

Intrusion-Detection Mechanism to Detect Reachability Attacks in PNNI Networks (Abstract)

Yves Cosendai, Marc Dacier and Paolo Scotton*

IBM Research Division
Zurich Research Laboratory
Säumerstrasse, 4
CH-8803 Rüschlikon / Switzerland

e-mail: {yvc, dac, psc}@zurich.ibm.com

Paper Submission for Raid'99

Topic: IDS in High Performance and Real-Time Environments

Yves Cosendai is a student at the Swiss Federal Institute of Technology, Lausanne, Switzerland. He is presently completing his specialization year in telecommunications at Institut Eurecom, Sophia-Antipolis, France. Towards his graduation, he is working on his Diploma Thesis at the IBM Research Laboratory, Zurich, Switzerland.

Marc Dacier graduated in Computer Science in 1989 from the Université Catholique de Louvain, Belgium, where he worked from 1989 until 1991 as a research assistant. From 1992 until 1994, He worked as a Ph.D. student in the dependability group headed by Jean-Claude Laprie at LAAS-CNRS in Toulouse, France. He obtained his Ph.D. in Computer Security in 1994 from the INPT in Toulouse, France, with a thesis entitled "Towards a Quantitative Evaluation of Computer Security" showing applications of fault-forecasting techniques to computer security. He then worked as a security consultant at Firstel in Paris, France. He joined the IBM Zurich Research Laboratory in 1996 where he currently is the manager of the Global Security Analysis Laboratory. His group is working on intrusion detection techniques and maintains one of the largest database on computer security vulnerabilities in the world. He has published over 20 papers and reports on his research. He has also spoken internationally at panels, conferences, symposia, and colloquia on these issues. He is a member of various international program committees and is the co-chair of the RAID Executive Committee, together with Kathleen Jackson from the Los Alamos National Laboratory.

Paolo Scotton graduated from Ecole Supérieure en Sciences Informatiques in Sophia Antipolis, France, in 1990 and received the Diplôme d'Études Approfondies and Ph.D. from University of Nice, France, in 1990 and 1993. He pursued his Ph.D. studies on the topic of video compression adapted for ATM networks. In 1994 he joined IBM Laboratory in La Gaude, France, where he worked on ATM control point software design and development. Since 1997, Dr. Scotton is with IBM Zurich Research Laboratory, Switzerland, where his activities include routing protocols, graph theory and routing intrusion detection.

*Contact author

This abstract summarizes the paper that presents the PNNI protocol and an attack directed against it. A novel detection algorithm is also presented. This algorithm is host-based and is implemented directly in the switches. Experimental results demonstrate the efficiency and the limitations of the mechanism.

The ATM forum has defined the private network-network interface (PNNI) for routing and signaling in ATM networks. PNNI routing is a link-state protocol derived from the open shortest path first (OSPF) protocol in which the topology information describing nodes, links, and reachable address prefixes is flooded so that all nodes can compute paths to any reachable destination in the network.

In order to enable routing to the end systems attached to a particular PNNI switch, each switch advertises a set of reachable prefixes. It is possible for an intruder to observe this legitimate information sent by other switches, and to flood false information in order to misroute communications.

Several works on intrusion detection in routing protocols exist, but their focus is more on OSPF. A recent work of SRI International presents a rationale for securing the routing infrastructure of PNNI based on heuristic rules about topology information changes. This work has strong requirements concerning network topology and the distribution of intrusion-detection-capable systems, which makes it more difficult to configure and exploit efficiently.

In this paper a novel algorithm to detect a reachability attack in a PNNI network is proposed. The principle is to observe the prefixes advertised by the nodes in the network and detect overlapping prefixes. The principle of overlapping is discussed in detail in the full paper. The working assumptions related to the development of the detection algorithm, their effect, and the way they are treated are also part of the paper. This results in a mixed approach for the algorithm, which is at the same time behavior-based and knowledge-based.

In a PNNI network it is possible to have an overlapping set by the network administrator for specific applications. Therefore it is necessary to go through a learning phase where the algorithm establishes a model of the normal network behavior. The detection phase is behavior-based in the sense that it detects deviations with regard to the "normal" model. It is also knowledge-based because it includes some knowledge about which kind of overlapping is most likely to constitute an attack.

We have defined three different ways to detect suspicious activities. Each technique can potentially generate an alarm that will be forwarded to the system manager. The full paper will describe those techniques and why we need to deal with several approaches to achieve our goals.

The full paper concludes with a presentation of the experimental framework we have used to implement, test, and validate this approach. Its use within various types of topologies will also be presented.