Protect Broadcast Addresses Against Misuse

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Shortly after publishing an article about protecting voice-mail, I received the following message from reader A. Robinson (slightly edited, and used with permission):

> You might be interested to know about the voicemail system at one of the “big-5” accounting firms at their offices in Australia. When a person calls after hours they get put through to the voicemail system and can leave a message for a person by choosing their name, or by selecting a “group” of people (which is ideally intended for internal use). Over the course of two weeks several anonymous messages were left to a group that included every single staff member in at least one office of the firm with over 1500 people. The messages were of either rather awful music or maniacal laughter and went for two or three minutes each. Is this the first instance of mass voicemail spam? It was a nuisance for staff arriving in the morning to receive the message, and it also jammed the voicemail system because so many people were trying to check their messages at once [because the messages were so long].<

I don’t know about its being the first instance, but this case illustrates the dangers of configuring uncontrolled broadcast addresses on any network. As the reader notes, such addresses should be restricted to internal use. I would add that they should be restricted to authorized internal users. Broadcast e-mail addresses, for instance, should not be used lightly by employees; sending a message to everyone in the organization has costs, and the costs grow with volume. For example, if the average hourly extended cost (wages + overhead) is even a modest $20 per employee, sending a useless message that requires 1 minute to read to 1,000 people who don’t need it will cost more than $300 in wasted resources. Wasting one minute of the time of even 10 professionals who could be billing $300/hour AND who cost $100/hour in extended costs could be construed as a total loss of $66. Does an organization really want to spend $66 on the latest urban myth, virus hoax or joke?

Worse still, people who bombard large numbers of their colleagues with unnecessary copies of detailed communications risk losing credibility as serious collaborators. Eventually, such broadcasters will find that most of their recipients ignore all of their messages, important or not.

On the technical side, the well-known SMURF denial-of-service attack depends on the unprotected IP broadcast address in a large network with a fast connection to the Internet. The attacker sends requests (e.g., a ping) with a forged originating address in the IP packet header to the broadcast address of an intermediate host, known as the amplifying network. The request is replicated and sent to all IP addresses on the network; these obligingly respond to the request by sending data to the apparent originator – which in this case is actually the designated victim of the denial-of-service attack. Thus the uncontrolled IP broadcast address is used to amplify the original request; as long as the amplifying network’s bandwidth is greater than the bandwidth of the victim’s Internet connection, the victim’s connection will be swamped.

A similar attack is known as Fraggle; Diane Levine and Gary Kessler describe this attack as follows: “. . . [T]he attackers send spoofed User Datagram Protocol (UDP) packets instead of
Echo messages to the broadcast address of the amplifying network. Each system on the
amplifying network that has the specific broadcast address port enabled will create a large
amount of traffic by responding to the victim’s host; if the port is not enabled, the system on the
amplifying network will generate ICMP Host Unreachable messages to the victim’s host. In
either case, the victim’s bandwidth is consumed.” – Chapter 11, “Denial of Service Attacks,” in

The essential protective measure is to enable ingress filtering at the firewall to blocking all
external attempts to use a network’s broadcast address.

And if you have employees who abuse internal broadcast addresses for voice mail and e-mail,
tell them to join a community radio station.

* * *

technical bookstore or from Amazon <http://www.amazon.com/exec/obidos/ASIN/0471412589>
> and Barnes & Noble <

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information
Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <
mabay@compuserve.com >. He invites inquiries about his information security and operations
management courses and consulting services. Visit his Web site at <
http://www.mekabay.com/index.htm > for papers and course materials on information

technology, security and management.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without
limit on any Web site, and to republish it in any way they see fit.