# Securing the National Knowledge Network

S.V. Nagaraj

RMK Engineering College, Kavaraipettai, 601 206, India
svnagaraj@acm.org
http://www.rmkec.ac.in

**Abstract.** The National Knowledge Network is an important initiative of the Government of India approved in the year 2010. This network is expected to connect over 1500 institutions specializing in higher education, research and development, health care, agriculture and governance and provide multi-gigabit connectivity. It is expected to create a revolution by ushering in technological progress through the rapid spread of knowledge. We look at ways of securing this network. We also study various security challenges it is likely to face and suggest remedial measures.

**Keywords:** Security, Knowledge Network, NKN, REN, Computer Networks.

## 1 Introduction

The Government of India approved in March 2010 the setting up of the National Knowledge Network (NKN). According to experts, this network is expected to be fully operational in 2 or 3 years time. It is currently being built by the National Informatics Center (NIC). A knowledge network may be considered as a center of knowledge which helps in the best utilization of available knowledge in order to bring benefits to its users. Many countries have high speed networks which connect various organizations and universities. Such networks are known as research and education networks (RENs). They have become indispensable all over the world. There are many national research and education networks. We give a few examples of such specialized networks.

The Internet2 is an American network that connects several thousand colleges, universities, government organizations, research institutes, libraries as well as schools and museums. Within the USA, there is another such network known as the National Lambda Rail. In Canada, there is a REN known as CANARIE. In Netherlands, the REN is known as SURFnet. In the UK, the REN is the JANET. In South Africa, there is a South African National Research Network (SANReN). ERNET is India's REN. Japan's REN is known as SINET. There are some RENs that span various countries. For example, the GLOBAL RING NETWORK FOR ADVANCED APPLICATIONS DEVELOPMENT (GLORIAD) network connects scientists in US, Russia, China, Korea, Canada, Netherlands, India, Egypt, Singapore, and Nordic Countries. The Trans Eurasia Information Network (TEIN3) connects researchers in China, India, Indonesia, Japan,

N. Meghanathan et al. (Eds.): CCSIT 2012, Part I, LNICST 84, pp. 538–541, 2012.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012

Korea, Laos, Malaysia, Nepal, Pakistan, the Philippines, Singapore, Sri Lanka, Taiwan, Thailand, Vietnam and Australia. Other countries such as Bangladesh, Bhutan and Cambodia are in the process of joining TEIN3. The GEANT is a pan-European REN. Such RENs may also have connectivity to other RENs. For example, TEIN3 has connectivity to GEANT.

## 2 Architecture of the NKN

The NKN will have three layers: a high-speed core (supporting speeds in excess of 10 Gbps), a distribution layer (to support the core), and an edge layer having more than 1500 nodes. The connections to the NKN will be provided through either the core layer or through the distribution layer. NKN will connect educational institutions (such as IITs), research and development institutions (such as CSIR), libraries, laboratories, and nuclear, space and defense research organizations (such as BARC, ISRO, DRDO). NKN will provide a variety of services including Internet, intranet, e-mail, messaging and caching gateways, Domain Name System, Web hosting, Voice over IP, video portals and video streaming. NKN will support IPv4 as well as IPv6 protocols. NKN is a IP-MPLS network that has already connected over 360 institutions (as on Sep 29, 2011). On completion, it will connect more than 1500 institutions. There are many criteria that must be fulfilled by organizations willing to join the NKN. These include compliance with policies for security and malware filtering among others.

## 3 Security Issues

One unfortunate aspect of the NKN design is that it depends on multiple bandwidth providers since no single provider has the geographical spread for creating a pan-India network. It should be emphasized that while the NKN will take care of the security of its core layer, it will not be able to address the security aspects of its numerous end nodes. The end nodes have to troubleshoot applications themselves. Since there are going to be over 1500 end nodes this only means that a large number of people specializing in information security are needed. They are currently unavailable and are unlikely to be available even after 2 or 3 years time. This only means that the potential users of the NKN must be provided information security education.

