International Journal of Web Engineering 2015, 4(1): 15-18
DOI: 10.5923/j.web.20150401.02

Building the Trusteeship of Internet Users

Tahadray Jean Tsitaitse*, Cai Yong Quan, Crentsil Kofi Agyekum

Computer Science Department, Beijing University of Tech, Beijing, China

Abstract As people become more reliant on storing and sharing data with their mobile devices, these tech tools become more attractive targets for hackers," observes Anders Lofgren, product management vice president at data backup vendors. "What's worse is that mobile devices by nature are portable and small, making them even more vulnerable to being lost or stolen. Better technology alone won't be enough to slow the erosion of trust in the Web as agitated many scholars in the field of cloud computing. Ensuring trust on the Internet is the key to doing business on the Web, today, and in the future. From gathering information to performing transactions, it is more important than ever that people's experience online is one of confidence and safety. The extent to which a user trusts a website has the potential to color many aspects our lives. It can influence whether we believe a trivial fact, what medicine we seek, where we sign up for driving school, to which we give our master card information. As we surf the web, we are constantly evaluating the websites we see and deciding how reliable they are. We look for clean user interfaces, the lock icon that indicates encryption, and names us recognize. As users, there are many tools at our disposal to help us decide whom to trust. This paper seems to discuss the trend at which internet users and subscriber build trust on the World Wide Web and the effects of this trusteeship.

Keywords Internet, Safety, Trust building, Internet users, Subscribers

1. Introduction

The extent to which a user trusts a website has the potential to colour many aspects of our lives. It can influence whether we believe a trivial fact, what medicine we seek, where we sign up for driving school, to which we give our credit card information, and so on. As we surf the web, we are constantly evaluating the websites we see and deciding how reliable they are. We look for clean user interfaces, the lock icon that indicates encryption, and names us recognize. As users, there are many tools at our disposal to help us decide whom to trust.

For instance, trust often relies on subtle interface cues. A 2004 study of patient's evaluation of medical websites found that certain UI elements had a dramatic effect on the perception of the trustworthiness. Over 94% of reasons cited for mistrust included UI features such as pop-up ads. Many popular websites use systems that allow the users themselves to control the reputations of other users. Users also rely on technical cues, such as the lock icon in the browser address bar, which indicates a secure connection.

These skills, however, are a double-edged sword. Online, we are all potential victims of charlatans, quacks, and identity thieves. These attackers have the same tools for building trust that legitimate sites have. We have trained ourselves to trust certain online sellers and banks based on many cues that can be abused. Trustworthy and untrustworthy entities alike can use professional-looking website design to promote user trust. The lock icon does not necessarily imply trustworthiness, because SSL certificates are extremely easy to obtain. Reputation systems can fool users or give them a false sense of security. Malicious sites often exploit this misplaced trust to lure unsuspecting users into providing sensitive information.

Through explanations and examples, we aim to show both how to trust is established on the Internet and how to decide which websites to trust.

The current trust deficit and ways to overcome it are the focus of a recent blog by Michael Moller, acting director of the UN Office in Geneva. It inspired this reflection on trust in an online world. According to sociologist Niklas Luham, 'a complete absence of trust would prevent us from even getting up in the morning'. Many of our daily routines presume trust. Trust not only makes our lives simpler, it makes societies richer, as Robert Putnam showed in his study on trust and the economic success of Renaissance Italy. The same logic applies to the success of Silicon Valley. Trust in institutions and in laws frees time for innovation and creativity. In many parts of the world institutions are weak and trust in them is low. A lot of energy is spent avoiding being cheated. Are current levels of mistrust greater than those of the past? Breaches of trust have been around since Adam and Eve's exploits in the biblical Garden of Eden. There has always been some failure to comply, and some abuse of trust. But, our times

* Corresponding author:
fahasoavajean@hotmail.com (Tahadray Jean Tsitaitse)

Published online at http://journal.sapub.org/web

and the Internet make trust more relevant. A significant part of our life takes place in online spaces, spaces which cannot be easily verified; this is an issue, particularly for those for whom 'to see is to believe'. With our growing interdependence, the stakes in trust (or the compensations we make in its absence) are higher.

2. Trusting in the Online World

Our online trust is machine-driven (mechanical trust). We perceive computers as another device that extends our capabilities. We demonstrate our trust in technical devices by our reliance on them. Just as we trust that our cars won't break down, and that they will bring us to where we intend to go, we also trust computers to complete the tasks we require of them daily.

In the wake of the Snowden revelations, trust in machines has evolved into a question of trust (or the lack thereof) in those humans who operate said machines. It is no longer about the competence of the machine - whether the Internet will function - but rather about the intentions of those operating it. But it is not only about intentions. It is also about systemic changes in how the Internet economy operates.

2.1. Systemic Challenge for Trust Online

The new Internet business model, as described in this illustration, poses systemic challenges for trust online. How transparent is this new model? What values are exchanged? Can we accept it?

2015-02-12-internetbussinesmodel01X2.jpg.

