Web Science for Security and Trust on the Web - Short Introduction

ERICE, 43rd INTERNATIONAL SEMINAR ON PLANETARY EMERGENCIES

Jacques Bus (www.digitrust.eu)

Since the World Wide Web blossomed in the mid-1990s, it has exploded to more than 15 billion pages that touch almost all aspects of modern life. Today more and more people's jobs depend on the Web. Media, banking and health care are being revolutionized by it. And governments are even considering how to run their countries with it. Little appreciated, however, is the fact that the Web is more than the sum of its pages. Vast emergent properties have arisen that are transforming society. E-mail led to instant messaging, which has led to social networks such as Facebook. The transfer of documents led to file-sharing sites such as Napster, which have led to user-generated portals such as YouTube. And tagging content with labels is creating online communities that share everything from concert news to parenting tips.

Few investigators are studying how the Web's emergent properties have actually blossomed, how we might harness them, what new phenomena may be coming or what any of this might mean for humankind. A new branch of science—Web science—aims to address such issues.

Web Science, looks to explain the evolution of the web as a complex organism and an independent ecology, through multidisciplinary analysis of the range of knowledge areas that converge in the web. These are mainly technological (how does the web evolve technologically), organizational (what standards and specifications support this evolution) and social (what use do users make of this technology).

There are also other areas involved in these changes, given that many economic, political and legal interests do not want to be left out of the evolution of the information society. Web science looks to provide a reference framework to ensure the proper analysis of all of these events from a range of perspectives and different levels of resolution, taking into account all the elements involved and the relationships established between them, with a clear multidisciplinary spirit to promote the participation of the widest possible selection of members of the scientific community.

The Web Science Research Initiative, WSRI, was created in November of 2006 with the main aim of proposing a new discipline, Web Science, to observe the web and all that that surrounds it. It defends the need to analyze what is going on inside and outside the web and, thus, be able to propose improvements and corrections. This idea requires combining disciplines that have, to date, been very disperse, such as IT, psychology, law or economics. This has led to a new professional profile, the Web Scientist, and, likewise, new academic needs. See: A Framework for Web Science (Berners-Lee et al., 2006) - the basic reference to Web Science.
(http://eprints.ecs.soton.ac.uk/13347/1/1800000001%5B1%5D.pdf)

WSRI (http://webscience.org/home.html) was an initiative of Tim Berners Lee and colleagues at the Massachusetts Institute of Technology together with by Wendy Hall, Nigel Shadbolt and others at the University of Southampton in England.

Thorough understanding of scale-free networks, gleaned by analyzing the Web, has also prompted experts to analyze other network systems. They have since found power-law degree distributions in areas as far-flung as scientific citations and business alliances. The work has helped the U.S. Centers for Disease Control and Prevention improve its models of sexual disease transmission and has helped biologists better understand protein interactions.

One of the last (and first) texts published is the provocative book *The Web's Awake*[i] (Tetlow, 2008) (http://www.thewebsawake.com/), which presents the web as a new way of life that we can no longer control. It provides a description of new web characteristics and types of behavior that we have not created, but which have emerged of their own accord.

Trust on the Web

Trust and trustworthiness are concepts which are at the basis of human existence. We use them intuitively and their assessments are invariably context dependent. But when we transpose these concepts to a digital environment, we can easily run into trouble.

O'Hara[ii], Luhmann[iii], Hardin[iv], Fukuyama[v], Putnam[vi], Nissenbaum[vii], O'Hara and Hall[viii] and a number of others have written about the concept of trust in general, and about its problems in the digital environment. Nevertheless, it is still insufficiently understood how trust on the Web can be made operational.

When analyzing trust in relation to technology we must make a difference between:

- Trust between persons who make extensive or exclusive use of digital technology for communication and transactions.
- Trust or confidence of people in the infrastructure of digital networks and systems they use for services, communication, data storage, services etc.