Various threats such as worms and viruses have shown that they can spread rapidly in networks and from one network to another network. Connecting networks benefits users, however, it also brings its own drawbacks such as the potential for the rapid spread of viruses, worms, spyware and malware. So the NKN must deal with all these threats. Since the NKN will be set up on commercial IP-MPLS networks and since there will be Virtual Private Networks (VPNs) based on these networks, the security aspects of such VPNs must be well studied. The NKN will be a massive network so it will be hard to say how secure it will be. Paraphrasing the well-known adage, we can say that the security of a network will only be as much as its weakest link. If a huge network such as the NKN is going to be designed using network components (such as routers and switches) not produced indigenously it will be hard to ensure its security as there could be Trojans, backdoors, spyware and malware in such network components. It must be ensured that at least core routers and switches are produced indigenously. But that is not going to be an easy task.

There is no doubt that the end nodes of the NKN must protect vital data using anti-virus and anti-malware packages, and by employing firewalls. The deployment of unified threat management systems for securing the NKN must be explored. Open source security software must be studied and developed for utilization by the NKN. It should be noted there is hardly any worthwhile open source anti-virus package. Such specialized software is produced by vendors with huge market presence. So issues such as licensing come into the picture. Updating anti-virus, anti-malware, anti-spyware packages is no easy task. Such updates are currently possible only by accessing the servers of some commercial vendors. We should also note that strict security policies (for say anti-virus, firewalls, anti-spyware, anti-malware) only retards the speed at which applications can be executed. We must also note that Network Address Translation has a similar effect on the performance of applications. However, we should also note that there can be no compromise on security at any point of time.

The NKN should have a dedicated Computer Emergency Response Team (CERT) (such as CERT-IN) on the lines of the emergency response teams of other RENs. The CERT must be responsible for security on a daily basis. Security policy for the NKN should be well-defined and those responsible for its compliance must be identified. Authentication, authorization and access control issues must be taken care of at all points in the network. Security features of the NKN must be clearly established. Security aspects of newer technologies and protocols such as MPLS and IPv6 must be well understood. Spam should be controlled so that it does not spread through the NKN. Denial-of-service attacks should be handled effectively. Hacking of core components on the NKN must be prevented. The principle of least privilege should be used when necessary. Special tools must be developed for checking the health of the NKN. Strong password policies must be used all through the NKN.

Packet filtering should be used wherever needed. Secure shell access must be restricted. Illicit traffic on the NKN must be handled effectively. Vulnerabilities of equipment to denial-of-service attacks should be monitored carefully. Core routers should be well protected from various types of attacks. Intrusion detection systems and intrusion prevention systems should be deployed. Attempted attacks on the NKN infrastructure must be spotted. Ways of protecting core equipment must be thoroughly studied. Anti-spoofing measures should be employed. Network performance must be monitored and poor performance detected and remedial measures should be taken. Packets exceeding rate-limiting thresholds must be observed. There should be notifications when such thresholds are exceeded. The security of roaming access services should be studied before they are deployed. Digital certificates issued by certification authorities must be used to guarantee secure communication between servers, between users, or between a server and a user.

Secure authentication procedures should be employed before allowing access to grid resources especially at sensitive locations (such as BARC). In the future, mobility of users will become paramount so the security of wireless local area networks will become an important concern. Computer security incidents require fast as well as effective response from the organizations concerned. Computer Security Incident Response Teams (CSIRTs) are responsible for responding to computer security incidents. International collaboration is essential to CSIRTs and much depends on their willingness to trust one another. The issue of privacy of users is often overlooked in huge networks. It must be ensured properly in the NKN. System administrators, site security teams and CERTs must receive adequate training and they should be familiar with the latest trends in the security arena. We should remember that security does not come gratis and also that it makes life more complex and difficult. Since RENs such as the NKN connect with other RENs located elsewhere this only implies that close co-operation between their respective CERTs will be required for successfully handling incidents.

## 4 Conclusion

We have seen that security is a complex subject and this is true for huge research and education networks such as the National Knowledge Network. The current shortage and possible future shortage of skilled information security professionals could be a major impediment for ensuring the security of the NKN. We have studied various ways of making the NKN a more secure and more profitable network.

**Acknowledgements.** The author is thankful to his institution as well as the Society for Electronic Transactions and Security (SETS).

## References

1. National Knowledge Network, `http://www.nkn.in`
2. Nagaraj, S.V.: National Knowledge Network: Applications and Challenges. In: Proc. International Conference on Advances in Engineering and Technology (ICAET 2011). Coimbatore Institute of Information Technology, India (2011) ISBN-978-1- 4507-6433-9