Security Model for Educational Satellite Networks

Sanjay Jasola
Indira Gandhi National Open University, New Delhi

Ramesh C. Sharma
Indira Gandhi National Open University, New Delhi

INTRODUCTION

Education has been the greatest tool for human resources development. The advances in information and communication technology has brought out a paradigm shift in the educational sector by making it more accessible, relevant, qualitative, and equitable for the masses. The use of satellite technology like INTELSAT, PEACESAT, and ATS in education has enhanced the opportunities for learners to acquire new skills (Moore & Kearsley, 1996). Both on-campus and distance mode students can be benefited by it. The satellite technology can serve a large geographical area. It allows audio and video signals uplinked from a station to be received to any number of downlink earth stations (Willis, 1995). Oliver (1994) reported that the transmission costs do not increase with the increase in the number of downlink stations. Satellite Instructional Television Experiment (SITE), one of the India's early experiments conducted during 1975 to 1976, produced and transmitted 150 different science programs of 10 to 12 minutes duration, offering them to more than 2,330 villages in six geographical clusters. According to Shrestha (1997) and Govindaraju and Banerjee (1999), this experiment demonstrates the effectiveness of satellite communication for educational purposes.

EduSat is the first exclusive educational satellite of India (*www.edusatindia.org* and *www.ignou.ac.in*), especially designed to provide satellite- based education through the audio-visual medium by employing DTH (direct-to-home) quality broadcast (*www.edusatindia.org*). A complete nationwide coverage is ensured through multiple regional beams. There are five Ku-band transponders with spot beams covering northern, northeastern, eastern, southern, and western regions of India. The entire Indian mainland is covered through the footprint of one national beam of a Ku-band transponder and six channels through extended C-band transponders. A two-way video communication system, Space Collaboration System (SCS), is being used as a cooperative distance education project between Japan, China, and Thailand (Tanigawa, Ileura, Anzai, & Kaneko, 2002). A Direct Broadcast Satellite (DBS) is being used extensively in the United States by the learners to receive educational programs at home or offices through a small inexpensive satellite dish, which soon would take over video broadcasting and narrowcasting (Moore & Kearsley, 2005). The University of the South Pacific also offers distance education to its 12 member countries through its own satellite communication network (USPNet) (see http://www.usp.ac.fj). USPNet is used for audio conferencing among various campuses, and video broadcast of live or pre-recorded lectures.

RELATED RESEARCH

The EduSat network operates under several different operating systems, a variety of Web-based and client/server applications, and other components from several vendors. This heterogeneous network introduces a high level of complexity when it comes to management and security issues. This complexity makes it impossible to effectively secure an entire networking environment with a single component such as a firewall. Such situation calls for a total information security solution, which includes policy and procedure, access control, user authentication, encryption, and content security. By focusing a security solution on only an individual component, such as access control or an encryption method, one risks leaving holes in the security shield that can be exploited by a hacker (Cheswick & Bellovin, 2000). The EduSat network is mainly utilized as the data transport mechanism, so one can expect various attacks mounted from the underlying infra-

structure. The attacks may not necessarily be aimed at the network, but also at the resources attached to the network and the information contained within. These attacks can be of various forms and impact corporate information resources in a variety of ways. The typical points of network vulnerabilities are weak administrative and user passwords, modem connections, system back doors, poor user adherence to security policy, and poorly configured firewalls and Web hosts. The corruption or compromise of data is accomplished in a variety of ways. Corporate data can be damaged, destroyed, and/or stolen when not properly protected. These attacks do not always originate from outside of the trusted environment. The different types of attacks that satellite-based information systems are subjected to are: social engineering, viruses/trojan horses, denial of service (DoS), IP spoofing, worm, replay attack, and theft of information (Oppliger, 1997).

Skinnemoen et al. (2004) proposed a consolidated approach for IP over satellite networks based on open standard DVB-RCS (Digital Video Broadcasting–Return Channel via Satellite). Cruickshank et al. (2005) offered measures for securing multicast in DVB-RCS satellite systems. The overview of the VIP-TEN project architecture and VoIP measurement campaign over the EuroSkyWay test-bed have been presented by Cruickshank et al. (2001). Togel et al. (2005) deployed IP telephony over satellite links and QoS as the enabling technology for the combination of data and voice service. The level of service quality achieved on LAN and satellite links by using QoS mechanisms (available, off–the-shelf routers and switches) has been discussed in Feltrin et al. (2003). Nguyen et al. (2001) reported the performance results of laboratory experiments for VoIP over satellite under different link and traffic conditions. A security system for satellite networks was developed by Cruickshank (1996). Noubir and Von Allmen (1999) have also discussed security issues in Internet protocols over satellite links.

OVERVIEW OF THE SECURITY MODEL

The implementation of a security model within the EduSat network has been achieved in the following, step-by-step manner:

1. **Development of an IT Security Policy:** The development of an IT security policy is carried out in three steps. First, the security level required and appropriate for the company is determined. The IT Security Committee (ITSC) is established with the task of attaining and maintaining the desired level of security. The ITSC then prepares the Internal Security Standards (ISSs).
2. **Elaboration of the Internal Security Standards:** In order to implement security targets, security standards are compiled based on a detailed risk analysis for applications requiring high-level protection and the use of standard security guidelines.
3. **Implementation of the IT Security Standards:** By defining priorities, designating responsible staff, and planning the realization of objectives, the ISS are implemented according to plan.
4. **Training and Awareness:** A training concept is developed in order to prepare all levels of the organization, from management to the end users, to increase their awareness of the security guidelines, to provide the necessary explanations regarding correct IT usage, and to ensure adherence to these guidelines.
5. **Ongoing Security Management:** The IT security process does not end when ISSs have been implemented, but requires periodical controls, which, in case of changes, also provide for the updating of the system security concept. The reactions to any incidents relevant to security are also monitored in order to limit damage and avoid repetition.

IMPLEMENTING THE IT SECURITY PROCESS

The first step in development of an information security model is to establish a high-level security policy. A security policy establishes the rules or protocol under which the entire organization or company will be required to operate. The protocols established in an organization's security policy are incorporated into the daily habits of every employee. The policy is backed up by an ISO 17799-based standards or procedures document that specifies the access control requirements for information and other assets throughout the organization. A typical security standards document will include information like: host and network marking requirements, host security control requirements,