---

i Tetlow, 2008 - http://www.thewebsawake.com/

ii Kieran O'Hara Trust: from Socrates to Spin, Icon Books, Cambridge (2006).

iii Niklas Luhmann - Trust: A mechanism for the reduction of Social Complexity, in TRUST and Power: Two works by Niklas Luhmann (1979)

iv Russell Hardin (2002) - Trust and trustworthiness; Russell Sage Foundation, NY

v Francis Fukuyama, Trust: The social virtues and the creation of prosperity (1995)

vi Robert D. Putnam, Making democracy work: Civic traditions in modern Italy (1993)

vii Helen Nissenbaum - Securing Trust Online: Wisdom or oxymoron? (2001)

viii Kieran O'Hara and Wendy Hall - Trust on the Web; Some Web Science Research Challenges (http://www.uoc.edu/uocpapers/7/dt/eng/ohara_hall.html)

The problems with trust between persons in the digital society in comparison with the "old society" relate to

- the new ways and uses (incl. profiling and new business cases) of data collection, storage and processing.
- Identification, reputation, authentication and accountability have a different meaning on the Internet, also due to different jurisdictions involved in transactions.
- Increase of complexity through incomprehensible technology with insufficient assurance through certification and standardisation, and lack of transparency.

But such trust between people can only be obtained in our technological world if one also can have trust in the technology used to communicate and interact. Networks, systems and services must be *trustworthy* to a certain level, i.e. a person can have a certain degree of justifiable trust that the system or service will deliver in accordance to its description and promises, and that it will not perform actions that are not described, independent of the circumstances. Justifiable trust can be given through accountability (product liability), transparency on data processing and storage, technical system certification, and ex-post auditability, and authentication and identification, as well as tools to support this.

Security of the Web

The ICT based societal revolution will lead to essential changes in the balance of power, at the national level where citizens are having abundant information on the political processes which will be used in the democratic process, but also at the international level. Access to the Internet is empowering citizens to be better included in economic and political life, and to understand situations and ways of life in other cultures. We have seen the way Obama used the social networks in his campaign and we may expect that similar activities will be developed in the future to support governmental policy making.

ICT also allows international companies to organize themselves in ways that make optimal use of opportunities all over the world. This can all give a strong boost to economic development and growth globally, and particularly in low-cost countries. We see already large developing countries taking advantage and become important economic and political players.

However, as with every revolution in history, together with the opportunities and benefits there always comes a downside.

The information and communication infrastructures and services have become a critical part of our economies. They are extremely vulnerable, as the many attacks reported almost daily demonstrate. Most of our other critical infrastructures, e.g. energy, water, transport, financial systems are heavily dependent on ICT for communication and control. There is therefore a high risk of accidents or deliberate attacks on these critical infrastructures that may potentially lead to chaos and enormous economic losses. This includes intrusion and attack on systems and databases of National Security Agencies.

These vulnerability of our societal ICT systems and the systems dependent on it make these systems an easy target for attacks in times of war or by terrorists. Cyber crime is becoming a very worrying issue. The number of malicious and criminal code threats is increasing exponentially, with 1.6 million threats detected by Symantec in 2008. There is general agreement that there is reason for alarm about the security of the Internet. Current trends risk increasing fear for and rejection of the new digital world by citizens. It may have huge economic consequences if politics and technology are not able to deal with these negative societal developments.

World leaders are facing enormous and unparalleled challenges. Climate change, rapid changes in global economic power and energy security, to name a few other issues, need to be managed at the same time as the transfer to a digitally connected global world. There are fascinating opportunities (e.g. in the use of ICT for climate change or energy economy and security) and fearful risks.

It will need a solid multi-disciplinary scientific basis and strong and visionary global political leadership in the interest of all to build a future of freedom, security, creativity and prosperity.

Acknowledgement

I am grateful to Prof. Nigel Shadbolt (Univ. Southampton) for allowing me to use some of his material.