Consequences of Diminishing Trust in Cyberspace

Dipankar Dasgupta, Center for Information Assurance (CAE-R), Department of Computer Science, University of Memphis, Memphis, TN, USA
Denise M. Ferebee, Center for Information Assurance (CAE-R), Department of Computer Science, University of Memphis, Memphis, TN, USA

ABSTRACT
The cyberspace has become an integral part of modern day life—social, economic, political, religious, medical and other aspects. Without the availability of the Internet, many businesses, governments and society would not function properly. Presently, the Internet brings people together to share their ideas, and allow their voices to be heard. In its inception and ideally, cyberspace has no political, geographical or social boundaries; as a result it facilitates in globalization and the uniting of people all over the world by providing a means for communication. While the potential benefits of this interconnectivity are unlimited, this virtual world is also becoming hackers’ playground, nation-states’ battle ground, and a vehicle for propaganda and misinformation. In this article, the authors argue that with the growing threat of coordinated attacks, creation of complex malware and gradually diminished trust in freely-available information, the openness of the web and the global connectivity will no longer exist. If this trend continues, the Internet will be partitioned, users will rely on information and news through membership-based services, the information flow will be highly regulated by governments, online businesses and critical knowledge will only be shared among alliance of friendly nations.

Keywords: Cyber Trust, Cyberspace, Hacking, Malware, Misinformation, Targeted Cyberwar

1. CYBERSPACE: SECURITY, PRIVACY AND TRUST ISSUES

The cyberspace is increasing providing unimaginable benefit to the humanity, this paper, however, focuses only on the consequences of misuse/abuse of openness of the this space. Figure 1 shows how different cyber entities continuously trying to damage, diminish, misguide, misuse, and abuse various components and subcomponents (both software and hardware) of cyber systems resulting in growing mistrust in different segments of the Internet users (Schneider, 1999).

Online social networks (OSNs) have become part of our daily life; almost everybody has a social presence in blogosphere. Different blog sites attract different people for participating in discussions, share information and forming groups and online community. While blogging, tweeting and other social and business networking usage growing, studies show that most OSN

DOI: 10.4018/ijcwt.2013070102
users are vulnerable to identity theft, target of third-party information tracking (via cookies used by data aggregators). This allows the aggregator to track the user’s movements across multiple websites, their navigation pattern and frequently visited sites. For example, Twitter has archived every tweet (250 million a day) and has agreed a deal allowing the UK-based company ‘Datasift’ to mine through data posted since January 2010. The company will use the information (users’ history, GPS information) to help firms with marketing campaigns and target influential users (Gladdis, 2012). Also OSNs are being used to spread rumors, misinformation and hatred with various intents.

Advertisers use different forms of spam for marketing such as in emails, blogs to promote products or services. It is also used to entice users familiar with the service to exploit search-engine reputation of the hosted service; to attract traffic from “neighboring” blogs, etc. Some companies are using third-parties for mining usage/access data of employees and customers to know their online behavior and loyalties. For furthering their businesses, some companies are not only seeking market data
The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies