (and use of mobile code); (4) Vulnerability to malicious code and denial of service attacks; etc. The following is a (non-exhaustive) list of challenges:

1. Core Internet Infrastructure (switching, rooting devices)

The main challenge is to protect the end-systems (edges) not so much the "core" infrastructure which is seen as less vulnerable. The sensitive core network elements are under clear responsibility and so there are reasonable business incentives to provide security and reliability. For example, *routers* still need to be protected against weaknesses of BGP protocol but operators will respond and fix the issues if it is essential for their business.

2. Internet Protocols

It has been recognized that Border Gateway Protocol (BGP) responsible for routing between networks contains vulnerabilities like, for instance, allowing false originator of inputs to routing registries. As far as the Domain Name System (DNS) is concerned, current challenges are the authentication of name servers, the assurance that the information in the DNS servers has not been maliciously altered (cache poisoning) and the stable and reliable availability of the root zone file. Another source of security concern is Denial of Service (DoS) attacks on DNS root servers that can strongly upset the normal functioning of the Internet.

3. Software for network services and applications

Software plays a critical role in modern digital networks. It spans from operating systems to communication middleware, to end-user applications. In this field, the main challenges are the security gaps in software applications and services. The trend is more vulnerabilities exploited in shorter time. On the other hand, patch management is complex and costly. Software bugs and errors result in too many patches, leaving many systems with holes. Moreover, the edges of the network are not easily patched and automatic enhancements/updates may interfere with consumer privacy and freedom of choice. Few (or single) technology providers of basic software infrastructure may raise problems of lack of diversity and, therefore, resilience to certain targeted attacks.

4. Future challenges: increase complexity and new vulnerabilities

Recent events show that Internet has a degree of recovery (self-healing), but new challenges are already perceived like (1) Increase of complexity and a tendency to put more “intelligence” and specification into the infrastructure; (2) More heterogeneity with the introduction of new technologies like RFID, mobile, wireless, VoIP, IPTV; (3) Multiplicity of devices, with different capabilities used with different user electronic identification and authentication mechanisms; (4) Diversity of actors and operators as result of liberalization of the telecommunication market and the convergence mobile/broadcasting, using IP technology and links to the global Internet.

5. Availability and reliability of information concerning threats, vulnerabilities and best practices

It is recognized that there is the lack of international standards, procedures and mechanisms to share threat and vulnerability data mainly due to traditional national and business concerns. As security incidents are not that frequent or easy to observe (collect relevant data), it is essential to have mechanism to make data available to the community. Together with common measurement techniques, benchmarking and assessment of progress would be more reliable. Prevention and prompt actions is crucial at EU and international level. Information should be available to the ones that need it to protect their systems.

6. Protection of Critical Information Infrastructure

National efforts may not to be sufficient to protect critical infrastructures due to different levels of inter-dependencies. Attacks on critical infrastructure are done through global interconnected networks (such as the Internet). Critical infrastructures are inter-connected and in some cases are heavily relying on the connectivity provided by electronic communication infrastructures. Monitoring systems of critical infrastructures are based on standard operating systems which contain vulnerabilities.

7. Mutual recognition and technical interoperability of identity and authentication mechanisms

For public services, security aspects like the protection of identity, authentication and privacy are mainly addressed at national level. The issue is that these security aspects should not be only addressed at national level but at regional and at global level. However, a careful analysis of costs involved in deploying and maintaining such infrastructures is essential. A key challenge is to better protect the end-user while using electronic identities, keeping freedom of choice and protecting privacy.

8. Lack of coordinated network and Information Security Policies

The issue is that without a co-ordinated international Network and Information Security (NIS) policy framework, each country will develop its own framework. The different plans might results in inconsistencies and may impact negatively on the overall effectiveness of security measures.

9. Lack of measurement metrics for threats and related risks

There is a lack of coordinated method to evaluate and measure threats and vulnerabilities. Lack of reliable method to measure the risk.

10. Awareness and Education

Security is also a distributed responsibility highly dependent on the actions of the ‘average user’. The user is often the weak link of security. It is essential to promote effective communication links to users (business and citizens) preparing them to develop and implement basic security policies

Attribution to category / ies

Please attribute the issue to one or more of the five categories on the table “Inventory of Public Policy Issues and Priorities”.

Stable and Secure Functioning of the Internet

SWOT Analysis

Please assess the strengths and weaknesses of the present system (internal factors). What are its opportunities and threats (external factors)?