It would be naïve to believe that the richness of the Internet services we enjoy is paid for only by our Internet subscriptions (in Switzerland, it is CHF 49/month). The cost of 'free' Internet services is much higher in terms of innovation, software, and reliable services. The difference between our Internet subscription and the real cost has to be covered by someone. And it is... it is covered by the monetisation of our data by Internet companies through business models based on online advertising.

Does this unclear arrangement undermine our trust in the Internet and in those who provide its services? In most cases it does. But in some cases we make a tacit deal. For example, Google monetising my data in exchange for giving a free use of its Google Translate application. Whatever it earns by using ones data is fair compensation for helping to overcome lack of talent for learning foreign languages. This is an 'implicit deal' with Google. But one might not like this type of deal. It is not transparent and may undermine your trust in the Internet.

3. Ensuring Trust and Growth of the Internet Economy and Suggested Solutions

First, the way in which our data is handled (including the monetisation of data) should be fully transparent. This will help us to make more informed decisions on how we want to use Internet services and applications. Second, governments and public authorities should require that the terms of service (ToS) are clear, concise, and apparent, perhaps including a ToS in plain language. Governments could require that the ToS be clearly available and not hidden. In particular, companies should increase the font size when it comes to delicate stipulations in fine print. Yet even these practical steps may not solve the problem, since it is not only related to the bad/good intentions of the main players; it is related to profound changes in the business model that question some pillars of existing values and rules (e.g. privacy protection

All paragraphs must be indented. All paragraphs must be justified alignment. With justified alignment, both sides of the paragraph are straight.

3.1. Need for a New Internet Social Contract as a Key Solution of Building Trust

Modern society may need a new Internet social contract between users, Internet companies, and governments, in the tradition of Thomas Hobbes's Leviathan (exchange freedom for security) or Rousseau's more enabling Social Contract. The new deal between citizens, governments, and business should address the following questions: What should the respective roles of governments and the private sector be in protecting our interests and digital assets? Would a carefully designed checks-and-balance system with a lot of transparency be sufficient? Should the Internet social contract be global or would a regional and national contract work?

A social contract could address the main issues and lay the foundation for the development of a more trustworthy Internet. Is this a feasible solution? Well, there is reason for cautious optimism based on the shared interests in preserving the Internet. For Internet companies, the more trusting users they have the more profit they can make. For many governments, the Internet is a facilitator of social and economic growth. Even governments who see the Internet as a subversive tool will have to think twice before they interrupt or prohibit any of its services. Our daily routines and personal lives are so intertwined with the Internet that any disruption to it could signify a disruption for our broader society. Thus, a trustworthy Internet is in the interests of the majority. Rationally speaking, there is a possibility of reaching a compromise around a new social contract for a trusted Internet. We should be cautiously optimistic, since politics (especially global politics), like trust (and global trust), are not necessarily rational.

3.2. Top Key Reasons for Evaluating Internet Sources

There is no quality assurance when it comes to information found on the Internet: Anyone can post anything. In most cases, information found on the web has not been checked for accuracy. Not all web sites are created equal. They differ in quality, purpose, and bias. Some web sites have sponsors who pay for specific content to promote their products or ideas. The information is not impartial but biased. Some web sites voice opinions rather than make informed arguments. Some web sites are meant to be entertaining rather than informative. Some web sites seek to scandalize and breed controversy rather than provide reliable information. Some web sites are old and the information found there is out of date. The quality and format of information you find on the Internet may not be appropriate for use in the academic context. As a researcher, you are responsible for evaluating all your sources, including the information found on the Internet. Billions of people around the world do not trust the internet, claims European Commission vice-president Neelie Kroes. Following allegations that the German Chancellor Angela Merkel's phone was hacked, Ms Kroes said it was clear that trust was now missing. Speaking at the Cebit tech fair in Hanover, Ms Kroes said the future of the internet was based on trust. “Trust can never again be taken for granted," she said.

The next phase of the internet will be data-centred and connectivity-driven. Cloud computing, big data, the internet of things; tools which support manufacturing, education, energy, our cars and more. The internet is no longer about emails.

Internet Usage and World Population Statistics are preliminary for Dec 31, 2014. Demographic Population numbers are based on data from the US Census Bureau and local census agencies. Internet usage information comes from data published by Nielsen Online, by GfK, local ICT Regulators and other reliable sources. www.internetworldstats.com. Copyright © 2001 - 2015, Miniwatts Marketing Group.

3.3. World Growth of Internet Users

In the table 2 depict the tremendous growth of internet users around the globe. Table 1 clearly shows the internet usage and population statistics from year 2000 to 2015. Internet users increase every year due to the important role it plays within our personal life’s and our businesses.

