Piggybacking (1)

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

One of my favourite BC cartoons (drawn by Johnny Hart) shows two cavemen talking about a third: "Peter has a mole on his back," says one. The other admonishes, "Don't make personal remarks." The final frame shows Peter walking by--with a grinning furry critter riding piggyback.

For readers whose native language is not English, "piggybacking" (origins unknown, according to various dictionaries) is the act of being carried on someone's back and shoulders. It's also known as pick-a-back. Kids like it.

So do criminals.

Now, if you are imagining masked marauders riding around on innocent victims' backs, you must learn that in the world of information security, piggybacking refers to unauthorized entry to a system (physically or logically) by using an authorized person's access code.

Physical piggybacking occurs when someone enters a secure area by passing through access control at the same time as an authorized person; e.g., walking through a door that has been opened by someone else.

Logical piggybacking means unauthorized use of a computer system after an authorized person has initiated an interaction; e.g., using an unattended terminal that has been logged on by an authorized user.

In a sense, piggybacking is a special case of impersonation--pretending to be someone else, at least from the point of view of the access-control system and its log files.

To interfere with physical piggybacking, we have to avoid making security a nuisance that employees will come to ignore out of contempt for ham-handed restrictions. For example, it is wise to control access to the areas that should be secure but not to unimportant areas.

The other crucial dimension of piggybacking is employee training. Everyone has to understand the risks of allowing normal politeness (e.g., letting in a colleague) to overcome security rules. Letting even authorized people into a secured area without registering their security IDs with the access-control system damages the audit trail but it also puts their safety at risk: in an emergency, the logs will incorrectly fail to indicate their presence in the secured area.

***

In the next article in this series, we'll look at logical piggybacking and how to make it more difficult.

***

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 © 2001 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.