Rather than strengths and weaknesses one has to look at the right balances to achieve in Network and Information Security. Network and Information Security raises a number of policy tradeoffs. In setting up policies related to secure, dependable network and information platforms, the right balance between the following (non-exhaustive) list of issues is essential:

- **Economics on Network and Information Security**: who should bear the costs of security in complex infrastructures? Should governments be actively involved and provide public resources or should private industry guarantee, by itself, robustness of infrastructures and services, incorporating security in their business models?

- **Privacy versus Accountability/Security**: how to reach an acceptable balance between privacy and accountability of users of electronic communication and information services?

- **Accountability/responsibility of industrial agents**: what kind of incentives, (regulation, co-regulation, etc.) should be put in place to develop sustainable approaches towards a better security in design and operation of infrastructures and services by the industrial actors concerned (manufacturers, network operators, access and service providers)?

- **Closed versus open standards for security enabling technologies**: what can be the impact on competition by the introduction of technologies related to security in markets with strong externalities?
- **Assurance and certification** – what is the relevance of industry-led standardisation and certification processes related to security technologies?

Actors (who, with whom?)

Please identify the main actor (government, private sector, civil society or international organization) dealing with this issue and who else among the relevant stakeholders is involved.

Different actors are involved, and interact with each-other in setting-up Internet based communication and information services:

End-Users, Content and Service Providers, Internet Service Providers (ISPs), Access Network Providers (ANPs) Internet Backbone Providers (IBPs), technology providers (manufacturers), infrastructure software, communication software and application software providers. Governments are also key actors by virtue of the various legislative initiatives taken to promote network security and in particular to provide for criminal sanctions against those who attack networks.

Forums (where?)
(a) who participates
(b) nature of forum

Please describe where this issue is being discussed or dealt with? Do these meetings make decisions? What is the nature of possible decisions? Who participates in discussions and decision-making processes? What are the decision-making procedures?

Governance Actors:

There are numerous governmental and inter-governmental organizations that are active in fields affected by the development of the Internet. The key governmental organisations in this respect are the UN and its various agencies (especially the ITU and WIPO), the Council of Europe, the OECD, and regional bodies such as the EU. There are also very many existing non-governmental organisations active in the field of Internet governance, organisations that develop or implement common policies to ensure Internet inter-operability and stability and to facilitate the introduction of new services and technologies.

The non-governmental actors include various groups of network operators and service providers. RIRs such as RIPE (*Réseaux IP Européens*), for example, bring together those who run IP networks and the DNS (*Domain Name System*) services in this region. In addition, other regional constituencie ssuch as the EOF (*European Operators Forum*) tend to meet alongside RIPE. There are other groups of course such as NANOG (No*rth American Network Operating Group*) and NordNOG (*the Nordic equivalent*). EURO-IX (*European Internet Exchanges*) brings together those who run exchange points in Europe. Elsewhere in the world, other Internet exchange bodies and organisations are responsible for providing similar services.

Domain name bodies:

ICANN (*Internet Corporation For Assigned Names and Numbers*): ICANN’s role in the administration of domain names and Internet addresses is mainly restricted to providing a forum for bottom-up policy making by the key actors who actually operate networks and DNS resources. They do however have a security and stability advisory committee that advises the ICANN Board on issues related to naming and addressing issues.

Council of Europe cybercrime convention: provides a common criminal policy aimed at the protection of society against cybercrime, thereby contributing to the effectiveness of sanctions against criminal attacks on information systems via the Internet.

Other organisations to be referenced are those concerned with registering domain names, the country code Top-level Domain (ccTLD) registries and the generic Top Level Domain (gTLD) registries. The former organisations register names under dot.be, dot.es, dot.fr, dot.de, etc., while the latter register names under dot.com. dot.net, dot.org etc. Most ccTLDs also belong to regional organisations where they exchange best practice, while each is responsible for their own local policy, developed and implemented locally in the context of national regulatory provisions and government policies.

Standardisation bodies (non-exhaustive list):

IETF (*Internet Engineering Task Force*) is one of the building blocks of the Internet. It has been, for almost 20 years now, the place where the major technological developments have been introduced

W3C (*WWW consortium*) was founded in 1994 to cover the development (standardisation) of the applications running over the Internet network infrastructure. The Web is an application built on top of the Internet and, as such, has inherited its fundamental design principles.

Governance mechanisms (how?)
(a) objectives of the rules system
(b) content of principles, norms and rules

Please describe the overarching objectives of the rules system or norms in question. What is the actual content of the principles, norms and rules designed to achieve these objectives?

