Detection of Subverted Routers In An Internet: An Audit Based Approach

James E. Pace, Christopher Wee, Biswanath Mukherjee,and Ronald A. Olsson*
{pace,wee,mukherje,olsson}@cs.ucdavis.edu
Department of Computer Science
University of California at Davis

Inter-networking, the connection of computers in a network, is crucial in today's world. Ensuring that networks are secure is a very difficult problem. We present one method of enhancing network security.

A network router is the basic entity which allows inter-networking. A router is a device which has multiple network interfaces, and copies each packet incoming on one interface to an interface closer to the packet's destination. The path a packet takes between source and destination is the route.

A router may act maliciously due to subversion or configuration errors. A subverted router is a powerful adversary; it has the ability to alter or destroy packets, and it can generate packets at any time. Additionally, the router is part of the network, so other elements trust it. This trusted, malicious router can subvert other routers and cause network wide problems.

It is often difficult to ascertain if a network of routers is performing correctly, instead one should focus on the detection of subverted routers [Kum93]. Our research looks at how to detect such a router. Our approach is based on the GOALS method [BWF96], which specifies how to successfully perform security audit. We have determined the auditing requirements for an abstract model of a router. With the resulting audit trails, we use a heuristic to detect the routers which are acting maliciously. Many of the detection concepts are based on [CL97].

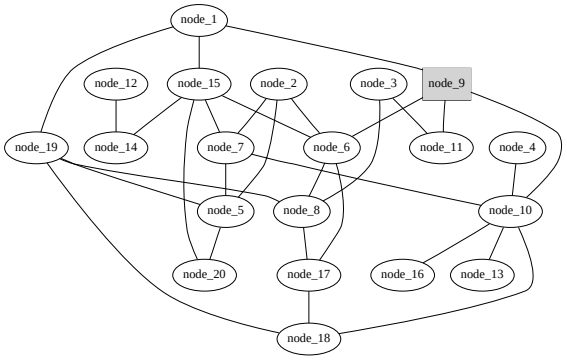

Figure 1: Example Network.

Our model of a router emulates the functionality of a physical router. Each of a router's interfaces is connected to some other network element, such as a point to point link, LAN, or host. The core of the router is the routing table, which makes routing decisions based on the routing function. The routing function takes as an argument a packet with a destination address. The output of the function is the address of one of the router's interfaces, which is where the packet should be delivered.

We have identified the events which cause a change in a router's state. A link status change, a router reboot, receipt of a routing table update, a time out, and network traffic all affect the state of the router. In order to perform a successful audit, all events which cause state changes, as well as the resulting state, which is the routing table, need to be recorded.

The detection heuristic is based on the audit logs

*James Pace is a graduate student working under Biswanath Muhkerjee and Ronald A. Olsson, and Christopher Wee is a post-doctoral researcher. Both work in the UC Davis Security Lab. This project is supported by grants from the NSA and ARPA. Address: Engineering Unit 2, Room 2245, Dept. of Computer Science, UC Davis, Davis CA 95616 Web: http://seclab.cs.ucdavis.edu/nra/

of the routers in the network and the actual network topology. Using the topology, a set of valid routing tables is generated for each router using the Floyd-Warshall all pairs shortest path algorithm. Then, each routing table in the audit trail is compared with the table of valid routes. If a discrepancy is found, our method determines all routers that were part of the route by following the actual routing tables from the source to the destination. The detector increments a suspicion counter for each of these routers. A discrepancy is either a route which does not have the correct metric or a route which does not use an appropriate router.

To test the method, we simulate networks with malicious routers. We generate random networks which are fed to a network simulator. We run the detection mechanism on the resulting logs. The output, which is the number of times each router was incriminated, has consistently placed the malicious element at the top. Figure 1 shows an example network of 20 nodes with 30 links and one malicious router. Using the detection engine produces the results shown in Table 1. The table correctly implies, due to the larger number of implications, that node_9 is a malicious router.

Node	*Implications*
node_9	123
node_10	80
node_1	62
node_11	59
node_6	45
node_15	32
node_3	26
node_13	17
node_4	17
node_16	17
node_14	16
node_2	11
node_8	10
node_19	9
node_12	8
node_17	8
node_20	8
node_7	6
node_18	6
node_5	3

Table 1: Detection Results.

References

[BWF96] Matt Bishop, Chris Wee, and Jeremy Frank. Goal-Oriented Auditing and Logging, 1996.

[CL97] Steven Cheung and Karl N. Levitt. Protecting Routing Infrastructure from Denial of Service: An Intrusion Detection Approach. February 1997.

[Kum93] Brijesh Kumar. Integration of Security in Network Routing Protocols. *ACM SIGSAC Review*, 11(2):18–25, Spring 1993.