Good Intentions

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

According to a recent news summary in _Innovation_, biometric technology is advancing rapidly enough that we can expect to see mobile phones that will enforce sensible security rules. John Gehl and Suzanne Douglas wrote, "Two scientists at Carnegie Mellon University are developing technology that one day may be capable of sensing when you're just too busy to take a phone call. The technology uses tiny microchips, cameras and sensors to analyze body language in order to determine whether a person is engrossed in a task. Pounding away at a computer keyboard, closing your office door, or conversing animatedly with another person would all serve as possible indicators that a person is too occupied to take a call."

This kind of automated interpretation of human motivation and intentions sends shivers up my spine. The potential for error and abuse is limitless. We have already seen countless examples of assumptions made by system designers turning out to be faulty; my favorite is the Windows Update, which by design has no user controls over it at all. Once activated, it – like the sorcerer’s apprentice’s brooms – cannot be shut off or even slowed down in its relentless, 12-times-an-hour checking for Windows updates. Once it’s been set in motion, the only way to control the Update is to remove the software entirely.

Well, imagine the innumerable situations in which the tiny microchips, cameras and sensors could make a mistake in analyzing human needs. Let’s start with controlling cellular phone abuse. Can't you just imagine someone designing a feature in mobile phones that whispers in the earpiece, "Lower your voice -- you are talking too loudly in public about corporate information." Then the phone shuts off if you ignore it – right in the middle of a critical discussion of response to a potentially disastrous breach of security at the corporate data center.

Or how about, “You are driving at 20 miles per hour over the speed limit in heavy traffic: don’t you think it would be wise to STOP TALKING ON YOUR PHONE??” Whereupon the driver actually does get shot by the maniac who has been stalking him for the last ten miles because his phone call to the police was interrupted by proxy by a programmer who designed the safety system without an override.

For real nightmares, I leave you to imagine a phone that monitors your speech to ensure compliance with a designer’s standards of politically correct speech. I imagine what such a device might do with peculiar words and phrases that have one meaning in ordinary discourse but a quite different meaning in a different context. For example, I remember one conversation with a system manager 20 years ago when I was on tech support for Hewlett Packard. He had had just had a system crash and I routinely asked, “Did you take a dump?” There was a long pause on the phone line, and the system manager replied with obvious puzzlement, “Yeesesss, but what does that have to do with the computer?” “No, no, “ I said, “a CORE dump!”

More seriously, the same technology might lend itself to identification and authentication for computer access. For example, software might identify authorized users by face, keyboard rhythm and voice and thus decrease the rate of both false positives (accepting an interloper) and
false negatives (rejecting the rightful user). But in all cases, we should be very careful to insist on safety overrides that maintain control by the human being on the spot, not by the human being who thought he or she could predict all possible situations and limit human response in advance. For example, an authorized user could have a secondary authentication method that could allow access even in the case of a false negative.

In any case, I hope that enthusiasts of remote control will remember the road surface of the highway to hell.

* * *

For further reading:

About INNOVATION &lt; http://www.newsscan.com/innovation-sample.html &gt;


Kabay, M. E. (2000). May the power be with you: A design philosophy for software engineers. ACM Ubiquity &lt; http://www.acm.org/ubiquity/views/m_kabay_4.html &gt;

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see &lt; http://www3.norwich.edu/msia &gt; for full details.


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 &lt;mailto:mkabay@norwich.edu&gt;; Web site at &lt; http://www.mekabay.com/index.htm &gt;.

Copyright © 2003 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.