Table 1. World internet usage and population statistics Dec 31, 2014 - mid-year update

World Regions	Population (2015 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population
Africa	1,158,353,014	4,514,400	318,633,889	27.5 %
Asia	4,032,654,624	114,304,000	1,405,121,036	34.8 %
Europe	827,566,464	105,096,093	582,441,059	70.4 %
Middle east	236,137,235	3,284,800	113,609,510	48.1 %
North America	357,172,209	108,096,800	310,322,257	86.9 %
Latin America / Caribbean	615,583,127	18,068,919	322,422,164	52.4 %
Oceania / Australia	37,157,120	7,620,480	26,789,942	72.1 %
WORLD TOTAL	7,264,623,793	360,985,492	3,079,339,857	42.4 %

Sources: sources.www.internetworldstats.com

Table 2.

World Regions	Growth 2000- 2015	Users %of table
Africa	6,958.2 %	10.3 %
Asia	1,129.3 %	45.6 %
Europe	454.2 %	18.9 %
Middle East	3,358.6 %	3.7 %
N/America	187.1 %	10.1 %
Caribbean	1,684.4 %	10.5 %
Australia	251.6 %	0.9 %

Sources: sources.www.internetworldstats.com

4. Conclusions

In 2014, nearly 75% (2.1 billion) of all internet users in the world (2.8 billion) live in the top 20 countries. The remaining 25% (0.7 billion) is distributed among the other 178 countries, each representing less than 1% of total users. China, the country with most users (642 million in 2014), represents nearly 22% of total, and has more users than the next three countries combined (United States, India, and Japan). Among the top 20 countries, India is the one with the lowest penetration: 19% and the highest yearly growth rate. At the opposite end of the range, United States, Germany, France, U.K., and Canada have the highest penetration: over 80% of population in these countries has an internet connection.

5th May 2014 – Releasing new statistics, the United Nations International Telecommunications Union (ITU) announced that by end 2014, there will be nearly three billion Internet users – two-thirds of them from the developing world – with mobile-broadband penetration approaching 32 per cent. “The newly released ICT information and communications technology table confirm once again that information and communication technologies continue to be the key drivers of the information society,” said Hamadoun I. Touré, ITU Secretary-General. Brahima Sanou, the Director of ITU’s Telecommunication Development Bureau, touted this newest record as a watershed moment in the world’s growing affinity for ICT. “Behind these numbers and statistics are real human stories. The stories of people whose lives have improved thanks to ICTs,” said Mr. Sanou, adding “our mission is to bring ICTs into the hands of ordinary people, wherever they live. By measuring the information society, we can track progress, or identify gaps, towards achieving socio-economic development for all.”

The research will extend to investigate the challenges associated with users and subscribers trust level of the internet.

ACKNOWLEDGEMENTS

I wish to acknowledge the entire stuff of Int. College of Beijing University of Technology. And also to Crentsil Kofi Agyekum and all friends in Beijing university of Technology (Bjut), for their massive support.

REFERENCES

[1] Cong Wang, Qian Wang Kui Ren, Ning Cao, and Wenjing Lou “Toward Secure and Dependable Storage Services in Cloud Computing” IEEE transactions on services computing, vol. 5, no. 2, april-june 2012.

[2] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou Jin Li “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing” IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011.

[3] Boris Tomas1and Bojan Vuksic2 “Peer to Peer Distributed Storage and Computing Cloud System” International conference on information technology interfaces, June-25-28, 2012, cavtat, Croatia.

[4] “Security and Privacy Challenges in Cloud Computing Environments” co-published by the IEEE computer and reliability ieee November/December 2010.

[5] Subashini S, Kavitha V., “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications (2011) vol. 34 Issue 1, January 2011 pp. 1-11.

[6] Balachander R.K, Ramakrishna P, A. Rakshit, “Cloud Security Issues, IEEE International Conference on Services Computing (2010).

[7] Kresimir Popovic, Željko Hocenski, “Cloud computing security issues and challenges,” MIPRO.

[8] Amazon.com, “Amazon Web Services (AWS),” Online at http://aws. amazon.com, 2008.

[9] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres1, Maik Lindner, “A Break in Clouds: Towards a cloud Definition,” ACM SIGCOMM Computer Communication Review, vol. 39, Number 1, January 2009.

[10] Patrick McDaniel, Sean W. Smith, “Outlook: Cloudy with a chance of security challenges and improvements,” IEEE Computer and reliability societies (2010), pp. 10-17.

[11] Sameera Abdurrahman Almulla, Chan Yeob Yeun, “Cloud Computing Security Management,” Engineering systems management and its applications (2010), pp. 1-7.

[12] Steve Mansfield-Devine, “Danger in Clouds”, Network Security (2008), 12, pp. 9-11.

[13] Anthony T. Velte, Toby J.Velte, Robert Elsenpeter, Cloud Computing: A Practical Approach, Tata Mc GrawHill 2010.

[14] Gary Anthes, “Security in the cloud,” In ACM Communications (2010), vol.53, Issue11, pp. 16-18.

[15] Lombardi F, Di Pietro R. Secure virtualization for cloud computing. Journal of Network Computer Applications (2010), doi:10.1016/j.jnca.2010.06.008.

[16] R. Rivest, the RC5 Encryption Algorithm[C]//the Second International Workshop on Fast Software Encryption, Leuven Belgium, December 1994: 86-96.