Security and stability is a concept covering a huge range of different security requirements depending on user perspectives. To a large extent, individual users and network managers make their own decisions about the level of security they want to have (and are willing to pay for). This part of the process does not have a “rule system” in the sense of governance. Where “rule systems” can apply is when we are dealing with legislation and standards making.

In relation to standards, the IETF (the Internet Engineering Task Force) promulgate RFCs (request for comments) that result in the widespread uptake of commonly agreed approaches to implementing technical objectives. They are not mandatory standards however, nor are they “adopted” in any formal sense.

IETF includes the open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

The whole process leading to an approved *Internet Standard* is quite complex and hierarchical in the sense that the proposed standard (technology) is checked and filtered at various levels. It can take several years to publish a standard but that does not mean early implementations of certain technologies cannot be released and publicly used in advance. The IESG (Internet Engineering Steering Group), consisting of the directors of all working groups, has the role of checking, approving or rejecting technical proposals for standards.

The IAB (Internet Architectural Board) provides architectural guidance to IETF technical work and has the role of approving new working groups. The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the Internet Society (ISOC) to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters.

Originally, the Internet Assigned Number Authority (IANA) had control over numbers assigned, and set the policy. In late 1998 a new organisation was created to handle address assignment. Named the Internet Corporation For Assigned Names and Numbers (ICANN), the organisation sets policy and assigns values for names and other constants used in protocols as well as addresses

Adequacy measured against criteria / benchmarks set out in Declaration of Principles:

(a) multilateral
(b) transparent
(c) democratic
(d) capacity to address Internet governance in a coordinated manner
(e) multi-stakeholder approach

(f) other

Please assess whether the mechanisms described above are adequate when measured against the criteria or benchmarks set out in the Declaration of Principles. Are they multilateral, transparent and democratic? Are they addressed in a coordinated manner? Are they based on a multi-stakeholder approach? Are there other principles they respect or should respect?

Security is a multilateral problem but few multilateral fora exist. Standards making bodies such as the IETF do operate transparent mechanisms for policy making and are democratic in the sense that a) anyone can participate b) meetings and proceedings are open and c) RFC's only tend to be implemented generally when the majority of actors involved agree on their usefulness.

The IETF has so far proved to be a reliable and efficient mechanism for the promulgation of Internet standards. The operational approach of IETF discussions and the non-bureaucratic structure allow for Internet standards to be made in "Internet time". Anyone can participate in IETF meetings and discussions, although it is noticeable that very few governments chose to participate on an active or regular basis..

Additional comments

Please make any additional comments you may wish to make with regard to this issue.

There are many different activities running in parallel during IETF meetings and at least 15 working groups work on issues related with network and information security.

Security is one of the key IETF areas in terms of intensity of work measured by the number of delegates attending the working groups (WG) sessions. However, IETF's scope is much wider as there is a great deal of work addressing other technological areas like IPv6 deployment, Mobility and Wireless AdHoc networking, Transport of Multimedia with QoS, etc. The working groups addressing security are in different maturity stages. Some are three and more years old and some others are just initiating activities. They all respond to the need to develop new tools and methods or revise exiting ones. New work in IETF can start only if there is enough quorum and support from developers.

Internet architects based their design choices on flexibility so that the whole system could evolve by incorporating innovation. This principle is called *design for change*. Recent literature points out that while Internet is established and *natural forces* opposing change become dominant, the above principle is put in danger unless there is explicit action to preserve the ability to design for change.

Another important design principle being questioned regards *transparency*. *Transparency*, in this context, means that the only task for the network is to transport information between two remote nodes or peers. The network processes packets to ensure transport optimization and robustness while leaving the information and application levels untouched. This is an important assumption that allowed many innovative end-to-end applications to be created without developers having to be much concerned with underlying network complexity.

Today's growing concern with security induces users and network operators to distinguish between good and bad network traffic with new devices to filter hostile traffic (firewalls). These architectures go against full *transparency* of the network. These devices are often configured as filters, without intelligence or the capacity to adapt, offering some aspects of security but leaving many others unsolved. Also on this point recent literature points out the imperfection of certain architectures that approach security in a maximalist way without flexibility and breaking essential design principles of the Internet.

Other developments, not necessarily related to security, may lead to increasing intelligence within the network. So, the Internet of tomorrow may develop in a balance between full transparency and some kind of embedded processing within the network.