Vulnerability Of Systems in Internet Relationship

Vasile Baltac

167 Calea Floreasca

72321 - Bucharest

ROMANIA

E-mail: Vasile.Baltac@softnet.ro

Abstract: Internet tends to become the largest man-made system, a global event with direct implication on globalization. The information content of Internet rapidly grows. Despite of the fact that routings, apparently chaotic, show a certain degree of connectivity and some self-organizing features, numerous elements of vulnerability are present. The paper reviews some of the research directions in Internet studies and an approach to reduce vulnerability is proposed.

At Internet micro level vulnerability is mainly under control as the complexity is not too high. Vulnerability at macro level results from the architecture of Internet as a network of unreliable elements and from induced incidents. The latter grow exponentially and the attacks are in the forefront of vulnerability. The e-Business development brought the necessity of a much higher level of security.

The quick development of Internet has not allowed countering the human factor in vulnerability. This is why the paper raises the question on *the study of human society as a source of solutions for vulnerability control.* Solutions may be found by analogy with human society confronted itself from the early stages with vulnerability. Various solutions have been found from fortified constructions to sophisticated alarm systems. But to the alternative to safe-proof every house the society opted for laws and law enforcement at community level. This is why the author considers that *the Internet has to go from almost an absence of regulations to local and global laws.* Regulations could reduce vulnerability at much lower costs than the technical solutions. The Internet world will become global, democratic and safe through both technical approach and national and international laws. The summary of the paper: The Internet phenomenon; Research studies on Internet; Elements of vulnerability; Human interaction as vulnerability element.

Keywords: World Wide Web: this paper is posted also on http://www.softnet.ro/vb/papers

Dr **Vasile Baltac** has a 40 -year long research background. He published books and papers on computers, software, information technology and society, management, industrial development. For more than 25 years, he held managerial positions in the electronics & IT industry. In 1984 he received the Romanian Academy's Prize for works in software engineering. A holder of Senior Research Fellow degree since 1974, Dr. Baltac is now University Professor, teaching MIS and Strategic Management of Information.

He is a Senior Member of the Institute of Electrical and Electronic Engineers – IEEE and President of the Romanian Association for Information Technology and Communications.

1. The Internet Event

The Internet network of networks becomes the largest man-made system. With tens of millions of servers, hundreds of millions of users and a data traffic, expected to surpass, since 2002, in the US, the voice traffic, Internet can be considered a major event that reflects on scientific, technical and business perspectives the evolution of human society at the end of the 20th century and the beginning of the 21st century.

It is to be said that the world telecommunications system has reached a telephone line density of 17% after 160 years of evolution. The world density of Internet usage has reached 7% in only 20 years.

We may consider Internet as a global phenomenon with an impact on globalization. Only accidentally can we notice white spots on the map in Figure 1 displaying world distribution of information technologies, communications and Internet [1]. The white spots are due less to technical difficulties and more to political and social considerations [2,3].

