Definity-G(x) Demystified:
By Walt Medak

Q: We think we have our Definity PBX secure against Toll Fraud and Hackers. Is there any report that can tell us if we have had attempts to overcome our security built into the Definity? We change our passwords regularly, but are there back-door ways for hackers to gain entry?

A: There are several things to consider when looking at securing against Toll Fraud and unauthorized entrance to the Definity system. First, most toll fraud experienced by corporate America is from within; i.e., from phones in common-area locations having a too-permissive COR. There are reports within the Definity to tell you about the possibilities of hacker-attacks, but nothing to warn you about suspicious or unusual calling patters. However, there are such warning features inherent in many of today's Call Accounting programs. Those are programs that read the CDR (SMDR) information from your system and allow for a variety of information for security, productivity, cost analysis or many other reasons. Call Accounting programs reside on a workstation or stand-alone PC and connect to the CDR interface from the Definity. Many will activate some type of alarm if calling patterns change or exceed preset thresholds. Some of the more prominent among them that I know of are Micro-Call, CallWhere and Review, all of which work very well.

As for the back-door possibility to your Definity, there is only three ways that I know of to reach the programming area of it. One is, of course, at the programming terminal that usually is installed with the Definity. Second is the INADS port whereby it can be accessed and programmed by dialing into it. And third, inherent in the Version 8 and above, you can access the Definity via an IP address via a Telnet session over a LAN, WAN or the Internet. The latter may be connected to any version of System75 or Definity if using an adjunct unit that's addressable via IP such as the LanSAT by Scottsdale Communications. By changing your passwords regularly you are guarding against a great deal of vulnerability, but you probably don't know all of the logins to your Definity, and if it's not being covered by Avaya or some other security conscious maintenance company, then chances are those other logins are not getting their passwords changed at all. In every Definity there are at least five logins, and in many there will be eight, of which Avaya or whomever will only change three to four of them, and the rest are up to you. You may not even know that there are "customer" level logins other than the one or two that you use, but the possibility is very good if you have had your Definity for over ten years and have upgraded it along the line. To find out how many logins are in your system give the command "list login" and it will show you all that are there. Only the first three or four will be changed by Avaya/whomever, and the rest are yours, and if there are some you don't recognize it's probable they've never had a password changed and might still be at the default. If you go looking around on the Internet, you will be amazed at the information out there revealing everything necessary to hack into your Definity system. Know ALL of your login responsibilities.

Also, enable and make use of the Security Violations Notification feature. If there are repeated attempts to hack into your system, it can be programmed to alarm and notify you at various customizable thresholds.

And finally, the very best "Firewall" for the Definity that I recommend is the "Lock & Key" adjuncts that go between the telephone line and the Definity INADS port. I suppose that everything in hacking is possible, but I can't for the life of me see how anybody can get past these units. One, the Lock, is installed between the INADS port and the telephone line, and the other, the Key, must be programmed to "match" the Lock, and then be used at the dialing computer ahead of the modem. It is by far the best protection I have seen, and is very much the same system that was built into the Definity at the Version 6 level called Access Security Gateway (ASG). If both the Lock & Key system and the ASG are utilized, it would boggle the mind to understand how anybody could ever hack into the system.

What you have asked, and what I have just touched on, is an emerging side-industry of Fraud and Security Consulting which is growing by leaps and bounds because of the skyrocketing incidents to PBX's of all makes. Having secured your system is only a beginning. Keeping it secure is an ongoing project that shouldn't be neglected, as hackers seem to come up with some new technique as the old ones are discovered and blocked.

For a more in-depth discussion of your Definity's security, please contact me if you wish.