CYBER CRIME AND SECURITY

Submitted By Aravindh.S

Abstract:

The opportunities provided by the information and communications technology, with a special emphasis on the Internet, have become an integral part of life. However, are we sufficiently aware and prepared as individuals, nations or the international community for the threats coming from cyberspace or for the denial of the use of that dimension of communication, commerce and even warfare? Namely, despite the growing number of users, the Internet is still beyond or below minimum regulation. Those are precisely the conditions for the organization and realization of hostile action in cyberspace. There are security issues within the cyberspace that represent a security risk and challenge of modern times. The development and application of the information and communications technology has created a new battleground. As a special challenge to international security, cyber terrorism arises. Cyber security will significantly affect international relations in the 21st century. This paper gives an overview of the concepts and principles of cyber threats that affect the safety and security in an international context.

Cyber security for data networks is in its infancy while attackers on networks are becoming increasingly sophisticated. The necessary widespread use of wireless networks provides more vulnerabilities. Network routing is key to a functioning network; once compromised, it can be difficult to recover. For many years, network practitioners have worked on methods to protect that routing through authentication of the updates passed in the network. The missing piece has been a usable, protectable key management system. This proposal uses recent advances in the creation of locally controlled and administered hierarchical web-of-trust certificates to provide a managed secure identity for routers that can be used to protect network routes from attack and misconfiguration. This proposal is the first phase of creating an authenticated routing infrastructure. The work involves adapting advances in evidentiary trust to a link state routing protocol, developing naming for certificate chains and an approach to use the certificates in link state updates. This phase is expected to result in a report and a design for a prototype to be added to open source protocols in a later phase. These results will be made publicly available through open source code and discussions and presentations at standards bodies and with router vendors and network operators. A successful approach should create opportunities to the proposer in contracts with government and commercial organizations. This could result in market opportunities for other organizations such as network management tool and router.