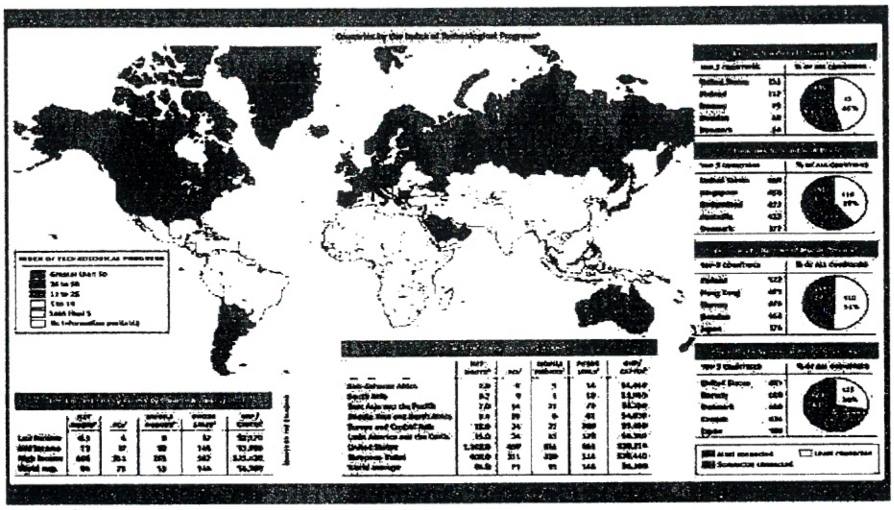


Figure 1. The World and Internet Development

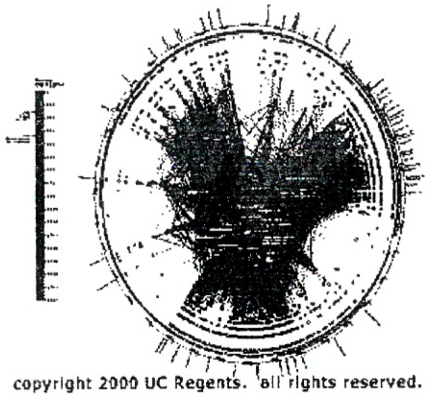
2. Internet-related Research

Despite the unusual quick Internet evolution, many research studies refer not only to new technologies, architectural aspects, standards and interaction with and intra- system(s), but also to vital topics for Internet future, mainly topologies, complexity mastering and vulnerability.

3. Volume of Information on the Internet

The volume of information stocked and accessed on the Internet grows at a very high rate. Some calculations by the author show that this volume could be estimated now at 10^{16}-10^{17} bytes. Out of it 50% is on move, 40% locally and 10% in wide areas.

Apparently the routings in this information ocean should appear with high dispersion. However, recent research shows that a concentration of connectivity is present. CAIDA of University of California at San Diego proved a concentration of connectivity of ISPs. The experimental graph of Figure 2 [4] reflects the orientation to other ISPs of more than 1 million links from hundreds of thousands of IP addresses. One explanation could be based on the US concentration of large ISPs, but the phenomenon will persist for reasons related to the costs of implementation of large data warehouses, preventing excessive fragmentation of them.



copyright 2000 UC Regents. all rights reserved.

Figure 2. Concentration of Connectivity

4. Internet Topology

The Internet nodes are actually link elements between information broadcasters and receivers. The probability of a node to be linked with k other nodes is given by a power law:

$$P(k) = \sim k^{-\lambda}$$

where λ is approximated at the value of 3.

Research on Internet topology shows in the apparent chaos of the networks scale-free characteristics and self-organization features.

Barabasi et al [5] prove that the diameter of *www*, defined as the median of shortest distances among two sites, was in the year 2000 not larger than 19 links. Due to its logarithmic relation to Internet volume, even at a 1000% growth of *www*, the number of links will not exceed 21.

Zipf's Law

Proposed for towns in 1949, the Zipf's law shows that the dimension of an event is related to its rank as follows:

$$P(r) = K * r^{-q}$$

where r is the rank of the event, P its dimension and K a constant.

The value of q was determined as 0.93.

The Zipf's law was revived for Internet and a correlation of GDP with *www* dimension for a certain country or world region was proved [6] (Figure 3).

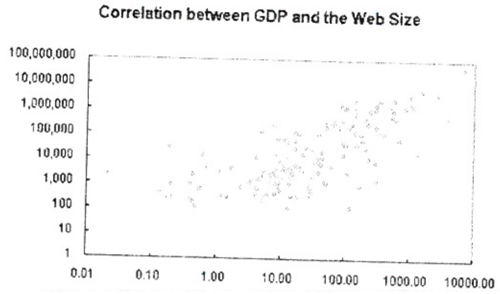


Figure 3. GDP and *www* Size Correlation

Studies on Vulnerability

An Internet type system is vulnerable. As Internet is a rapidly growing system of systems, with a quite unreliable infrastructure, there are many vulnerability elements that have generated their study enterprise.

Some of these vulnerability elements will be discussed.

5. Elements of Vulnerability

Internet system vulnerability is higher than the vulnerability of preceding systems. This has been true at first as the volume of information is much higher, compared with other systems. Then the growth of the

Internet has been fast and it has not happened in conjunction with a special approach to limit vulnerability. It seemed to be important at a certain stage to be present on Internet, and less important to be secure.

In addition to classic vulnerability, the Internet experienced the software attacks induced or accidentally produced. The first incident reported in 1988 was the so-called Morris Worm [7] and was followed by a quick rise of incidents of this type and subsequently by a diversity of other types.

It is well -known that the information can be lost, stolen, modified, unproperly used and illegally decrypted. It is possible to lose the integrity, the confidentiality and the availability of data.

Vulnerability aspects are different at micro- and macrosystem levels.

Vulnerability at Microsystem Level

Vulnerability is controllable at microsystems level, as the complexity is enough small. The sources of risk are the hardware, the software and the databases.

As regards the hardware, beside the current problems generated by the intrinsic nonreliability of system components, the vulnerability comes from natural disasters (storms, flood, earthquakes, etc.), electricity supply breakdowns or spikes and vandalism.

As regards the software, the applications and the databases, the vulnerability comes from theft, data alteration or destruction, computer viruses and non-intended accidents.

The reduction of vulnerability risks at microsystems level is possible through security measures of access to data control and through program real robustness.

This integration of security measures is done with a certain cost which is lower as the measures are taken earlier in the design and implementation phases, as shown in Figure 4.

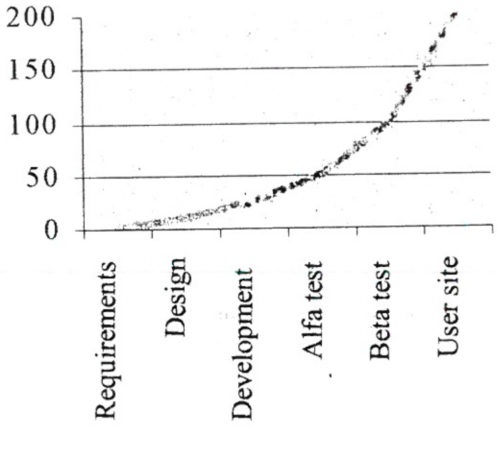


Figure 4. Cost Multiplying Factor

Security Measures

There are numerous methods to reduce vulnerability. Among these the design with security features, separation of functions, network checks, encryption and firewalls.

The use of such methods significantly increases the proofing of systems against perturbation and attacks.

Contingency Plans

As full avoidance of vulnerability problems cannot be achieved, the adoption of contingency plans is necessary. These plans provide efficient solutions to various breakdowns or attacks.

Unfortunately, this kind of contingency plan is resorted to very seldom.

The Cost of Security Measures

The Internet networks are made up of unreliable and vulnerable elements. The cost of security improvement measures appears to be high, and in fact it is high for the users being dependent on the desired level of security, as shown in Figure 5.

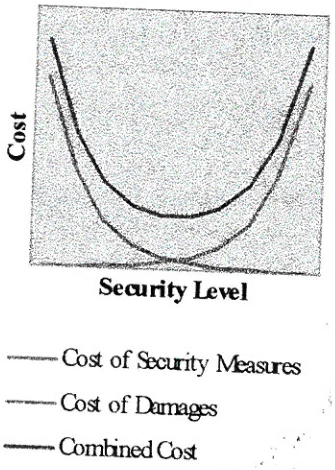


Figure 5. The Cost of Security Measures

The cost of potential damages gets lower as a function of the security level. This cost is described by the formula:

$$C_t = \Sigma\ (C_1xP_1 + C_2xP_2 + ... + C_nxP_n)$$

where *Ct* is the cost of potential damage, *Ci* the cost and P_i the probability of occurrence of the damage *i*.

An economic optimum could be found by calculating the combined cost of security assurance for the microsystems as represented in Figure 5.

Communication Channels Vulnerability Elements

Internet has grown mainly over existing communication networks. The traditional communication networks prove to be, however, the most vulnerable component of Internet. Unsecure data exchange protocols are added to the low reliability of communication lines. Table 1 shows a comparison of various media used in communications, including Internet, from capacity, vulnerability to electromagnetic interference and availability point of views.

Table 1. Comparison of Communication Media

Media	Capacity	Vulnerability to Electromagnetic Interference	Comparative Cost	Global Availability
Metal Wires	Small	High	Small	General
Coaxial Cable	Average	Small	Average	Little
Microwaves	High	Small	High	High
Optical Cable	High	Zero	High	Limited

Vulnerability Elements at Macrosystem Level

The Internet vulnerability at macro level is a result of its architecture as a network of microsystem level vulnerable components, and induced perturbations. The sources of incidents are non-voluntary or provoked attacks.

