On Wednesday April 10, 2002, The San Jose Mercury News reported that a voice-mail message from Hewlett-Packard Chairperson and Chief Executive Officer Carleton S. ("Carly") Fiorina to Chief Financial Officer Robert Wayman had been leaked to one of the newspaper’s reporters. The particulars of this case are not significant for today’s column, but anyone interested in the gory details can just type "Carly Fiorina HP voice mail" into a search engine for more than you are likely to want (GOOGLE.COM produced _pages_ of references to the incident). This case of data leakage should remind network managers that protecting information stored in a voice-mail system should be part of the enterprise systems security mandate. After all, clients can leave orders by phone; suppliers can warn of delivery delays; prospects can request information; executives can discuss highly sensitive matters.

There have been many documented cases of voice-mail penetration. For example, in the late 1980s, a New Jersey magazine publisher began receiving complaints from its customers. Voice mail messages renewing valuable and important advertising had never been heeded. Employees claimed they never received the calls at all; the voice-mail system supplier was called in for technical support but found nothing wrong. Soon, however, customers began reporting that employees’ I’m-not-in-leave-me-a-message blurbs included rude and lewd language. The culprits proved to be a 14-year old and his 17-year old cousin, both residents of Staten Island who had gotten mad at the failure to receive a poster from the magazine publisher. The kids’ sabotage resulted in lost revenue, loss of good will, loss of customers, expenses for time and materials from the switch vendor, and wasted time and effort by the publisher's technical staff. Total cost, according to the victim, was U$2.1 million.

In July 1996, high-school students in the San Francisco area broke into the PBX of a local manufacturing firm and attacked its voice-mail system. They erased information, changed passwords, created new accounts for their own use, and eventually crashed the system through overuse. The company spent $40,000 on technical support from an outside technician.

In November 1996, a former employee of Standard Duplicating Machines Corporation of Andover, MA pleaded guilty to using his knowledge of non-existent security on the firm's voice-mail system to retrieve sales leads and other valuable data on behalf of a direct competitor, Duplo U.S.A. Corporation. Most of the mailboxes had canonical (default) passwords (the voice-mailbox number itself – known in the trade as a “Joe” account).

In May 1997, after MI5 placed ads for recruits in Britain, 20,000 hopeful security agents called in only to hear a disconcerting message on the voice-mail system: "Hello, my name is Colonel Blotch. I am calling on behalf of the KGB. We have taken over MI5 because they are not secret any more and they are a very useless organization."

In May 1998, Michael Gallagher, a reporter for the Cincinnati Enquirer, broke into the voice mail system of Chiquita Fruits. The, ah, fruits of his espionage were stories in the paper accusing Chiquita of illegal activities. The reporter was fired; the Enquirer eventually paid
$10M to Chiquita in damages and published front-page apologies three days in a row to forestall a legal contest.

As late as May 2001, Vodafone Australia's mobile phone voice mail was using a canonical password if a user has not set one.

Recommendations:

* Warn your users never to allow their voice-mail password to be the phone number itself or any other canonical password.
* Scan your own PBX looking for those pesky Joe accounts and change them.
* Change the voice-mail password for an ex-employee’s voice mail immediately upon termination.
* Turn off the remote-access features for your PBX; you can turn it on for maintenance when necessary and then disable it again.
* Make sure your PBX maintenance accounts are properly safeguarded by effective security mechanisms – tokens or biometrics identification and authentication if possible.
* Check regularly to be sure no one has inserted unauthorized voice-mail boxes on your system.

The bottom line: secure your PBX and voice-mail systems with the same attention that you apply to any other computer-based system you care about.

* * *


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 <mkabay@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.