Back Doors (1):
Secret Access

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

In the 1983 movie, *War Games*, directed by John Badham, a young computer cracker (played by a very young Matthew Broderick) becomes interested in breaking through security on a computer system he's located by automatic random dialing ("war dialing") of telephone numbers. Thinking that he’s cracking into a video-game site, he eventually manages to break security by locating a secret password that gives him the power to bypass normal limitations. He goes on to play Global Thermonuclear War--which nearly results in the real thing.

The unauthorized, undocumented part of the source code which bestows special privileges is, in the language of computer security, a "back door," sometimes called a "trap door." A back door will not necessarily cause harm by itself; it merely allows access to program functions – including normal functions – by breaching normal access controls.

Why would anyone install a back door in a program?

In cases where the culprit means no harm, back doors are leftovers from the development and testing phases of software development. When functions are deep in nested series of commands or screens, programmers often insert a shortcut that lets them go directly to a specific function or screen so they can continue testing from that point rather than having to go through the entire sequence of data entry, menu-item selection, and so on. Such shortcuts can significantly shorten testing time for those people unfortunate enough still to be using manual quality assurance techniques (as opposed to automated testing).

The problem occurs when the programmers forget to remove the back doors. When this happens, a poorly-tested program can enter production (use for real business or distribution to real customers) with a dangerous, undocumented feature that can bypass normal restrictions such as edit checks during data entry. Back doors of this kind sometimes result in data corruption, as when a database program allows someone to short-circuit the usual validation of entered data and simply lets a user cut directly to an update function that happens to have bad data in the input buffers.

Back doors are part of a program; they are distinguished from Trojan Horses, which are programs with a covert purpose. A Trojan Horse is a program which has undocumented or unauthorized functions that can cause harm during normal usage by innocent users as well as by criminals. Thus many Trojan Horse programs have back doors, but back doors may exist in programs that would not usually be described as Trojan Horses. A specific kind of Trojan Horse program is known as an Easter Egg; this is usually an undocumented game or display intended by its authors to be harmless. Unfortunately, due to poor programming or software incompatibilities that develop as operating systems change, Easter Eggs can also cause major problems such as system lockups or crashes. All Easter Eggs depend on back doors – usually undocumented keystroke sequences – to be invoked.

In the next installment of this short series, I will give examples of some classic back doors.

***
For more about _War Games_ see <http://us.imdb.com/Title?0086567>.

Easter eggs were featured in this newsletter in the article “Easter Eggs and the Trusted Computing Base” (2000-03-27) http://www.nwfusion.com/newsletters/sec/0327sec1.html

***


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.