The classic types of incidents are well -known: attempts, scanning, user account or root corruption, packet data capture, denial of service, fraud, malign code use, attacks on infrastructure.

The rise of incidents takes place exponentially. It is true that intrinsically the systems show some degree of robustness [7]. In many situations the system downgrading (partial functioning) reduces vulnerability.

The main vulnerability element has become the attacks. Only in the US, in the year 2000, some US$337 million were spent to repair damage caused by attacks.

The main causes of this type of vulnerability are unreliable nodes and the use of unencrypted communication. It is true that in the initial phases of the Internet development, there were no major applications to require reduced vulnerability. The growth has been fast and has not been accompanied by dedicated security measures. The staff on user side has also lacked sufficient training.

The development of e-Business claimed a new, much higher, security level. Encryption has become the tool commonly used by hundreds of millions of users as compared with very few in the pre-Internet era.

Technically the speed of growth and especially the short time have not allowed the efficient counteraction of human factor influence on the increase of Internet vulnerability.

6. Human Interaction in Internet As A Factor of Vulnerability

Systems without humans behave differently from systems with humans. On the Internet there are today 50 million servers and 410 million people. Human interaction becomes in this way the main factor of vulnerability. The Internet size is already comparable, from the perspective of the complexity of interaction, to human communities.

One may then question about the opportunity *to study the human communities as a source of solutions for the decrease of vulnerability.*

The vulnerability of human society is also very high. The human society as a system has in its nodes the people, who are quite unreliable. The similitude with the Internet goes even further: much redundancy, vulnerable communication and increasing vulnerability of stored information.

The trend towards globalization intensifies the force of attacks in the human society, as well as it is prominently manifested on the Internet.

A Point of View on Reducing the Vulnerability in Internet relationship

It is hard to disagree that the vulnerability of systems in relationship with Internet is high and increasing. There are enough technical solutions to counteract, but they are expensive, difficult to spread and their success will be limited.

Solutions could be found from the analogy with human society. The human society has been confronted since its advent with its vulnerability. Diverse solutions were found from fortified constructions and communities to the use of sophisticated alarm systems.

It is not a dilemma to decide whether in a community you have to have steel proof doors at every house or to use efficient public order forces. The human society decided early for an organization based on rules and laws, and on their enforcement.

The Internet world has to evolve from the absence of rules to national and global laws

The rules and laws can reduce vulnerability with much lower costs than technical measures can do. The Internet world could become global, democratic and safe by both technical measures and international ruling.

The opponents to this approach could invoke the spirit of free enterprise that has contributed significantly to the rise of Internet, and the difficulties any ruling will cause to its further development.

But as the Internet is used more and more in vast business, education, cultural and public administration applications, to ignore the vulnerability issues will bring more stagnation than insufficiently based regulations.

Through its global character the Internet asks for transborder global regulation.

REFERENCES

1. **Nua Internet Surveys, How many on-line**, http://www.nua.net
2. COFFMAN, K. G. and ODLYSKO, A.M., **The Size and Growth Rate of the Internet**, FIRST MONDAY PEER-REVIEWED JOURNAL ON THE INTERNET, http://www.firstmonday.dk
3. *** **Digital Planet 2000**, The Global Information Economy, WITSA, November 2000.
4. CAIDA, **Visualizing Internet Topologies At A Macroscopic Scale,** http://www.caida.org/analysis/topology/as_core_network/
5. BARABASI, A. L. et al, **Scale Free Characteristics of Random Networks: the Topology of the World-Wide Web**, Physica A, ELSEVIER SCIENCE B.V., 2000
6. SHIODE, N. et al, **Power Law Distributions in Real and Virtual Worlds**, Inet 2000 Proceedings, Internet Society, http://www.isoc.org/inet2000
7. CARNEGIE MELLON SOFTWARE ENGINEERING INSTITUTE, **Security of the Internet**, Fröhlich/Kent Encyclopedia of Telecommunications, Vol. 15.
8. REKA, A. et al, **The Internet Achilles' Heel: Error and Attack Tolerance of Complex Networks**, Physica A, ELSEVIER SCIENCE B.V., 2000.